PARADIGM INITIATIVE

UNE ANALYSE SUR

SUR LES PRATIQUES DE DONNÉES

DES

APPLICATIONS DE PRÊT NUMÉRIQUE EN AFRIQUE

UNE ÉTUDE SUR 19 PAYS

UNE ANALYSE SUR LES PRATIQUES DE DONNÉES DES APPLICATIONS DE PRÊT NUMÉRIQUE EN AFRIQUE

UNE ÉTUDE SUR 19 PAYS

Juin 2022.

Auteures: 'Gbenga Sesan, Bonface Witaba, Dércio Tsandanza, Jackline Akello, Steven Akomian
Éditeurs de Copie: Nana Nwachuckwu

Paradigm Initiative
374 Borno Way
Yaba
Lagos, Nigeria
hello@paradigmhq.org

Conținut

4
5
9
19
26
36
51
60
66
79
88
98
105
110
118
112
136
148
156
163
171

Introduction
Angola
Cameroon
Cap-Vert
Côte d’Ivoire
Egypt
Eswatini
Ethiopie
Gabon
Ghana
Kenya
Mali
Morocco
Mozambique
Namibia
Nigéria
Afrique du Sud
Tanzanie
Ouganda
Zimbabwe
Conclusion

Introduction

La prolifération de l'infrastructure numérique dans les pays africains a entraîné une augmentation de l'accès à l'internet. La déréglementation des services de télécommunications conduit à l'innovation et à la concurrence, ce qui favorise la réduction des coûts de connexion, augmentant ainsi le nombre d'internautes. Par conséquent, le partage d'informations, y compris de données personnelles, est devenu plus accessible et plus répandu. Cette facilité a soulevé des inquiétudes quant à l'abus de l'accès aux données personnelles par les entreprises, l'usurpation d'identité par les particuliers et le ciblage malveillant à l'aide d'informations personnelles identifiables. L'Union européenne a répondu à ces inquiétudes sur la sécurité des données personnelles en promulguant le Règlement général sur la protection des données (RGPD). Dans le monde entier, ce règlement a incité les pays à adopter des lois de protection des données très strictes et à créer des autorités de protection des données.

Alors que 32 pays d'Afrique ont promulgué des lois[1] sur la protection des données, les derniers en date étant le Rwanda, l'Afrique du Sud et le Kenya, certaines lacunes permettent à des sociétés axées sur la technologie d'avoir un accès déloyal aux données transmises par les failles de la protection et de leur mise en application. En l'absence d'une protection adéquate des données personnelles, de nouvelles sociétés financières profitent de la mise à disposition de ces données pour cibler les personnes vulnérables du numérique et les immigrés avec des prêts « sur salaire ». Les prêts sont accordés avec peu ou pas de vérifications des antécédents en échange de données personnelles, parmi lesquelles figurent, entre autres, des informations sur l'employeur, des listes de contacts de téléphones portables, etc. Le recouvrement pour défaut de paiement de ces prêts utilise un dispositif de "honte publique".

Paradigm Initiative a analysé la protection des données et les applications de prêt dans dix-neuf (19) pays africains. Ce rapport décrit en détail les lois de protection des données de ces pays, les failles de protection exploitées par ces plateformes de prêt numériques et les types de données personnelles visibles et collectées par ces sociétés d'applications de prêt.

Dans l'ensemble des pays de cette enquête, 12 pays disposent d'une législation standard en matière de protection des données et offrent un cadre juridique et institutionnel clair pour la gestion des données personnelles, tandis que les 7 autres sont en train de mettre en place des lois sur la protection des données ou s'appuient sur des lois spécifiques au secteur pour la réglementation et l'orientation. Il est toutefois intéressant de noter que des pays comme le Ghana et le Nigeria soumettent les fintechs numériques à des lois bancaires et à des réglementations de la Banque Centrale qui les obligent à passer par des étapes et des règles précises pour être accréditées. Ces réglementations n'accordent que peu d'attention aux données des consommateurs.

Les applications mobiles non conventionnelles de banque et de prêt analysées ont recueilli des informations personnelles identifiables malgré le niveau d'autorisation accordé par l'utilisateur. Malgré l'existence des lois sur la protection des données dans les pays analysés, les applications mobiles trouvent le moyen de contourner la législation avec des autorisations "tout en un". Dans certains cas, la localisation d'un utilisateur a été enregistrée par l'application mobile de prêt

1 Paradigm Initiative and Olumide Babalola LP. Data Protection Authorities (DPAs) In Africa: Un rapport sur l'établissement, l'indépendance, l'impartialité et l'efficacité des autorités de contrôle de la protection des données au cours des deux décennies de leur existence sur le continent. (2021)

sans autorisation ni consentement. Les applications partagent des informations personnelles identifiables, dont les données de localisation, avec des tiers sans que l'utilisateur ait la possibilité de se soustraire à ce partage d'informations. Les applications ne précisent pas pendant combien de temps ces données sont partagées avec les tiers. Des logiciels malveillants cachés dans certaines applications automatisent des paiements non autorisés au nom des utilisateurs et dérobent également des informations financières et personnelles sensibles. Les pays dotés de mécanismes de réglementation plus stricts, comme l'Angola, ont pu mettre fin aux activités de certaines applications, comme l'application de prêt Xikhila.

Il ressort clairement de l'étude que, si les applications mobiles de prêt font état des informations qu'elles collectent, ces informations ne sont pas évidentes au moment de l'inscription et sont souvent cachées en petits caractères. Par ailleurs, il n'existe que peu ou pas d'informations sur le degré d'accès ou de contrôle d'un utilisateur sur ses données stockées. Il est important que les autorités compétentes en matière de protection des données dans les différents pays se penchent sur l'impunité des abus de données dans les applications de prêt numérique afin de prendre des mesures appropriées pour protéger les personnes concernées, et qu'elles collaborent avec d'autres parties prenantes pour sensibiliser à la protection des données.

Angola

Profil du pays

Situé en Afrique australe, l'Angola est un pays lusophone dont la population[2] est estimée à 31 millions d'habitants pour un PIB d'environ à 208,034 milliards en 2019. Ce pays lusophone au Sud de l'Afrique a obtenu son indépendance du Portugal en 1975[3]. Le président actuel, João Lourenço, a été élu en 2017, après plus de 30 ans de gouvernance par le précédent chef d'État, José Eduardo dos Santos.

2 Statistiques de l'Angola, Banque mondiale https://data.worldbank.org/country/AO > consulté le 15 août 2021.
3 Barrow Munslow, " Angola: The Politics of Unsustainable Development' (1999) 20(3) Third World Quarterly 551-568.

Protection des données en Angola

Selon DLA Piper[4], l'Angola régule les questions de confidentialité et de protection des données en vertu de la loi sur la protection des données (loi n° 22/11, 17 juin 2011)[5], de la loi sur les communications électroniques et la loi sur les services de la société de l'information (loi n° 23/11, 20 juin 2011)[6], et de la loi sur la protection des systèmes et réseaux d'information (loi n° 7/17, 16 février 2017)[7].

Data Guidance relève[8] que le décret présidentiel 214/16 du 10 octobre 2016 établit les règles qui régissent la structure et le fonctionnement de l'organisme de réglementation, l'Agence nationale de protection des données (APD)[9]. L'Angola a également promulgué la loi 11/20 du 23 avril 2020 sur l'identification et la localisation des téléphones cellulaires[10], et la surveillance électronique[11] effectuée par les autorités policières.

L'Angola compte trois entreprises de téléphonie mobile, Movicel, Unitel, et l'entreprise publique Angola Telecom, qui avait le monopole des services téléphoniques jusqu'en 2005. La pénétration de l'Internet en Angola est de 31 %, tandis que l'accès à la téléphonie mobile

4 https://www.dlapiperdataprotection.com/index.html?t=law&c=AO > consulté le 15 août 2021.
5 https://platform.dataguidance.com/sites/default/files/lei_de_proteccao_de_dados_pessoais_v.pdf > consulté le 15 août 2021
6 https://minttics.gov.ao/fotos/frontend_10/gov_documentos/lei_das_comunicacoes_electro_19324146535f1886da78b9b...s_sociedade_da_informacao.pdf > consulté le 15 août 2021.
7 https://minttics.gov.ao/fotos/frontend_10/gov_documentos/redes_e_sistemas_informaticos_20864175955f109a14374be.pdf > consulté le 15 août 2021.
8 https://www.dataguidance.com/notes/angola-data-protection-overview > consulté le 12 août 2021.
9 https://apd.ao/fotos/frontend_1/editor2/200420_lei_11-20_de_23_abril-identificacao_celular_vigilancia_electronica.pdf > consulté le 13 août 2021.
10 https://apd.ao/fotos/frontend_1/editor2/200222_lei_2-20_de_22_janeiro-videovigilancia.pdf > consulté le 13 août 2021.
11 https://apd.ao/fotos/frontend_1/editor2/200222_lei_2-20_de_22_janeiro-videovigilancia.pdf > consulté le 13 août 2021.

s'élève à plus de 15 millions d'utilisateurs, soit 46 % de la population totale[12].

Dans son rapport « Net 2020 »[13], Freedom House qualifie le " niveau de liberté sur internet « de l'Angola comme »[14] relativement libre ". Il n'y a pas de restrictions gouvernementales sur l'accès à l'Internet. À l'exception de la pornographie enfantine et du contenu protégé par le droit d'auteur, le gouvernement ne bloque ni ne filtre le contenu internet. Il n'existe aucune restriction sur le type d'informations échangées en ligne.

Système financier et Fintech en Angola

La Banque Nationale d'Angola (BNA) est la principale entité de gestion du secteur financier en Angola. En ce qui concerne les transactions électroniques, le fait le plus marquant est l'adoption de la loi sur la prévention et la lutte contre le blanchiment d'argent, le financement du terrorisme et la prolifération des armes de destruction massive.[15] Elle stipule que les institutions financières qui autorisent les virements électroniques doivent inclure des informations dûment vérifiées dans le message ou le formulaire de paiement accompagnant le transfert, notamment le nom complet, le numéro de compte, l'adresse et, le cas échéant, le nom de l'institution financière du donneur d'ordre. La réglementation concernant les applications mobiles comme Xikila Money est minimale.

Dans un article publié le 26 juillet 2021, AllAfrica[16] indiquait que l'Angola était devenu le pays le plus vulnérable avec les cybercriminels professionnels du monde entier qui ciblent la population florissante d'utilisateurs de téléphones mobiles en Afrique. Selon le rapport de "State of Mobile Fraud in Africa"[17], l'Angola est l'un des pays les plus vulnérables d'Afrique, où 34 % des transactions mobiles sont suspectes.

Le rapport précise[18] également que les applications malveillantes contiennent secrètement des logiciels malveillants et sont programmées pour effectuer des paiements au nom des utilisateurs à leur insu. Il y a aussi le clickjacking, où un fraudeur intercepte un clic légitime et dirige à son insu l'utilisateur vers un site web frauduleux. Ce site web peut subtiliser des données financières sensibles et d'autres données personnelles.

Selon Statista[19], 29,4 millions de transactions bancaires mobiles ont été enregistrées en Angola en mars 2021, soit une augmentation substantielle par rapport au même mois de l'année précédente. Les internautes ont effectué 7,4 millions d'opérations bancaires avec un appareil mobile en mars 2020 sur l'Application Multicaixa Express, lancée en 2019. Après avoir configuré une ou plusieurs cartes de débit sur l'Application, l'utilisateur peut se servir d'un appareil mobile pour exécuter des paiements, faire des achats et des transferts en ligne.

Xikila Money : L'application mobile de prêt d'argent

Lancée en 2017 par Banco Postal[20], Xikila Money était une plateforme qui permettait d'utiliser le téléphone mobile comme un portefeuille numérique et, sur cette base, d'effectuer divers paiements via le téléphone mobile. L'application utilise les téléphones mobiles comme des comptes bancaires pour effectuer des transactions financières et

12 Digital 2021 in Angola - Hootsuite https://datareportal.com/digital-in-angola, consulté le 20 mai 2021.
13 Freedom House Angola https://freedomhouse.org/country/angola/freedom-net/2020, consulté le 1er juin 2021.
14 L'Angola a obtenu 62/100 points https://freedomhouse.org/country/angola/freedom-net/2020, consulté le 14 août 2021.
15 Loi nº 05/2020 du 27 janvier https://www.bna.ao/uploads/%7B5ff3bf3f-eba6-4b79-94e4-f16d8a01e74c%7D.pdf, consulté le 12 août 2021
16 https://allafrica.com/stories/202107260738.html, consulté le 13 août 2021.
17 https://www.techfinancials.co.za/2021/07/26/mobile-fraud-continues-to-hit-africa-hard/, consulté le 15 août 2021.
18 https://www.bizcommunity.africa/Article/410/793/218325.html, consulté le 15 août 2021.
19 https://www.statista.com/statistics/1228848/number-of-transactions-with-mobile-banking-in-angola/, consulté le 15 août 2021.
20 https://www.menosfios.com/conheca-xikila-money-um-servico-permite-efectuar-pagamentos-via-mobile/, consulté le 11 août 2021.

octroyer des prêts[21]. Pour commencer à utiliser le service Xikila Money, il faut ouvrir un compte dans une agence Xikila Money et effectuer un dépôt. L'application est disponible pour les utilisateurs[22] d'Android et d'iOs.

Suspension de l'application

La plateforme semblait avoir connu un certain succès en Angola. Dans un reportage publié en 2017[23], l'Angola Journal mentionnait que l'application avait déjà atteint 100 000 clients en sept mois, augmentant plus de 40 000 comptes en seulement deux mois. Cependant, une décision de la Banque Centrale d'Angola (BNA) a changé l'histoire en 2019.

La principale raison annoncée par la BNA était l'incapacité de Banco Postal à se conformer aux liquidités financières requises pour opérer en Angola.[24] Banco Postal disposait de 200 points locaux du réseau Xikila Money dans la capitale Luanda et dans la ville de Huambo[25] et la banque affirmait avoir plus de 250 000 clients avant sa fermeture. À l'heure actuelle, le site Web de Xikila Money ne fonctionne plus.[26]

Aperçu des données collectées par les applications de prêt numérique

Xikila Money	Informations collectées et traitées par l'application	
	Autorisations requises	Comme l'application était associée à une banque, l'une des principales autorisations requises était l'identification personnelle du client et l'historique de ses transactions financières.
	Informations recueillies auprès de l'utilisateur	Lire l'état et l'identité du téléphone Localisation approximative (sur le réseau) Localisation précise (GPS et réseau) Trouver des comptes sur l'appareil
	Informations recueillies auprès de l'appareil de l'utilisateur	Recevoir des données d'Internet Afficher les connexions réseau Accès complet au réseau Fermer d'autres applications Contrôler les vibrations Empêcher l'appareil de se mettre en veille
	Utilisation des informations de l'utilisateur par l'application	Consulter le statut et l'identité du téléphone Afficher les connexions Wi-Fi Enregistrer des données audio - l'application nécessite un microphone pour la validation sécurisée des transactions.
	Stockage des informations sur l'utilisateur par l'application	Informations d'identification Compte bancaire Transactions avec d'autres utilisateurs

Le retrait de la licence de la Banque postale et l'interdiction de l'appli Xikila Money limitent notre analyse. Cependant, nous avons pu constater via Google Play que la dernière mise à jour de l'appli date de mai 2018, soit près d'un an avant son interdiction par le gouvernement angolais, ce qui est d'autant plus vrai que les termes et conditions

21 Xikila Money - Un nouveau service financier change le visage de la banque en Angola https://www.youtube.com/watch?v=PW392kJVm7w, consulté le 14 août 2021

22 https://play.google.com/store/apps/details?id=tagattitude.mwallet.app.xikila et https://appadvice.com/game/app/xikila-money/1261392972 consulté le 14 août 2021.

23 https://www.jornaldeangola.ao/ao/noticias/detalhes.php?id=393253, consulté le 14 août 2021.

24 https://novojornal.co.ao//sociedade/interior/bna-tambem-fechou-o-xikila-money-um-servico-bancario-inovador-em-angola-e-de-utilidade-confirmada-pelos-utilizadores-65247.html, consulté le 16 août 2021

25 Article https://sol.sapo.pt/artigo/650953/joao-lourenco-limpa-sistema-bancario, consulté le 12 août 2021.

26 http://www.xikilamoney.co.ao/, consulté le 14 août 2021.

d'utilisation devant contenir la politique de confidentialité sont inaccessibles.[27] D'une part, l'absence de site web n'a pas permis d'accéder à davantage de données sur la manière dont les tiers authentifient les "cookies" ou suivent les informations des utilisateurs.
Bien qu'elle soit restée sur le marché angolais pendant une courte période, Xikila Money a constitué une nouvelle méthode de circulation des finances en Angola. D'après les informations obtenues dans ce qui reste de l'application, nous constatons un grand volume de données collectées auprès de ses utilisateurs. Une chose importante à noter est le silence de l'Agence de protection des données pendant la période où Xikila Money opérait dans le pays. Il n'y a aucune mention que l'Agence de protection des données ait jamais fait des observations sur la façon dont l'application collectait et utilisait les informations de ses clients.

Par exemple, l'un des principaux problèmes qui se posent encore aujourd'hui est que certains clients et travailleurs ont perdu leurs comptes et attendent toujours une indemnisation de Banco Postal.[28] L'article 16 de la loi sur la protection des données stipule que "le traitement des données personnelles concernant le crédit et la solvabilité ne peut être effectué qu'avec le consentement de la personne concernée et avec l'autorisation de l'Agence de protection des données." Or, cela n'a pas été le cas, et les clients de Xikila Money ignorent toujours l'avenir de leurs données après l'interdiction de Banco Postal.

27 http://www.xikilamoney.co.ao/TermosUtilizacao, consulté le 17 août 2021.
28 https://www.novagazeta.co.ao/artigo/1186 / https://valoreconomico.co.ao/artigo/80-dos-trabalhadores-do-extinto-banco-postal-continuam-no-desemprego, consulté le 17 août 2021.

Cameroun

Profil du pays

Situé en Afrique centrale, le Cameroun, ou République du Cameroun, compte 25 876 380 habitants[29]. Il partage une frontière avec le Nigeria, le Tchad, la République centrafricaine, le Congo, le Gabon, la Guinée équatoriale, et une ouverture maritime sur le Golfe de Guinée. Deux langues officielles : le français et l'anglais, y sont parlées. Son PIB est estimé à 39,01 milliards USD (2019) et représente plus de 40% de celui de la Communauté économique et monétaire de l'Afrique centrale, dont elle est membre. Elle est régie par un régime présidentiel.

29 countryeconomy.com 2022. Cameroun. [en ligne] Disponible sur : https://fr.countryeconomy.com/pays/cameroun, consulté le 11 février 2022.

Protection des données au Cameroun

Le Cameroun ne dispose pas d'un cadre juridique précis et adapté à la protection des données personnelles. En attendant la mise en place d'une législation et la nomination d'un organisme indépendant chargé de la protection des données personnelles, seules les communications électroniques et le marché des TIC sont réglementés. La réglementation émane des textes suivants :

- Loi n° 2010 / 012 du 21 décembre 2010, relative à la cybersécurité et à la cybercriminalité,
- Loi n° 2010 / 013 du 21 décembre 2010, régissant les communications électroniques,
- La loi n° 2010/021 du 21 décembre 2010, régissant le commerce électronique,
- Loi n ° 2006/018 du 29 décembre 2006, régissant la publicité, et
- Loi n ° 2011/012 du 6 mai 2011, relative à la protection des consommateurs.
- Au niveau réglementaire, le Décret n° 2013/0399 / PM du 27 février 2013 fixe les modalités de protection des consommateurs de services de communications électroniques.
- Au niveau continental, le Cameroun a ratifié la Convention de l'Union africaine (UA) sur la cybersécurité et la protection des données personnelles du 27 juin 2014 .
- Et au niveau communautaire, le Cameroun a adopté la directive n° 07/08-UEAC-133-CM-18 et le règlement n° 03/16-CEMAC-UMAC-CM du 21 décembre 2016, relatifs aux systèmes et incidents de paiement qui traitent des questions relatives aux données personnelles collectées lors des transactions de mise en relation à divers services de communication électronique.

L'Agence de régulation des télécommunications (ART)[30] et l'Agence nationale des technologies de l'information et de la communication (ANTIC)[31] gèrent ces différentes réglementations. Pourtant, leur marge d'action en matière de protection des données informatiques personnelles est étroite. En effet, la protection des données informatiques personnelles par l'ART apparaît comme un incident dans ses missions réglementaires et reste limitée au secteur des télécommunications, qui n'est pas le seul à pouvoir restreindre les données personnelles. L'ANTIC trouve son origine dans la loi sur les communications électroniques, bien que la loi ait précisé son champ d'intervention sur la cybersécurité et la cybercriminalité. L'analyse de ces missions laisse penser qu'elles couvrent la protection des données informatiques personnelles dans leurs missions formulées de manière assez large. Cependant, à la lecture des missions, il ne ressort pas une qualification particulière de l'ANTIC en matière de protection des données personnelles. La loi sur la cybersécurité et la cybercriminalité de 2010 se limite à la protection des données personnelles au niveau pénal. Cette restriction s'explique par l'impossibilité d'intervenir en cas d'activité contentieuse relative à la protection des données personnelles, tant pour le juge pénal que pour le juge administratif.[32] Ce processus restreint laisse présager des dérives dans le traitement des données personnelles au Cameroun.

Introduction

Le développement quasi généralisé du Mobile Money (MM) en Afrique subsaharienne (ASS) peine à prendre de l'importance en Afrique centrale[33]. Selon le rapport 2019 de l'Association mondiale des opérateurs mobiles(GSMA), sur environ 400 millions de comptes actifs en ASS, moins de 10% étaient localisés dans la sous-région Afrique centrale. Le Cameroun domine les autres pays en termes de développement du MM dans cette sous-région. Son taux de pénétration pour le MM est de 15%, et le volume des transactions associées a représenté 76% sur les 7 964 milliards de FCFA réalisés en 2018 en Afrique centrale.

En raison des activités du MM, les transactions sont principalement portées par les opérateurs de téléphonie mobile, à savoir Orange Cameroun et MTN Cameroun. Ces deux leaders du marché de la téléphonie mobile au Cameroun ont réalisé un chiffre d'affaires cumulé de 500,3 milliards de FCFA au cours de l'année 2020. Selon Orange Cameroun, le service Orange Money lancé en 2011 représente un chiffre d'affaires de 9 600 milliards FCFA par an, soit près de deux fois le budget de l'État du Cameroun au cours de l'exercice 2021. A la fin de l'année 2020, MTN Cameroon a réalisé un chiffre d'affaires de 1,73 milliard de rands (environ 66 milliards de FCFA).

Ces deux opérateurs proposent à plus de 20 millions d'abonnés à la téléphonie mobile au Cameroun, des activités de dépôt et de retrait, de transfert d'argent, de paiement de factures, de salaires, et tout ce qui est paiement marchand, etc. à partir de leurs comptes MM. Conscients du potentiel de ce marché, ils ont décidé de se tourner vers les activités de microcrédit. Orange Money Cameroun, a donc déposé une demande d'agrément en 2019 pour développer ses services en s'orientant vers le microcrédit. MTN Cameroun est en train de finaliser une démarche similaire à la fin de l'année 2020. Les Fintechs et les entreprises de l'écosystème économique et bancaire non domiciliées au Cameroun sont

30 L'Agence de régulation des télécommunications (ART) est un établissement public administratif doté de la personnalité juridique et de l'autonomie financière, créé par la loi sur les communications électroniques. En tant qu'établissement public administratif, l'ART est placée sous la tutelle administrative du ministère des postes et télécommunications (MINPOSTEL) et sous la tutelle financière du ministère des finances (MINFI). Sa création est régie par le décret n° 2012/092 et n° 2012/180 d'avril 2012 portant création, organisation et fonctionnement de l'Agence nationale des technologies de l'information et de la communication.

31 L'ANTIC est un établissement public administratif doté de la personnalité morale et de l'autonomie financière dont les principales missions sont d'assurer pour le compte de l'Etat : la promotion et le suivi de l'action des pouvoirs publics en matière de Technologies de l'Information et de la Communication (TIC) ; la régulation, le contrôle et la surveillance des activités liées à la sécurité des systèmes d'information et des réseaux de communications électroniques ainsi que la certification électronique en collaboration avec l'ART.

32 Article 74 de la loi n° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité.

33 L'Afrique centrale regroupe les 6 pays de la Communauté économique et monétaire de l'Afrique centrale (CEMAC) : Cameroun, République centrafricaine, Congo, Gabon, Guinée équatoriale et Tchad. Et la République démocratique du Congo (RDC).

à l'origine de ces offres de prêts basées sur des applications mobiles. Ces applications sont Treoloans App[34] , Cameroon Direct Loan Hub[35] et Kiva[36]. Dans un environnement macroéconomique sans cadre réglementaire fondamental pour la protection des données personnelles, la prolifération de ces offres, au-delà des bénéfices attendus sur l'inclusion financière, peut poser des problèmes pour la vie privée de leurs utilisateurs. La question est de savoir si les pratiques de traitement des données de ces applications, telles que définies dans leurs politiques et conditions d'utilisation, prennent en compte l'intérêt du respect de la protection de la vie privée ? Cette étude a pour objectif d'analyser les politiques de confidentialité et les conditions d'utilisation de ces applications et d'examiner leur respect des différentes lois relatives à la protection des consommateurs (utilisateurs) au Cameroun. La première partie comprend un aperçu des données collectées par ces applications. La deuxième partie examine leurs activités de traitement au regard des différentes lois sur la protection des consommateurs. La dernière partie indique enfin si ces applications respectent ou non la loi sur la protection des données personnelles.

Aperçu des données collectées par les applications de prêt numérique

TreoLoans Application[37] Lien de téléchargement : Google Play Store	Informations collectées et traitées par l'application

34 Treoloans App est une application mobile permettant d'obtenir des prêts sans garantie compris entre 5 000 et 30 000 FCFA (environ 9 dollars US) et à des taux d'intérêt mensuels compris entre 10 % et 30 % au Cameroun. Elle est proposée aux personnes disposant de comptes MM auprès des opérateurs mobiles Orange Money Cameroun et MTN Money Cameroun à partir d'avril 2019.

35 Cameroon Direct Loan Hub est une offre d'EasyLoan pour les prêts numériques. Fondamentalement, EasyLoan ne prête pas ses propres fonds mais fournit simplement une plateforme de mise en relation entre les fournisseurs de prêts et les demandeurs. Son objectif est de supprimer le protocole bancaire traditionnel entre les agents ayant besoin de financement et les agents ayant une capacité de financement.

36 Kiva App est une offre de Kiva US pour les prêts numériques. Kiva est une plateforme de crowdfunding qui permet aux fournisseurs et aux demandeurs de prêts de se connecter et d'interagir facilement. Son objectif est de s'affranchir du protocole bancaire traditionnel entre agents ayant un besoin de financement et les agents ayant une capacité de financement. Les membres de l'offre Kiva peuvent bénéficier de prêts à partir de 25 dollars. Actuellement, la communauté Kiva est composée de 1,9 millions de personnes qui ont bénéficié d'un crowdfunding estimé à 1,4 milliard de dollars de prêts à 3,4 millions d'emprunteurs dans plus de 90 pays.

37 Conditions générales de l'application TreoLoans. La politique de confidentialité de TreoLoans est contenue dans les conditions générales.

	Autorisations demandées	Au démarrage de l'application, TreoLoans App demande d'accéder à la position de l'utilisateur, position précise (GPS et réseau) et position approximative (réseau). Accéder à l'appareil photo pour prendre des photos et filmer des vidéos. Accéder aux informations d'identité de l'utilisateur et rechercher des comptes sur l'appareil de l'utilisateur. Accéder à Photos / Multimédia / Fichiers, modifier ou supprimer le contenu de la mémoire de stockage USB et lire le contenu de la mémoire de stockage USB. Accéder aux numéros de téléphone des utilisateurs, afficher et modifier les contacts, rechercher des comptes sur l'appareil et appeler directement des numéros de téléphone. Accéder au stockage, modifier ou supprimer le contenu de la mémoire de stockage USB et lire le contenu de la mémoire de stockage USB. Accédez au microphone et enregistrez un fichier audio. Accéder aux informations de connexion Wi-Fi et afficher les connexions Wi-Fi. Effectuer diverses actions : recevoir des données avec la connexion Internet, s'exécuter au démarrage, empêcher l'appareil de se mettre en veille, modifier les paramètres audios, afficher les connexions réseau et avoir un accès complet au réseau.
	Informations recueillies auprès de l'utilisateur	Lors de la souscription au service de prêt, TreoLoans App collecte des informations personnelles sur l'utilisateur sans spécifier la nature ou la qualité de ces données.
	Informations collectées à partir de l'appareil de l'utilisateur Informations collectées à l'aide du site web	TreoLoans App collecte diverses informations sur l'appareil de l'utilisateur sans spécifier le type de données. TreoLoans ne fournit aucune information sur le site web
	Informations reçues de tiers	L'application ne donne aucune information sur les données obtenues auprès de différents tiers.
	Utilisation par l'application des informations relatives aux utilisateurs	La politique de confidentialité de TreoLoans indique qu'elle collecte les données des utilisateurs à diverses fins non spécifiées dans sa politique de confidentialité.

	Informations partagées avec des tiers Durée des données Accès aux tiers	TreoLoans partage les informations des utilisateurs avec différents tiers non spécifiés dans sa politique de confidentialité. La politique de confidentialité de TreoLoans indique qu'elle partage des informations avec des tiers sans préciser la durée de l'accès aux données qui leur est accordé.
	Technologies de suivi du site web/cookies	La politique de confidentialité et le site Web de TreoLoans sont sans aucune précision sur l'utilisation des cookies.
	Stockage des informations sur l'utilisateur par l'application	La politique de confidentialité de TreoLoans indique qu'ils prennent toutes les mesures pour assurer la sécurité des données collectées sur les utilisateurs. Cependant, ils ne fournissent aucune information sur la période de stockage des données collectées.

Cameroon Direct Loan Hub[38] External Download Link et Google Play store	Informations collectées et traitées par l'application	
	Autorisations demandées	Au démarrage de l'application, Cameroon Direct Loan Hub demande à voir les connexions réseau et à obtenir un accès complet au réseau.
	Informations collectées auprès de l'utilisateur	La politique de confidentialité de Cameroon Direct Loan Hub est ne comporte aucun renseignement sur les informations qu'elle recueille auprès des utilisateurs.
	Informations recueillies sur l'appareil de l'utilisateur Informations recueillies lors de l'utilisation du site web Cameroon Direct Loan Hub	La politique de confidentialité de Cameroon Direct Loan Hub ne mentionne aucun renseignement sur les informations recueillies dans l'appareil d'un utilisateur. La politique de confidentialité de Cameroon Direct Loan Hub ne mentionne pas les informations recueillies sur son site Web. En outre, le site Web du fournisseur de l'application n'est pas accessible.
	Informations reçues de tiers	La politique de confidentialité de Cameroon Direct Loan Hub ne donne aucune précisions sur les informations des tiers
	Utilisation des informations de l'utilisateur par l'application	La politique de confidentialité de Cameroon Direct Loan Hub ne mentionne pas l'objectif des données collectées auprès des utilisateurs.
	Informations partagées avec des tiers Durée de l'accès des données aux tiers	La politique de confidentialité de Cameroon Direct Loan Hub ne fait aucune mention des informations partagées avec des tiers. La politique de confidentialité de Cameroon Direct Loan Hub ne mentionne pas la durée pendant laquelle les tiers peuvent accéder aux informations personnelles des utilisateurs et sur la durée de possession de ces informations.

38 Cameroon Direct Loan Hub et le fournisseur de son application n'ont pas de politique de confidentialité.

	Technologies de suivi du site web/ cookies	La politique de confidentialité de Cameroon Direct Loan Hub ne prévoit pas l'utilisation de "cookies". En outre, le site web associé à l'application n'est pas fonctionnel.
	Stockage des informations de l'utilisateur par l'application	La politique de confidentialité de Cameroon Direct Loan Hub ne donne aucune précision sur la sécurité, la confidentialité et la durée de conservation des données collectées.

Kiva[39] Lien de téléchargement : Google Play Store et Apple Store	Les informations collectées et traitées par l'application	
	Autorisations demandées	Au démarrage de l'application, Kiva App demande à recevoir des données d'internet . Afficher les connexions réseau . Bénéficier d'un accès complet au réseau . Empêcher l'appareil de se mettre en veille Kiva App se réserve également le droit d'ajouter d'autres demandes d'autorisation pour son interface utilisateur.
	Informations recueillies auprès de l'utilisateur	Lors de la souscription au service de prêt, Kiva App collecte les informations de l'utilisateur : prénom et nom, photo, adresse électronique et adresse physique, numéro de téléphone, description et bilan de l'entreprise, références personnelles, conditions de prêt souhaitées, compte de paiement et certaines informations démographiques, informations sur les médias sociaux de l'utilisateur.
	Informations collectées à partir de l'appareil de l'utilisateur Informations collectées lors de l'utilisation du site Web Kiva	L'application Kiva recueille les informations suivantes à partir de l'appareil d'un utilisateur : informations sur l'appareil, y compris le type de mobile et le numéro de téléphone, les informations sur la localisation actuelle fournies par la technologie GPS et d'autres services de localisation. Références du compte de paiement de l'utilisateur Dès qu'un utilisateur utilise le site web Kiva App sur son téléphone mobile, le nom, l'adresse électronique et un moyen d'authentifier le compte de l'utilisateur (par exemple, un mot de passe) sont recueillis. Les informations et les commentaires postés sur toute autre page Web hébergée par Kiva (telle qu'une page de prêt, un blog ou un forum de bénévoles) ou par le biais de la fonction Kiva Lender Mail sont également collectés.
	Informations reçues de tiers	L'application obtient des informations d'autres entités du groupe, de Kiva (filiales), des bureaux d'information du crédit (BIC), des fournisseurs de réseaux mobiles, des agences de recouvrement, des partenaires commerciaux, etc.

39 Politique de confidentialité de Kiva App

	Utilisation des informations de l'utilisateur par l'application	La politique de confidentialité Kiva's déclare qu'elle collecte les données des utilisateurs aux fins suivantes : Vérifier l'identité d'un utilisateur Traitement des transactions d'un utilisateur Crédit et modèles dans l'évaluation des prêts, les décaissements et la collecte des paiements. Obligations de Kiva envers les utilisateurs Conformité avec les réglementations applicables concernant les exigences KYC "Know Your Customer", PBC, "Prévention du Blanchiment de Capitaux", et la lutte contre le financement du terrorisme. Communications promotionnelles et services de marketing.
	Informations partagées avec des tiers Durée de l'accès des données aux tiers	Kiva partage les informations des utilisateurs avec: Ses filiales, sa société mère et d'autres filiales de notre société mère (« son groupe »). Toute personne agissant au nom d'un utilisateur Des agences d'évaluation du crédit ou d'autres institutions financières Des partenaires commerciaux dans le cadre de transferts, cessions, fusions et acquisitions d'entreprises, etc. De prestataires de services tiers, notamment les GAFA (Google, Facebook, etc.) et Twitter. La politique de confidentialité indique qu'elle partage les informations avec des tiers pendant une période raisonnable, sans préciser explicitement la durée de cette période.
	Technologies de suivi / cookies du site web	Le service de prêt Kiva utilise des cookies, des balises web et d'autres systèmes automatisés pour collecter des données sur le comportement des utilisateurs. L'application précise ces éléments dans sa politique en matière de cookies. Avec ces outils, Kiva et son site web récupèrent des informations de manière indépendante et par le biais d'outils et de programmes tiers (tels que Google Analytics). Les données collectées comprennent certaines informations techniques (par exemple, votre itinéraire vers le site Web, les pages visitées, l'adresse IP d'origine, le type d'appareil, le type de navigateur, la langue du navigateur, le type de connexion réseau, ainsi que la date et l'heure de votre visite).

	Stockage des informations sur l'utilisateur par l'application	Kiva recueille et stocke toutes les données aux États-Unis. Kiva, ses sociétés affiliées, ses prestataires de services, ses agents et ses représentants aux États-Unis ou ailleurs dans le monde peuvent consulter ces informations personnelles. Kiva s'engage également à respecter sa politique de confidentialité, quel que soit le lieu de traitement de vos informations personnelles. La politique de confidentialité de Kiva indique également qu'elle prend des mesures raisonnables pour maintenir une sécurité physique, technique et administrative appropriée afin d'aider à prévenir la perte, l'utilisation abusive et l'accès non autorisé, la divulgation ou la modification des informations.

Étude de cas : Construction et mise à disposition de bases de données sur l'historique de crédit des clients de Kiva.

Le modèle de développement de Kiva facilite l'octroi de petits prêts dans plus de 80 pays en mettant en relation les personnes ayant besoin d'un financement et celles ayant des capacités de financement. Pour ce faire, Kiva met à disposition des bases de données sur les historiques de crédit des bénéficiaires dans le cadre d'un vaste système de crédit en ligne. Ces bases de données, qui sont librement accessibles, résultent de la collecte de données personnelles (nom, prénoms, sexe, historique de crédit, etc.) des utilisateurs. Cette pratique n'est pas clairement indiquée dans les politiques de confidentialité de Kiva et peut conduire à des abus. De même, le consentement donné par les utilisateurs lors de la souscription aux offres de prêts Kiva ne devrait pas justifier la communication de leurs données à d'autres utilisateurs. L'Etat camerounais doit donc mettre en place une réglementation et une autorité dédiée à la protection des données personnelles.

Outre la question du partage des informations sur l'historique de crédit des utilisateurs de Kiva, les législateurs camerounais doivent également se pencher sur la relation entre Kiva et certains géants du numérique : Facebook, Google et Apple. En effet, la politique de confidentialité de Kiva indique que lorsque les utilisateurs se connectent à leur site web via leur compte Facebook, les informations relatives au compte (adresse électronique, photo du compte, liste des amis Facebook qui utilisent également Kiva) sont collectées. Grâce à ce dispositif, Facebook peut obtenir les activités de prêt des utilisateurs de Kiva sans que l'utilisateur ne donne son consentement explicite. Cette pratique se produit également avec les comptes Google et Apple.

Analyse des pratiques de protection des données des applications de prêt numérique par rapport aux lois sur la protection des droits des consommateurs au Cameroun

Le Cameroun ne disposant pas de législation dédiée à la protection des données personnelles, il n'est pas aisé d'analyser les pratiques des applications de prêt numérique à la lumière des textes existants. Les lois sur la protection des consommateurs et celles relatives à la sécurité des communications électroniques ne servent pas l'objectif du droit numérique. Cette carence constitue un terrain propice au traitement illicite des données personnelles et à la violation des droits numériques des utilisateurs d'applications de prêt numérique et de toute autre activité de ce type.

Les différents aspects des pratiques de traitement des données des applications de crédit numérique au Cameroun ne sont pas conformes aux principes et normes internationaux

de protection des données personnelles. Une législation et une autorité spécifiques sont nécessaires pour obliger les responsables du traitement des données de ces applications à adopter des politiques de confidentialité des données plus responsables. Dès qu'un organisme soutenu par la loi sera créé à cette fin, il devra disposer des compétences matérielles et techniques nécessaires à l'exercice de ses fonctions. Ces ressources lui permettront de contrôler en temps réel le volume, la qualité et la quantité de données collectées par les responsables du traitement des données des applications mobiles et autres processeurs de données.

Cap-Vert

Profile du pays

Avec une population estimée à 550 000 habitants et un PIB de 4,323 milliards en 2019, le Cap-Vert, également appelé Cabo Verde, comprend dix îles volcaniques qui se trouvent à 620 km au large de la côte ouest de l'Afrique. Praia, située sur l'île de Santiago, est la capitale du Cap-Vert. Le Cap-Vert se compose de neuf îles habitées, d'une île inhabitée et de divers îlots. Les îles sont restées une colonie portugaise jusqu'en 1975.[40]

40 Carling, Jørgen, et Luís Batalha. 'Cape Verdean Migration and Diaspora' in Transnational Archipelago : Perspectives on Cape Verdean Migration and Diaspora, Carling Jørgen et Batalha Luís (eds) (Amsterdam University Press, 2008) 13-32.

Protection des données au Cap-Vert

Le Cap-Vert offre aux individus plusieurs droits constitutionnels et statutaires à la protection des données personnelles. La Constitution contient des dispositions importantes pour la protection des données et fournit une marge de légitimité supplémentaire. Le Cap-Vert a deux lois importantes sur la protection des données : La loi 133-V-2001 sur la protection des données personnelles (telle que modifiée par la loi n° 41/VIII/2013 - Régime juridique général pour la protection des données personnelles des individus (uniquement disponible en portugais ici) et la loi n° 121/IX/2021 du 17 mars 2021. En 2001, le Cap-Vert a adopté sa loi phare sur la protection des données, la loi n° 133.

Depuis lors, la loi a subi plusieurs modifications. En 2013, le Parlement a adopté la loi n° 41 pour compléter et mettre à jour la loi n° 133. Plus récemment, en mars 2021, le Parlement a adopté la loi n° 121 pour préciser les responsabilités de l'autorité cap-verdienne de protection des données, connue sous le nom de Comissão Nacional de Proteção de Dados Pessoais (CNPD). Le régime juridique du Cap-Vert en matière de protection des données s'inspire de l'Europe[41]. La loi sur la protection des données (« la loi ») couvre le traitement des données par des moyens automatisés et non automatisés par des entités établies au Cap-Vert ou la collecte ou la transmission de données personnelles par tout moyen dans le pays.

Fintech et systèmes financiers au Cap-Vert

La première intervention de la Banque du Cap-Vert en tant que régulateur de système de

41 https://dataprotection.africa/cape-verde/ et https://www.dataguidance.com/notes/cape-verde-data-protection-overview consulté le 2 août 2021.

paiement a eu lieu en 2018, lorsque la Banque a lancé l'application mobile de prêt d'argent Makeba. La réforme du cadre réglementaire du système de paiement cap-verdien, décret-loi nº 7/2018, du 28 novembre[42], a réglementé les questions relatives aux principes directeurs que tout système de paiement opérant dans le pays doit respecter pour garantir l'efficacité et la sécurité. L'un des principes énumérés à l'article 10 du décret-loi fait référence à la définition de politiques et de mécanismes de sécurité pour garantir la fiabilité opérationnelle d'un système de paiement, y compris les paiements mobiles.

Le 17 juin 2021, la Banque du Cap-Vert[43] a publié un règlement visant à établir les exigences de base pour renforcer l'efficacité et la sécurité de la mise en œuvre des services de paiement mobile au Cap-Vert. L'article 1 indique qu'il vise à établir les exigences de sécurité minimales et normes applicables à la sécurité des paiements mobile et qui doivent être respectées par les prestataires de services de paiement (PSP).

L'article 4 fait référence aux questions de sécurité et souligne que la conception du service de paiement mobile doit être axée sur des mécanismes permettant la transmission, le traitement ou le stockage d'informations sensibles de manière sûre et sécurisée. Il définit également des politiques et l'adoption de mesures pour prévenir et détecter la modification ou la falsification des informations. Il ajoute que les prestataires de services de paiement (PSP) doivent mettre en œuvre des processus fiables de suivi des transactions et des systèmes permettant d'identifier les profils de paiement anormaux et de prévenir les comportements frauduleux.

L'une des dispositions qui a attiré notre attention est l'article 6 de ce même texte. La Banque du Cap-Vert indique que le prestataire de services de paiement mobile doit garantir des procédures rigoureuses d'authentification du client pour l'autorisation du paiement, conformément à la définition fournie dans ce règlement. La même banque souligne que les prestataires de services de paiement doivent s'assurer que le service fourni intègre des mécanismes sécurisés de stockage des données de transaction. L'instrument doit comporter une référence permettant d'identifier l'opération de paiement, la date et l'heure d'exécution, la modification des paramètres et l'accès aux données, permettant ainsi la traçabilité des transactions à tout moment.

Enfin, les processus mis en œuvre et les fichiers de journalisation doivent permettre d'identifier et de retracer la source qui initie le paiement (point de vente, internet) et le bénéficiaire (commerçant). Nous constatons qu'il s'agit d'une mesure qui donne aux prestataires de services un pouvoir excessif dans le suivi des informations de leurs clients.

Makeba : l'application mobile de prêt d'argent

L'application est arrivée sur le marché financier capverdien en 2018[44]. Les utilisateurs peuvent télécharger l'application sur les systèmes iOS ou Android[45]. Il s'agit d'une application qui permet aux utilisateurs d'effectuer des retraits et des prêts ou de déposer de l'argent chez BAI-CV[46] ou chez les marchands Makeba adhérents. Comme l'indique cette application, Makeba fonctionne par la lecture d'un code QR ou de données biométriques. Pourtant, elle ne précise pas à quelles données personnelles elle accède, d'autant plus que c'est l'agent qui gère l'application qui lit les données et pas forcément le client. En d'autres termes, l'utilisateur doit remettre son téléphone portable au gestionnaire pour qu'il lise les données avant de déposer ou de prêter l'argent.

42 Décret-loi nº 7/2018, du 28 novembre https://www.bcv.cv/pt/O%20Banco/Sectores/Documents/2018/Bo_28-11-2018_78.pdf, consulté le 29 juillet 2021.
43 Banque du Cap-Vert https://www.bcv.cv/pt/Paginas/Homepage.aspx, consulté le 2 août 2021.
44 https://www.makeba.money/cv-por/howitworks.html, consulté le 1er août 2021.
45 iOS - https://itunes.apple.com/pt/app/makeba-money/id1458893785 et Android - https://play.google.com/store/apps/details?id=money.makeba.makebamoney&hl=pt_cv, consulté le 3 août 2021.
46 https://www.bancobai.cv/particulares/produtos-e-servicos/servico-de-pagamento/makeba, consulté le 3 août 2021.

Lors de son lancement, le PDG de Makeba, Yamandou Alexander, avait souligné[47] que l'application apporterait plus de facilité et de dynamisme dans les affaires. Cependant, plus de deux ans plus tard, rien ne prouve qu'elle révolutionne le marché financier du Cap-Vert, car des doutes subsistent quant à son fonctionnement. On ignore combien de clients elle compte et le solde monétaire actuel des transactions depuis le début de sa mise en œuvre au Cap-Vert.

Aperçu des données collectées par les applications de prêt numérique

Makeba[48]	Les informations collectées et traitées par l'application Makeba	
	Autorisations demandées	En acceptant le contrat, BAICV s'engage à fournir à l'utilisateur le service MAKEBA selon les conditions et modalités décrites dans les clauses de la convention. L'utilisateur autorise l'inscription au débit de son compte courant auprès de la Banque. Cette écriture de débit reflète les montants correspondant aux paiements qu'il effectue par le biais du service MAKEBA et l'écriture de crédit ou de débit des sommes liées aux virements bancaires qu'il reçoit ou commande, respectivement, par le biais du service MAKEBA.
	Information collected from the user	Carte d'identité. Carte d'identité nationale, passeport, permis de séjour. Numéro d'identification du contribuable, pays/ville de naissance, adresse, ville, boîte postale, téléphone, mobile et e-mail. L'obligation de fournir le service MAKEBA ne prendra effet qu'après confirmation de BAICV ou d'un tiers pour son compte et en son nom. Cette confirmation montrera que le service MAKEBA a été activé (par la communication à l'utilisateur que le service MAKEBA est opérationnel). La BAICV émettra la confirmation de l'acceptation des conditions par l'utilisateur. Cette confirmation se fait par le biais du numéro de téléphone mobile fourni par l'utilisateur lors de la souscription au service MAKEBA. Pour que BAICV puisse fournir le service MAKEBA à l'utilisateur, ce dernier devra acquérir l'autorisation d'utilisation et installer l'application MAKEBA sur un appareil mobile doté d'un système d'exploitation iOS ou Android. L'obligation de fournir le service MAKEBA n'est contraignante que si et aussi longtemps que le client de façon cumulée : a) Conserve le numéro de téléphone mobile qui lui est fourni actif sur son appareil mobile. b) Conserve les informations d'identification que le client utilise pour effectuer des transactions MAKEBA, actives au moment de chaque utilisation. c) S'assurer que le client reçoit la notification push demandant la confirmation de la transaction MAKEBA sur l'appareil mobile du client ou est installée l'application.

47 https://expressodasilhas.cv/eitec/2018/12/14/app-que-permite-transferir-dinheiro-e-pagar-online-e-lancada-para-a-semana/61403, consulté le 28 juillet 2021.

48 Politique de confidentialité - https://www.makeba.money/cv-por/terms.html/ https://www.makeba.money/app/terms/terms-money-cv-por.html, consulté le 10 août 2021.

	Informations recueillies à partir de l'appareil de l'utilisateur	L'utilisateur autorise BAICV à traiter les informations personnelles fournies par l'utilisateur à BAICV. Cette autorisation s'inscrit dans le cadre de l'exécution et de la maintenance du présent contrat. Elle comprend les informations transmises lors de l'installation et de l'utilisation de l'application MAKEBA, directement ou indirectement, dont la finalité est la fourniture du service MAKEBA par BAICV à l'utilisateur. Les données personnelles sont collectées selon la procédure KYC (Know Your Customer) conformément à la loi sur la protection des données personnelles et autres législations applicables en vigueur au Cap-Vert. Le traitement des données personnelles fournies par l'utilisateur à la Banque dans le cadre de la souscription et de l'entretien se fait également dans le cadre de la loi sur la protection des données personnelles en vigueur au Cap-Vert. Bien que le propriétaire de l'application MAKEBA effectue le traitement des données, c'est ce dernier qui définit la finalité et les moyens du traitement, étant l'entité responsable de celui-ci. L'utilisateur accepte que, dans les limites légales, les stockages effectués par le système informatique à travers lequel le service MAKEBA est fourni et qui se rapportent aux opérations effectuées par l'utilisateur soient utilisés par BAICV à des fins de preuve, de communication d'informations statistiques ou agrégées, ou autres.
	Les informations recueillies lors de l'utilisation du site web de Makeba	Le site web ne demande pas l'authentification des cookies.
	Les informations reçues de tiers	Informations financières (compte bancaire) Numéro d'identification fiscale (NIF).
	Utilisation des informations de l'utilisateur par l'application	Chaque utilisateur est associé à un seul numéro de téléphone portable et à un seul numéro d'identification fiscale (NIF). Dans les transferts MAKEBA effectués par l'utilisateur, ce dernier reconnaît que le destinataire ne recevra les fonds transférés que s'il est déjà un utilisateur ou s'il le devient à cette fin. L'utilisateur autorise BAICV à transmettre ses données à la société MAKEBA INC, dont le siège social est aux États-Unis d'Amérique, et aux sociétés du groupe BAI. Une clause restrictive interdit à la société d'utiliser ces données à d'autres fins que celles pour lesquelles elles ont été recueillies et les protège contre toute publication ou accès non autorisé. Elle empêche également le Titulaire d'accéder aux données ci-dessus pour leur rectification, leur mise à jour et leur élimination aux textes de la loi.

	Informations communiquées à des tiers	L'utilisateur affirme qu'il autorise BAICV à transmettre à des tiers agissant pour son compte ses données personnelles, indispensables pour l'activation, le suivi, la gestion et la maintenance du service MAKEBA et le développement de toute activité liée à celui-ci.
	Durée de l'accès des tiers	a) Pendant un minimum de 7 (sept) ans à compter de la dernière transaction ou de la fin du contrat b) Tant qu'il existe des obligations découlant de la relation contractuelle. c) Tant que les droits de BAICV peuvent être invoqués.
	Technologies de suivi / cookies du site web	Le site web ne demande pas l'authentification des cookies.
	Stockage des informations sur l'utilisateur par l'application	Informations financières Informations sur les contacts

Makeba est une application qui offre une communication élaborée à ses clients. Son site web présente un tutoriel clair sur la façon dont les clients peuvent adhérer au service, avec une explication détaillée, du téléchargement à l'utilisation. Bien qu'il y ait une section contact, elle ne fonctionne pas. En effet, on ne sait pas si les responsables de la plateforme ont reçu le message vu qu'il n'y a pas de notification. Dans une partie, l'application indique que Makeba est destinée à être utilisée par des personnes et des entreprises qui se font confiance. La principale exigence pour utiliser l'application est de vérifier l'identification, au moins en ajoutant la carte d'identité sur la plateforme, ce qui montre clairement la transmission de données personnelles.[49]

La section FAQ[50] apparaît sans aucune mise en évidence, et elle précise que l'utilisateur ne peut pas annuler les transactions une fois qu'elles ont été approuvées. Elle souligne que les dernières technologies de cryptage pour protéger les comptes des clients et garantir la confidentialité de leurs données sont utilisées. Si les utilisateurs soupçonnent que leur compte est compromis, ils doivent contacter les responsables de l'application.

En outre, on ne sait pas comment la technologie cryptée est appliquée pour protéger les données des clients, car en accédant à l'application, on ne peut pas voir les informations recueillies. L'application indique que les dépôts effectués sur Makeba sont sécurisés par le partenaire bancaire Banco BAI Cabo Verde pour ce qui est des données personnelles. L'application mentionne également que les clients doivent utiliser leur NIB pour accéder au compte Makeba et transférer leurs fonds bancaires. On ignore comment ce NIB est conservé et dans quelle mesure la Banco BAI-CV peut gérer ou accéder aux données du client, surtout lorsqu'il s'agit d'informations sensibles sur les comptes bancaires des clients. Un cas qui a gagné en visibilité dans les médias est lié à une amende que l'Agence de protection des données (CNPD) a imposée à la Banque centrale du Cap-Vert et à une banque commerciale appelée Novo Banco Cabo Verde[51]. Cette amende était due à la divulgation dans la presse d'une liste de 50 débiteurs de la banque commerciale. Les sanctions étaient

49 https://www.makeba.money/cv-por/limits.html, consulté le 29 juillet 2021.
50 https://www.makeba.money/cv-por/faq.html, consulté le 30 juillet 2021.
51 On sait que l'amende était d'environ 30 000 dollars https://www.voaportugues.com/a/banco-de-cabo-verde-e-novo-banco-multados-violar-lei-proteccao-de-dados/3898368.html, consulté le 29 juillet 2021.

liées au fait que les banques n'ont pas pris les mesures appropriées pour protéger les données personnelles. La Banque centrale et la Banque commerciale ont toutes deux fait appel devant le tribunal.

Lorsque la liste a été rendue publique, la Banque du Cap-Vert et le ministère des Finances ont pris leurs distances. L'objet de l'enquête de la CNPD n'était pas de savoir comment la liste a été rendue publique mais s'il y a eu des violations de la protection des données des clients par la Banque[52]. Nous constatons que cette partie montre les faiblesses de l'utilisation d'applications comme Makeba pour protéger les données de leurs clients. Cependant, elle indique également une certaine action de l'agence de protection des données.

Étant donné que le Cap-Vert est un pionnier de la législation sur la protection des données en Afrique, nous constatons que l'Agence de protection des données se concentre clairement sur la manière dont le secteur financier utilise les données de ses utilisateurs. Toutefois, nous n'avons pas pu vérifier comment les régulateurs peuvent appliquer ces actions aux applications mobiles de prêt d'argent comme Makeba. Il n'existe pas d'exemples marquants d'activités de la CNPD visant à protéger les données des utilisateurs de ces applications, ce qui constitue une véritable lacune. D'autre part, nous ne voyons pas beaucoup d'actions de la part de la Banque du Cap-Vert, qui en principe devrait être l'institution chef de file sur la façon dont ces applications sont utilisées, d'autant plus qu'il n'y a pas beaucoup d'initiatives autres que Makeba.

52 https://www.dn.pt/lusa/banco-central-e-novo-banco-de-cabo-verde-multados-por-falha-na-protecao-de-dados-8563648.html, consulté le 28 juillet 2021.

Côte d'Ivoire

Profil du pays

La République de Côte d'Ivoire est un pays francophone d'Afrique de l'Ouest qui compte plus de 26 millions d'habitants en 2020[53]. Ce pays partage ses frontières avec le Mali, le Burkina Faso, le Ghana, le Liberia et la Guinée et représente 40 % de l'économie de l'Union économique des États de l'Afrique de l'Ouest (UEMOA). Le PIB du pays est estimé à 58,54 milliards USD, et il est régi par un système de gouvernement présidentiel.

53 Source Fiche pays Côte d'Ivoire produite par l'Atlas des Pays et des Populations du Monde et disponible au lien suivant : https://www.populationdata.net/pays/cote-divoire/

Protection des données en Côte d'Ivoire

La protection des données personnelles en Côte d'Ivoire est couverte par la loi n° 2003-450[54]. Cette loi s'applique à tout traitement automatisé ou non effectué dans le territoire de la Côte d'Ivoire[55]. Il est difficile de savoir si la règle s'applique aux données des Ivoiriens résidant en dehors du pays. L'Autorité de Régulation des Télécommunications de Côte d'Ivoire (ARTCI) est l'APD nationale en Côte d'Ivoire. L'ordonnance n° 2012-293 du 25 juin 2013 a créé l'organisme mais règlemente les traitements de données à caractère personnel par la loi n° 2003-450 du 16 juin 2013[56]. Elle est chargée de veiller au respect des dispositions légales en matière de traitement des données personnelles et de s'assurer que les différents traitements ne portent pas atteinte aux libertés et à la vie privée.[57]

Introduction

Avec une part de marché de 70,9%, le Mobile Money[58] est en plein essor en Côte d'Ivoire. Il est commercialisé par les principaux opérateurs de téléphonie mobile[59], qui se partagent 20 789 662 abonnés. Conscients du potentiel de ce marché, deux (2) de ces opérateurs, à savoir Orange et MTN, se sont lancés dans le crédit numérique, une offre de services

54 Source Fiche pays Côte d'Ivoire produite par l'Atlas des Pays et des Populations du Monde et disponible au lien suivant : https://www.populationdata.net/pays/cote-divoire/

55 Article 3 de la loi n° 2003-450 du 16 juin 2013.

56 Disposition pertinente ?

57 Article 47 de la loi n° 2003-450.

58 Le Mobile Money est une monnaie électronique créée par les opérateurs de télécommunications et stockée dans un porte-monnaie électronique relié au forfait téléphonique. Cette technologie permet aux utilisateurs d'envoyer ou de recevoir de l'argent numérique par l'intermédiaire de leur téléphone. Il suffit de connaître le numéro de téléphone du destinataire pour lui envoyer de l'argent. Ainsi, le numéro de téléphone mobile est devenu, en quelque sorte, un numéro de compte bancaire sans avoir de compte bancaire. Cependant, les coûts de l'argent mobile restent bien inférieurs à ceux d'un compte bancaire. D'où sa popularité et le fort soutien des populations au Mobile Money.

59 Orange, MTN et Moov sont les 3 opérateurs de téléphonie mobile en Côte d'Ivoire.

financiers qui permet à la population ivoirienne d'accéder à des prêts rapides et à court terme via des applications mobiles. Cet accès rapide offre et favorise l'inclusion financière des personnes peu bancarisées, les aide à régler leurs dépenses courantes, et présente une opportunité pour la population d'être une source potentielle de développement du marché financier en Côte d'Ivoire. Pour preuve, la première offre de crédit numérique lancée le 16 février 2018 par MTN et Bridge Microfinance Côte d'Ivoire a attiré 1 900 000 clients en un an.

En juillet 2020, Orange a lancé une offre similaire. Entre juillet 2020 et le 31 mai, son service de microcrédit a mis 44 milliards de FCFA de prêts à la disposition des clients ivoiriens, dont 1,2 million de demandes de prêts traitées pour des montants compris entre 5 000 FCFA et 250 000 FCFA. Le portefeuille d'Orange comptait 6 000 clients à la fin du mois de mai 2021, et les dépôts d'épargne ont été rémunérés à un taux de 3,5 %, ce qui représente 1,5 milliard de FCFA. Pour le recouvrement des prêts et le suivi des plans d'épargne, ces opérateurs collectent les données personnelles de leurs clients par le biais d'applications mobiles[60] qui servent d'interface utilisateur. Cette pratique peut porter atteinte à la vie privée des utilisateurs et doit être questionnée avec impartialité. Ces services de prêts basés sur des applications mobiles ont vu le jour après l'adoption de la loi sur la protection des données personnelles en Côte d'Ivoire[61]. Il est donc primordial de savoir si les pratiques de traitement des données de ces applications, telles que définies dans leurs politiques et conditions d'utilisation, tiennent compte de la régulation sur la protection de la vie privée. Cette étude vise à analyser les politiques de confidentialité, les termes et conditions de ces applications et à examiner leur conformité avec la loi sur la protection des données en Côte d'Ivoire. La première partie comprend un aperçu des données collectées par ces applications. La deuxième partie examine leurs modalités de traitement au regard de la loi sur la protection des données personnelles. La dernière partie conclut en indiquant si ces applications sont conformes ou non à la loi sur la protection des données personnelles.

Aperçu des données collectées par les applications de prêt numérique

Orange Money Africa[62] Lien de téléchargement : Google Play Store et Apple Store	Informations collectées et traitées par l'application

60 Le service de microcrédit et de micro-épargne de MTN Mobile Money, appelé MOMO KASH, repose à la fois sur un code USSD associé au numéro de téléphone et sur l'application mobile MyMTN CI. Les deux sont associés au compte MTN Mobile Money du client. Du côté d'Orange Côte d'Ivoire, le service de microcrédit et de micro épargne appelé Tik-Tak est également associé à un code USSD et à une application mobile : Orange Bank Africa. Les deux sont associés au compte Orange Money du client.

61 Loi n° 2013-50 du 19 juin 2013 relative à la protection des données à caractère personnel en Côte d'Ivoire.

62 Politique de confidentialité pour les données personnelles sur Orange Money et les conditions générales d'utilisation (CGU) des services d'épargne et de crédit d'Orange Bank.

	Autorisations demandées	Au démarrage, Orange Money Africa demande de : . gérer les appels des utilisateurs . d'accéder aux SMS d'un utilisateur : Il affiche les SMS d'un utilisateur pour collecter des informations financières et des données de transaction afin de recueillir des informations sur l'historique financier d'un utilisateur et de déterminer sa solvabilité . accéder aux contacts de l'utilisateur . accéder aux données de localisation, d'appareil et d'utilisation : l'application Orange Money utilise la technologie GPS ou d'autres services de localisation pour déterminer l'emplacement actuel d'un utilisateur.
	Informations recueillies auprès de l'utilisateur	Lors de l'inscription, Orange Money Africa recueille les informations de l'utilisateur : nom, adresse, adresse e-mail et numéro de téléphone, numéro de téléphone de l'appareil, carte SIM, âge, nom d'utilisateur, mot de passe, informations financières et de crédit, description de l'ion personnel et photographie, et autres informations d'inscription.
	Informations recueillies à partir de l'appareil de l'utilisateur Les informations recueillies lors de l'utilisation de Orange Côte d'Ivoire website	Orange Money Africa collecte les informations suivantes sur l'appareil de l'utilisateur : Modèle de l'appareil mobile, numéro IMEI de l'appareil ou numéro de série, informations sur la carte SIM, informations sur le réseau mobile, système d'exploitation de l'appareil, type de navigateur, emplacement de l'appareil et réglage du fuseau horaire. Informations stockées dans l'appareil : liste de contacts, journaux d'appels, journaux de SMS, contacts de comptes de médias sociaux, photos, vidéos ou tout autre contenu numérique pertinent. Dès qu'un utilisateur utilise le site internet d'Orange Côte d'Ivoire sur son téléphone mobile, Orange et Moi collecte automatiquement les informations suivantes et les stocke dans ses fichiers Journaux : L'adresse IP de l'utilisateur, le type de navigateur, le fournisseur d'accès Internet (FAI), les pages de renvoi/de sortie, le système d'exploitation, l'horodatage et le support de navigation. Ces informations sont ensuite regroupées à des fins d'analyse ou de marketing et mises à la disposition d'Orange Bank.

	Informations reçues de tiers	Des informations ont été obtenues auprès d'autres entités du groupe Orange : Orange Money Côte d'Ivoire et Orange Côte d'Ivoire, Bureaux d'information sur le crédit (BIC), fournisseurs de réseaux mobiles et agences de recouvrement.
	Utilisation des informations de l'utilisateur par l'application	La politique de confidentialité d'Orange Money Africa affirme qu'elle collecte les données des utilisateurs aux fins suivantes : le traitement des transactions d'un utilisateur vérification de l'identité d'un utilisateur décaissement des prêts et recouvrement des paiements évaluation du crédit et création de modèles de crédit analyse du comportement de l'emprunteur les obligations d'Orange Money App envers les utilisateurs respect des lois, réglementations relatives à la "connaissance du client" et aux règles de lutte contre le blanchiment d'argent prévention des fraudes, services de marketing
	Partage d'informations avec des tiers Durée de l'accès aux données par des tiers	Orange Money partage les informations des utilisateurs avec : Ses membres, agents, prestataires de services, les entités du groupe Orange Money, et les entités qui sous-traitent les données collectées. Toute personne agissant pour le compte d'un utilisateur des institutions financières, des bureaux de crédit et des agences (BIC). Les partenaires commerciaux en cas de transferts d'activités, de cessions, de fusions et d'acquisitions, etc. Les prestataires de services tiers Organismes d'application de la loi (l'Autorité nationale de régulation des télécommunications / TIC de Côte d'Ivoire (ARTCI)4), les représentants du gouvernement, sur la base de : Demande ou décision formelle de justice Respect de la loi ou signalement d'une activité illégale présumée La politique ne contient aucune indication sur la durée pendant laquelle les tiers peuvent accéder aux informations personnelles des utilisateurs et les conserver.
	Technologies de suivi / Cookies du site web	Orange Money Africa utilise une technologie de suivi mobile et des cookies de site Web pour distinguer les utilisateurs de l'application.

	Stockage des informations de l'utilisateur par l'application	Orange Money Africa enregistre les données des utilisateurs en dehors de la Côte d'Ivoire. Les informations sont également traitées par le personnel d'Orange Money Côte d'Ivoire, Orange Bank Africa, et son CECOM à Madagascar qui interviennent en dehors de la Côte d'Ivoire. L'application n'a pas fourni de détails sur la durée de conservation des données par Orange Côte d'Ivoire.

MyMTN CI[63] Lien de téléchargement : Google Play Store et Apple Store	Les informations collectées et traitées par l'application	
	Autorisations demandées	Au démarrage, MyMTN CI demande à : Manage user calls access a user's SMS: It displays a user's SMS to collect financial and transactional information data to collect information about a user's financial history and determine their creditworthiness Access user contacts user Access location, device and usage data: MyMTN CI uses GPS technology or other location services to determine the current location of a user - gérer les appels des utilisateurs - accéder aux SMS d'un utilisateur : Il affiche les SMS d'un utilisateur et permet de collecter les données financières et transactionnelles pour recueillir des informations sur l'historique financier d'un utilisateur et déterminer sa solvabilité accéder aux contacts de l'utilisateur accéder aux données de localisation, d'appareil et d'utilisation : MyMTN CI utilise la technologie GPS ou d'autres services de localisation pour déterminer l'emplacement actuel d'un utilisateur.
	Informations recueillies auprès de l'utilisateur	Lors de l'inscription, MyMTN CI collecte les informations d'un utilisateur : l'identité du client (nom, prénom, sexe, date de naissance), ces coordonnées (adresse postale, adresse email, numéros de téléphone), sa localisation (situation géographique) et le lien entre ces préférences de paiement (chèque, espèces, carte bancaire, mobile money).

63 Politique de confidentialité de l'application MyMTN CI et les conditions générales d'utilisation () pour les comptes MTN Mobile Money Côte d'Ivoire

	Informations recueillies à partir de l'appareil de l'utilisateur Informations recueillies lors de l'utilisation du site web de MTN Côte d'Ivoire	MyMTN CI collecte les informations à partir de l'appareil d'un utilisateur : Technique d'intelligence artificielle (IA) : modèle de l'appareil mobile, numéro IMEI ou numéro de série de l'appareil, informations sur la carte SIM, informations sur le réseau mobile, système d'exploitation de l'appareil, type de navigateur, emplacement de l'appareil et réglage du fuseau horaire. Informations enregistrées dans l'appareil : liste de contacts, journaux d'appels, journaux de SMS, contacts de comptes de médias sociaux, photos, vidéos ou tout contenu numérique pertinent. Dès qu'un utilisateur utilise le site web de MTN Côte d'Ivoire, MyMTN CI collecte automatiquement les informations suivantes et les stocke dans ses fichiers journaux : L'adresse IP de l'utilisateur, le type de navigateur, le fournisseur de services Internet (ISP), les pages de référence / de sortie, le système d'exploitation, l'horodatage et le support de navigation. Ces informations sont combinées à des fins d'analyse ou de marketing.
	Informations reçues des tiers	Informations obtenues auprès d'autres entités du Groupe MTN : MTN Côte d'Ivoire et MTN Mobile Financial Services Côte d'Ivoire, Bureaux d'information de crédit (BIC), fournisseurs de réseaux mobiles et agences de recouvrement.
	Utilisation des informations de l'utilisateur par l'application	La politique de confidentialité de MyMTN CI indique qu'elle collecte les données des utilisateurs aux fins suivantes : . traiter les transactions d'un utilisateur . vérification de l'identité de l'utilisateur 'un utilisateur . décaissements de prêts et notation de l'encaissement des paiements . crédit et création de modèles de crédit . analyse du comportement de l'emprunteur . les responsabilités de l'application Orange Money envers les utilisateurs . respect des lois, et règlementations relatives à la « connaissance du client » et à la lutte contre le blanchiment d'argent . prévention des fraudes, . services de marketing

	Partage d'informations avec des tiers Durée de l'accès des données aux tiers	MyMTN CI partage les informations des utilisateurs avec : . ses membres, agents, prestataires de services, entités du groupe MTN et entités qui sous-traitent les données collectées. . Toute personne agissant au nom d'un utilisateur . les institutions financières, les bureaux et agences de crédit (BIC) . des partenaires commerciaux en cas de transferts d'entreprises, de cessions, de fusions et d'acquisitions, etc. . les prestataires de services tiers . organismes d'application de la loi (l'Autorité nationale de régulation des télécommunications / TIC de Côte d'Ivoire (ARTCI4), représentants du gouvernement, sur la base de : . une demande ou une décision formelle La justice . respect de la loi ou signalement d'une activité illégale présumée La politique ne mentionne pas la durée pendant laquelle les tiers peuvent accéder aux informations personnelles des utilisateurs et les conserver.
	Technologies de suivi / Cookies du site web	MyMTN CI utilise une technologie de suivi mobile et des cookies de site web pour distinguer les utilisateurs de l'application.
	Stockage des informations sur l'utilisateur par l'application	MTN CI enregistre les informations des utilisateurs dans un emplacement hors de la Côte d'Ivoire. Les informations peuvent également être traitées par le personnel de MTN Côte d'Ivoire hors de la Côte d'Ivoire. La politique de confidentialité de MyMTN CI indique que la durée maximale de conservation des données collectées est de dix ans à compter de la fin de la relation contractuelle et peut être prolongée en cas de procédure judiciaire ou administrative.

Étude de cas

Orange Money Africa : La question de la durée de conservation des données des utilisateurs

La politique de confidentialité, les conditions générales d'utilisation (CGU) des comptes Orange Money Côte d'Ivoire et la politique de conformité publique d'Orange Côte d'Ivoire, associées aux applications Orange Money Africa ne donnent aucune précision sur la durée de conservation des données des utilisateurs. Une insuffisance qui constitue une violation de la loi relative à la protection des données en Côte d'Ivoire exige que les données soient collectées pendant une période déterminée.[64]

Analyse des pratiques de la protection des données des applications de prêt numérique au regard de la loi sur la protection des données personnelles

La loi sur la protection des données personnelles en Côte d'Ivoire a clairement défini les

64 Article 16 et 43 de la loi n° 2013-50 du 19 juin 2013.

obligations en matière de protection de la vie privée, applicables à tout traitement, qu'il soit automatique ou non[65]. Ce faisant, les applications numériques font l'objet de prêts. Toutefois, en raison de leur développement récent, les risques qu'elles présentent pour la protection de la vie privée sont réels. Cette section met en évidence les dispositions pertinentes de la loi afin de déterminer si ces applications sont conformes à ces dispositions.

Droit à la vie privée

La loi sur la protection des données exige que les responsables du traitement et les sous-traitants (dans ce cas, les applications de prêt numérique) traitent les données à caractère personnel de sorte que le droit à la vie privée[66] soit respecté. En l'occurrence, la loi demande aux applications de veiller à ce que le droit à la vie privée des emprunteurs soit prioritaire lors du traitement de leurs données. Les applications étudiées violent ce droit et traitent les données de manière intrusive et sans rapport avec l'objectif de la collecte des données. Par exemple, ces applications collectent des informations telles que les contacts enregistrés sur l'appareil d'un emprunteur, les informations de connexion des plateformes de médias sociaux et la localisation précise en temps réel, ce qui est intrusif et excessif pour la collecte de données.

Légalité, équité et transparence

La loi sur la protection des données exige que ces applications traitent les données légalement, équitablement et en toute transparence.[67] Toutes les applications doivent informer les personnes concernées de manière claire et concise sur la façon dont leurs données seront traitées et veiller à ce que tous les paramètres de la loi soient respectés lors de ce traitement.[68]

Dans ce cas, les applications doivent informer les utilisateurs des raisons pour lesquelles leurs données sont collectées, de la manière dont l'entreprise utilisera leurs données et, en cas de partage avec des tiers, des personnes avec lesquelles l'entreprise partagera leurs données et de la durée de conservation de ces dernières. On peut dire que les applications étudiées sont transparentes quant aux raisons pour lesquelles elles collectent les données des utilisateurs et avec qui elles les partagent. Cependant, elles n'indiquent pas pendant combien de temps les tiers auront accès aux données et combien de temps ils les conserveront.

Limitation de l'objectif, pertinence et adéquation

Les applications de prêt numérique sont tenues, en vertu de la loi sur la protection des données, de traiter les données personnelles après leur collecte.[69] Cela signifie que les applications ne doivent collecter que des données concernant le prêt numérique et non des données excessives. Les applications ne doivent collecter que des données pertinentes, adéquates et limitées à la collecte de données.[70]

Les applications étudiées collectent des informations personnelles qui ne sont pas pertinentes pour l'objectif de la collecte de données. Elles collectent des informations sur les emprunteurs telles que des numéros de carte de crédit, des transactions financières, des informations sur les comptes de connexion aux médias sociaux, des contacts sur les médias sociaux, des contacts téléphoniques, des photos et des vidéos, etc. qui ne sont pas pertinentes dans le cadre des prêts numériques.

65 Article 3 de la loi n° 2013-50 du 19 juin 2013
66 Article 3 de la loi n° 2013-50 du 19 juin 2013
67 Articles 14, 15 et 16 de la loi n° 2013-50 du 19 juin 2013.
68 Article 28 de la loi n° 2013-50 du 19 juin 2013
69 Article 14 de la loi n° 2013-50 du 19 juin 2013
70 Articles 16 et 43 de la loi n° 2013-50 du 19 juin 2013

Partage des informations avec des tiers

La loi ivoirienne sur la protection des données stipule que ces applications doivent informer les tiers avec lesquels leurs données seront partagées, y compris les détails adoptés pour protéger leurs données avant leur collecte[71]. Dans le cas spécifique des applications d'Orange Money Africa, l'absence de durée déterminée pour le traitement des données constitue une violation du droit à la vie privée[72].

Les applications examinées partagent les informations relatives aux utilisateurs/emprunteurs avec le bureau d'information sur le crédit (BIC), les partenaires commerciaux, les conseillers professionnels, les organismes gouvernementaux et les organismes chargés de l'application de la loi, etc. et n'indiquent pas les mesures de protection adoptées pour protéger les données des emprunteurs. Les demandes n'indiquent pas non plus pendant combien de temps ces parties auront accès aux données et combien de temps elles les conserveront.

Transfert de données personnelles hors de la Côte d'Ivoire

Disposition appliquée par les différents fournisseurs d'applications

Confidentialité par conception et par défaut

La loi prévoit que le responsable du traitement des données doit prendre toutes les dispositions pour traiter les données des utilisateurs[73].
Les applications disposent de mesures de cryptage pour protéger les communications et le contenu privé de leurs utilisateurs - un niveau de sécurité nécessaire pour protéger les données des utilisateurs. Toutefois, le niveau de protection inclus ne peut empêcher le fournisseur d'applications de collecter des informations excessives.

Droit d'accès et de suppression des données personnelles

Les utilisateurs des applications ont le droit d'accéder à leurs données détenues par ces applications[74] et ont le droit de demander la suppression ou la destruction de leurs données que les applications ne sont plus autorisées à conserver. Les utilisateurs ont également le droit de demander la suppression des données non pertinentes, excessives ou obtenues illégalement[75]. Les fournisseurs d'applications ont mis en place des services dédiés pour recevoir les demandes des utilisateurs à ce sujet.

Portabilité des données

La loi donne aux personnes concernées le droit de recevoir leurs données dans un format structuré et lisible par machine[76]. Elle leur donne également le droit, lorsque cela est techniquement possible, de faire transmettre les données directement à d'autres responsables de traitement ou gestionnaires de traitement des données[77]. Les applications examinées ne permettent pas aux utilisateurs d'exercer ce droit.

L'évaluation d'impact sur la protection des données

La loi exige qu'un rapport sur le processus de traitement des données soit produit annuellement et envoyé à l'ARTCI. En outre, les autorisations de transfert de données ont indiqué la nécessité pour les contrôleurs de données d'effectuer une évaluation de l'impact sur la protection des données (DPIA). Cependant, aucun des responsables du traitement des données des deux applications n'a produit ou mis à disposition ses rapports.

71 Article 16 et 43 de la loi n° 2013-50 du 19 juin 2013
72 Article 49 de la loi n° 2013-50 du 19 juin 2013
73 Articles 39, 40, 41 et 44 de la loi n° 2013-50 du 19 juin 2013.
74 Article 49 de la loi n° 2013-50 du 19 juin 2013
75 Article 30, 31, 3, 33, 34, 35 et 36 de la loi n° 2013-50 du 19 juin 2013.
76 Article 49 de la loi n° 2013-50 du 19 juin 2013
77 Articles 30, 31, 3, 33, 34, 35 et 36 de la loi n° 2013-50 du 19 juin 2013.

Les pratiques de traitement des données des applications de crédit numérique en Côte d'Ivoire ne respectent pas la loi sur la protection de la vie privée. Des études portant sur l'impact de la protection des données (DPIA) doivent être menées par les responsables du traitement de ces applications numériques pour forcer le strict respect des obligations légales en la matière. Par ailleurs, une révision de la loi n° 2013-50 du 19 juin 2013 relative à la protection des données personnelles doit être envisagée, en tenant compte des risques potentiels pour la vie privée. Au-delà, il est également nécessaire que l'ARTCI se dote d'une expertise et d'équipements techniques pour contrôler en temps réel le volume, la qualité et la quantité de données collectées par ces gestionnaires de données pour le traitement des applications mobiles.

Égypte

Profil du pays

Située au nord-est de l'Afrique, l'Égypte, ou République arabe d'Égypte, comptait plus de 106 millions d'habitants en 2021. Elle est située sur la côte sud de la Méditerranée orientale, bordée par Israël, la Libye, le Soudan et fait partie du groupe de pays du Moyen-Orient et de l'Afrique du Nord (MENA). Son PIB est le deuxième plus important d'Afrique et était d'environ 362 milliards de dollars en 2019/20. Elle pratique un régime semi-présidentiel.

Protection des données en Égypte

La protection de la vie privée est régie par la loi n° 151 du 15 juillet 2020 relative à la protection des données personnelles. Cette loi s'applique à tout traitement, automatique ou non, effectué sur le territoire ou en dehors de l'Égypte[78]. Le Centre de protection des données ("CPD") est une APD égyptienne. Il a été créé par la loi n° 151 du 15 juillet 2020 et a commencé ses activités en avril 2021. Il est habilité à superviser et à faire appliquer la loi sur la protection des données, y compris, entre autres, à délivrer les licences, autorisations et certifications requises en vertu de la loi sur la protection des données[79] .

Introduction

En 2020, le continent africain comptait 562 millions de comptes Mobile Money, soit 45% des comptes Mobile Money ouverts dans le monde, c'est-à-dire 1,2 milliard. La plupart de ces comptes se répartissent entre l'Afrique de l'Est (293 millions) et l'Afrique de l'Ouest (198 millions), et ils sont utilisés au minimum pour des opérations de paiement de différentes natures. On note également une augmentation plus significative du nombre de comptes en valeur absolue au cours des cinq dernières années en Afrique du Nord, en raison des efforts nouveaux et renouvelés dans le secteur de cette région. En effet, en Afrique du Nord, 14 millions de comptes de mobile money ont été enregistrés en 2020 pour 248 millions de transactions, soit l'équivalent de plus de 3 milliards de dollars US ($), une augmentation de 24% par rapport à 2019. L'un des pays leaders dans cette dynamique en cours est l'Égypte, où quatre services de mobile money sont proposés aux populations depuis avril 2013. Ces services concernent (i) les paiements mobiles (paiement de factures, paiements

78 Article 1 et 2 de la loi n° 151 du 15 juillet 2020
79 Article 19 de la loi n° 151 du 15 juillet 2020

groupés et paiements marchands), les transferts (transferts nationaux et internationaux), les décaissements de salaires (Versement des salaires d'une structure à son personnel) et les services bancaires (dépôt, retrait d'argent, compte d'épargne, crédit numérique...). Grâce à ses services, l'Égypte comptait environ 4,5 millions de transactions électroniques par mois, effectuées par 13,5 millions de portefeuilles électroniques (e-wallets) mobiles actifs sur son territoire, selon les dernières statistiques de l'Autorité nationale de régulation des télécommunications (NTRA), publiées en juin 2020. Les principaux opérateurs de téléphonie mobile sont également des fournisseurs de services de porte-monnaie électronique, fintech. Vodafone Egypt reste ainsi le leader sur ce segment, représentant 62,7 % du total des portefeuilles électroniques et 86,5 % des transactions par portefeuille électronique, suivi par Orange Egypt (25 % des portefeuilles électroniques et 8,5 % des transactions), Etisalat Misr (12 % des portefeuilles électroniques et 4,5 % des transactions) et We (0,3 % et 0,5 %). Les services les plus utilisés par les utilisateurs sont les dépôts et retraits d'argent (35% du total des transactions par portefeuille électronique), les transferts d'argent (33%) et la recharge de mobiles prépayés (26%).

Pour ce qui est du crédit numérique, il a été introduit pour la première fois en Égypte par la Start-up Kayshat[80] en février 2020 avec l'accord de l'Autorité de régulation financière d'Égypte. Cette application permet aux personnes d'obtenir des prêts entre 100 et 1 500 livres égyptiennes (EGP). Un boom pour un pays où près de 70% de la population est sans accès bancaire et surtout représente un marché pour les acteurs du secteur bancaire et financier. En effet, conscients de l'intérêt potentiel de ce type de service, plusieurs offres (Shahry [81], MNT Halan[82] et MoneyFellows[83]) vont se développer. La multitude de ces offres, au-delà de l'avantage pour l'inclusion financière et l'amélioration des conditions de vie des populations, pose des défis en termes de protection des données personnelles en Égypte. Dès lors, les pratiques de traitement des données de ces applications, telles que définies dans leurs politiques et conditions d'utilisation, prennent-elles en compte la réglementation sur la protection de la vie privée ?

Cette étude vise à analyser les politiques de confidentialité et les termes et conditions de ces applications et à examiner leur conformité avec la loi sur la protection des données en Egypte. La première partie comprend un aperçu des données collectées par ces applications, et la deuxième partie examine leurs activités de traitement dans le cadre de la loi sur la protection des données personnelles. La dernière partie se termine en indiquant si ces applications respectent ou non la loi sur la protection des données personnelles.

Aperçu des données collectées par les applications de prêt numérique

80 Kashat est la première application mobile de prêt Nano en Égypte, offrant des prêts à court terme allant de 100 EGP à 1500 EGP avec un plan de remboursement allant jusqu'à 61 jours.

81 Shahry permet aux Égyptiens d'obtenir des crédits instantanés et des crédits à la consommation pour acheter des biens et des services dans le pays.

82 Halan est une application multiservice qui permet aux Égyptiens, au-delà des services de livraison et d'achat de biens, d'obtenir des crédits instantanés. Une offre de crédit numérique qui résulte d'une collaboration entre la société néerlandaise MNT Investments BV et la société de capital-risque Tasaheel. Elle permet notamment aux commerçants d'obtenir des fonds à partir de 3 000 EGP et jusqu'à 200 000 EGP en quelques clics. Il a été lancé le 24 juin 2021.

83 MoneyFellows offre une large gamme d'options de cercle d'argent que chaque utilisateur peut choisir. En fonction du comportement de paiement, l'utilisateur peut obtenir des crédits instantanés. Les frais commencent à partir de 8% et diminuent progressivement en fonction de la niche sélectionnée, jusqu'à atteindre zéro. La sélection des niches de prêt et du montant accordé aux utilisateurs se fait par l'évaluation du crédit de l'utilisateur effectuée par les équipes de MoneyFellows.

Kashat[84] Lien de téléchargement : Google Play Store et HUAWEI AppGallery	Les informations collectées et traitées par l'application	
	Autorisations demandées	Au démarrage, l'application Kashat demande de : . gérer les appels et accéder aux contacts des utilisateurs, trouver des comptes sur l'appareil, lire vos contacts, lire les journaux d'appels, appeler directement des numéros de téléphone et lire le statut et l'identité du téléphone. . d'accéder aux SMS d'un utilisateur : Elle affiche les SMS et ou MMS d'un utilisateur pour recueillir des informations financières et transactionnelles fournies afin de collecter des informations sur l'historique financier d'un utilisateur et de déterminer sa solvabilité. . accéder aux données stockées dans le mobile d'un utilisateur, modifier, lire ou supprimer le contenu de votre stockage USB. . données sur la localisation, l'appareil et l'utilisation de l'utilisateur : Kashat App utilise la technologie GPS et d'autres services de localisation pour déterminer l'emplacement actuel. . afficher les connexions Wi-Fi . accéder au calendrier de lecture des événements de l'agenda ainsi qu'aux informations confidentielles, ajouter ou modifier des événements de l'agenda et envoyer des e-mails aux invités à l'insu des propriétaires. . effectuer diverses actions : se lier à un service d'accessibilité, recevoir des données Internet tirer sur d'autres applications, lire la configuration du service Google, afficher les connexions réseau, s'exécuter au démarrage, accéder à l'ensemble du réseau et empêcher l'appareil de dormir.
	Informations recueillies auprès de l'utilisateur	Lors de l'inscription au service de prêt, Kashat recueille les informations sur l'utilisateur : nom, adresse, téléphone, adresse électronique, carte d'identité nationale, photo de vous, nom d'utilisateur et mot de passe et d'autres informations d'inscription : statut et domaine professionnels, état civil, informations financières et de crédit.

84 Politique de confidentialité de l'application Kashat

	Informations recueillies sur l'appareil de l'utilisateur Informations collectées lors de l'utilisation du site web Kashat	L'application Kashat recueille les informations suivantes à partir de l'appareil d'un utilisateur : le modèle de l'appareil mobile, les identifiants uniques (IMEI ou numéro de série), le système d'exploitation de l'appareil et l'emplacement de l'appareil ainsi que le fuseau horaire Informations sur le réseau mobile Les données enregistrées sur vos appareils, telles que la liste de contacts, les journaux d'appels, l'historique des SMS et la galerie photos Les informations sur la localisation actuelle fournies par la technologie GPS et d'autres services de localisation Lorsqu'un utilisateur utilise le site web de l'application Kashat sur son téléphone mobile, celui-ci collecte automatiquement les informations et les enregistre dans ses fichiers journaux. Ces données peuvent inclure des informations telles que l'adresse IP de l'utilisateur mobile, le fournisseur d'accès à Internet (FAI), le nom de l'appareil, la version du système d'exploitation, le type de navigateur, le parcours de navigation, ainsi que l'heure et la date de votre utilisation du service. C'est-à-dire des données statistiques sur les actions et les habitudes de navigation des utilisateurs, sans permettre de les identifier formellement. Lorsqu'elles sont utilisées avec d'autres informations collectées, ces informations permettent d'améliorer l'analyse et la sécurité des utilisateurs.
	Informations reçues de tiers	Informations obtenues auprès d'autres entités du groupe Kashat (filiales), des bureaux d'information du crédit (BIC), des fournisseurs de réseaux mobiles, des agences de recouvrement, des partenaires commerciaux, etc.

	Utilisation des informations de l'utilisateur par l'application	La politique de confidentialité de l'application Kashat précise qu'elle collecte les données des utilisateurs aux fins suivantes : . Vérification de l'identité d'un utilisateur . Traitement des transactions des utilisateurs . Evaluation du crédit et création de modèles de crédit . Analyse du comportement de l'emprunteur . Décaissement des prêts et obligations de recouvrement des paiements Kashat aux utilisateurs . Respect des réglementations applicables en matière de KYC (Know Your Customer), la lutte contre le blanchiment d'argent et la lutte contre le financement du terrorisme . Communications promotionnelles et services de marketing
	Informations partagées avec des tiers Durée de l'accès des données aux tiers	Kashat partage les informations des utilisateurs avec : . Ses filiales, sa société mère et d'autres filiales de leur société mère (" son groupe "). . Toute personne agissant au nom d'un utilisateur . Des fournisseurs de portefeuilles mobiles, des compagnies d'assurance, des agences d'évaluation du crédit ou d'autres institutions financières. . Des autorités chargées de l'application de la loi des agences gouvernementales internationales pour aider à la détection, à la prévention et à l'investigation d'activités criminelles ou de fraudes. . De partenaires commerciaux dans le cadre de transferts, cessions, fusions et acquisitions d'entreprises, etc. . Prestataires de services tiers La politique ne mentionne pas la durée pendant laquelle les tiers peuvent accéder aux informations personnelles des utilisateurs et les conserver.
	Technologies de suivi / Cookies du site web	Le service de prêt Kashat n'utilise pas explicitement ces "cookies". Toutefois, pour offrir une meilleure expérience utilisateur, Kashat fait appel à des prestataires de services tiers, tels que des fournisseurs d'analyses ou des agences de marketing, qui peuvent choisir d'utiliser des cookies ou d'autres technologies de suivi mobile pour vous distinguer des autres utilisateurs de l'application ou du site Web.

	Stockage des informations de l'utilisateur par l'application	Les données de Kashat sont enregistrés sur des serveurs en Égypte, mais elles peuvent être transférées et sauvegardées vers une autre destination en dehors de l'Égypte. Elles peuvent également être traitées par du personnel situé hors d'Égypte et travaillant pour Kashat ou ses fournisseurs. Ces membres du personnel peuvent être engagés dans l'exécution des demandes des utilisateurs. Vous acceptez ce transfert, ce traitement ou ce stockage de données en soumettant vos informations. Kashat affirme qu'elle prend toutes les mesures raisonnables nécessaires pour garantir que les données des utilisateurs sont traitées en toute sécurité et conformément à sa politique de confidentialité.

Shahry[85] Lien de téléchargement : Google Play Store et Apple Store	Les informations collectées et traitées par l'application	
	Autorisations demandées	Au démmarage, l'application Shahry demande à: . Gérer les appels et accéder aux contacts des utilisateurs, trouver des comptes sur l'appareil, lire vos contacts, appeler des numéros de téléphone et lire le statut et l'identité du téléphone. . Accéder aux données de localisation, d'appareil et de l'utilisateur : l'application Kashat utilise la technologie GPS d'autres services de localisation pour déterminer l'emplacement actuel d'un utilisateur. . Afficher les connexions Wi-Fi . Accéder aux données stockées dans le mobile de l'utilisateur, modifier, lire ou supprimer le contenu de votre stockage USB. . Effectuer diverses actions : recevoir des données d'Internet, afficher les connexions réseau, s'associer à des appareils Bluetooth, accéder à l'ensemble du réseau, empêcher les appareils d'être en veille et modifier les paramètres du système.
	Informations recueillies auprès de l'utilisateur	Lors de la souscription au service de prêt, Shahry collecte les informations de l'utilisateur : nom, date de naissance, numéro d'identification national, adresse, profession, données personnelles scolaires et financières passées et présentes.

85 Privacy Policy of Shahry

	Informations recueillies sur l'appareil de l'utilisateur Informations recueillies sur le site web	Shahry recueille les informations suivantes à partir de l'appareil d'un utilisateur : . le modèle de l'appareil, les identifiants uniques de l'appareil (IMEI ou numéro de série), le système d'exploitation de l'appareil, la localisation de l'appareil et le fuseau horaire, et l'adresse IP. . le réseau mobile . les informations enregistrées sur votre appareil, telles que la liste de contacts, l'historique d'appels, l'historique de SMS et la galerie de médias. . les informations sur la localisation actuelle fournies par la technologie GPS et d'autres services de localisation. Lorsqu'un utilisateur utilise le site web de Shahry sur son téléphone mobile, l'application Shahry recueille automatiquement les informations suivantes et les enregistre dans ses fichiers journaux. Les données de journal peuvent inclure des informations telles que l'adresse de protocole Internet ("IP") de l'utilisateur mobile.
	Informations reçues de tiers	Informations obtenues auprès d'autres entités du Groupe Shahry (filiales), les bureaux d'information de crédit (BIC), fournisseurs de réseaux mobiles, agences de recouvrement, partenaires commerciaux, etc.
	Utilisation des informations de l'utilisateur par l'application	La politique de confidentialité de Shahry précise qu'elle collecte les données des utilisateurs aux fins suivantes : . Vérifier l'identité d'un utilisateur . traiter les transactions d'un utilisateur . crédit et création de modèles de crédit-prêt . décaissements et recouvrement de paiements . Responsabilités de Shahry envers les utilisateurs . Respect des réglementations applicables en matière de KYC (Know Your Customer), la lutte contre le blanchiment d'argent et la lutte contre le financement du terrorisme. . Communications promotionnelles et services de marketing

	Informations partagées avec des tiers Durée de l'accès des données aux tiers	Shahry partage les informations relatives aux utilisateurs avec : . Ses filiales, sa société mère et d'autres filiales de notre société mère (" son groupe "). . Toute personne agissant au nom d'un utilisateur . Des fournisseurs de portefeuilles mobiles, des compagnies d'assurance, des bureaux de crédit ou d'autres institutions financières. . Des autorités chargées de l'application de la loi, des organismes internationaux ou gouvernementaux pour aider à la détection, à la prévention et à l'investigation d'activités criminelles ou de fraudes. . De partenaires commerciaux dans le cadre de transferts, cessions, fusions et acquisitions d'entreprises, etc. . Prestataires de services tiers La politique ne mentionne pas la durée pendant laquelle les tiers peuvent accéder aux informations personnelles des utilisateurs et les conserver.
	Technologies de suivi / Cookies du site web	La politique de confidentialité de Shahry ne donne aucune précision sur l'utilisation des cookies. Le site web associé à l'application n'offre aucune possibilité de choisir les préférences en matière de cookies.
	Stockage des informations de l'utilisateur par l'application	Les données d'identification personnelles des utilisateurs de Shahry sont enregistrées, cryptées et sauvegardés sur ses serveurs en Egypte et ne sont pas accessibles aux entités ou personnes non autorisées. Ces informations ne sont pas divulguées à des fins de location ou à d'autres fins commerciales (publicité).

Halan[86] Lien de téléchargement : Google Play Store et HUAWEI AppGallery	Les informations collectées et traitées par l'application

86 Politique de confidentialité de Halan

	Autorisations demandées	Au démarrage, Halan demande à : . Gérer les appels et accéder directement aux numéros de téléphone des appels. . Accéder aux données enregistrées dans le mobile de l'utilisateur, modifier, lire ou supprimer le contenu de votre stockage USB ; accéder à la localisation, au dispositif et aux données d'utilisation de l'utilisateur : l'application Halan utilise la technologie GPS et d'autres services de localisation pour déterminer le site actuel. . visualiser les connexions Wi-Fi . Effectuez diverses actions : recevoir des données Internet, accès complet au réseau, empêcher l'appareil de se mettre en veille, lire la configuration du service Google, afficher les connexions réseau.
	Informations recueillies auprès de l'utilisateur	Lors de la souscription au service de prêt, Halan recueille les informations de l'utilisateur : nom, adresse électronique, numéro de téléphone portable, adresse postale, photo de profil, mode de paiement, actualités financières et carte de crédit.
	Informations collectées à partir de l'appareil de l'utilisateur Informations recueillies sur le site web WhileHalan	Halan recueille les informations suivantes à partir de l'appareil d'un utilisateur : informations sur appareil, y compris le type d'appareil, les identifiants uniques de l'appareil (IMEI ou numéro de série), le système d'exploitation de l'appareil ainsi que l'emplacement et le fuseau horaire de l'appareil Réseau mobile Informations enregistrées sur l'appareil, telles que la liste de contacts, l'historique des appels, l'historique des SMS, la galerie multimédia, les données SMS et les données de transaction Les informations de localisation actuelles fournies par la technologie GPS et d'autres services de localisation. Lorsqu'un utilisateur visite le site web Halan, l'application Halan recueille automatiquement les informations de l'utilisateur et les enregistre dans ses fichiers journaux. Les données de journal peuvent inclure des informations telles que l'adresse de protocole Internet ("IP") de l'utilisateur mobile, le fournisseur d'accès Internet (FAI), le nom de l'appareil, la version du système d'exploitation, le type de navigateur, les données de parcours, ainsi que l'heure et la date de votre utilisation du service. C'est-à-dire des données statistiques sur les actions et les habitudes de navigation des utilisateurs, et ne permettant pas de les identifier formellement. Utilisées avec d'autres informations recueillies, ces informations permettent une meilleure analyse et une meilleure sécurité pour les utilisateurs.

	Informations reçues de tiers	Informations obtenues auprès d'autres entités du groupe Halan (filiales), des bureaux d'information du crédit (BIC), de fournisseurs de réseaux mobiles, d'agences de recouvrement, de partenaires commerciaux, etc.
	Utilisation des informations de l'utilisateur par l'application	La politique de confidentialité de Halan indique qu'elle collecte les données des utilisateurs aux fins suivantes : . Vérification de l'identité d'un utilisateur . Traitement des transactions des utilisateurs . Evaluation du crédit et création de modèles de crédit . Analyse du comportement de l'emprunteur . Décaissement des prêts et recouvrement des paiements . Les responsabilités d'Halan envers les utilisateurs . Respect des réglementations applicables en matière de KYC (Know Your Customer), la lutte contre le blachiment d'argent et la lutte contre le financement du terrorisme. . Communications promotionnelles et services de marketing
	Informations partagées avec des tiers Durée de l'accès des données aux tiers	Halan partage les informations relatives aux utilisateurs avec : . Ses filiales, sa société mère et d'autres filiales de notre société mère ("son groupe"). . Toute personne agissant au nom d'un utilisateur . Des fournisseurs de portefeuilles mobiles, des compagnies d'assurance, des bureaux de crédit ou d'autres institutions financières. . Des autorités chargées de l'application de la loi, des organismes internationaux ou gouvernementaux pour aider à la détection, à la prévention et à l'investigation d'activités criminelles ou de fraudes. . De partenaires commerciaux dans le cadre de transferts, cessions, fusions et acquisitions d'entreprises, etc. . Prestataires de services tiers La politique ne mentionne pas la durée pendant laquelle les tiers peuvent accéder aux informations personnelles des utilisateurs et les conserver.
	Technologies de suivi/cookies du site web	Le site web Halan's utilise des cookies pour se distinguer des autres. Ils permettent d'offrir une excellente expérience à l'utilisateur lorsqu'il navigue sur son site et permettent également d'améliorer et de développer les services proposés. Ces cookies peuvent être acceptés ou refusés par les utilisateurs.

	Stockage des informations de l'utilisateur par l'application	Les données de Halan sont stockées sur des serveurs en Égypte, mais elles peuvent être transférées et enregistrées vers une destination hors d'Égypte. Elles peuvent également être traitées par du personnel situé hors d'Égypte et travaillant pour Halan ou l'un de ses fournisseurs. Ces membres du personnel peuvent être engagés dans l'exécution des demandes des utilisateurs. Vous acceptez ce transfert, ce stockage ou ce traitement des données en soumettant vos données. Halan déclare qu'elle prend toutes les mesures raisonnables nécessaires pour garantir que les données des utilisateurs sont traitées en toute sécurité et conformément à sa politique de confidentialité.

MoneyFellows Circuits financiers fiables et pratiques[87] Lien de téléchargement : Google Play Store et Apple Store	Les informations collectées et traitées par l'application	
	Autorisations demandées	Au démarrage, MoneyFellowsHandle demande à : . accéder aux appels et aux contacts des utilisateurs, trouver des comptes sur l'appareil, lire vos contacts, appeler directement des numéros de téléphone et lire le statut et l'identité du téléphone. . accéder aux SMS d'un utilisateur : Il affiche les SMS et ou MMS d'un utilisateur pour recueillir des informations financières et les transactions pour collecter les informations sur l'historique financier d'un utilisateur et de déterminer sa solvabilité. . accéder aux données enregistrées dans le téléphone portable de l'utilisateur, modifier, lire ou supprimer le contenu de votre clé USB. . accéder à la localisation de l'utilisateur, à son appareil et à ses données d'utilisation : l'application MoneyFellows utilise la technologie GPS et d'autres services de localisation pour déterminer l'emplacement actuel. . effectuer diverses autres actions : recevoir des données d'Internet, s'associer à des appareils Bluetooth, s'exécuter au démarrage, afficher les connexions réseau, accéder à l'ensemble du réseau, contrôler les vibrations, utiliser les comptes de l'appareil, empêcher l'appareil de se mettre en veille.
	Informations recueillies auprès de l'utilisateur	Lors de la souscription au service de prêt, l'application MoneyFellows collecte les informations de l'utilisateur : nom, adresse, téléphone, adresse e-mail, carte d'identité nationale, photo, nom d'utilisateur, mot de passe et d'autres informations d'inscription : statut et domaine professionnels, état civil, informations financières et de crédit.

87 Politique de confidentialité de MoneyFellows

	Informations collectées à partir de l'appareil de l'utilisateur	MoneyFellows collecte les informations suivantes à partir de l'appareil d'un utilisateur : . Les données d'identité comprennent le prénom, le nom de jeune fille, le nom de famille, le nom d'utilisateur ou un identifiant similaire, l'état civil, le titre, la date de naissance et le sexe. . Les données de contact comprennent l'adresse de facturation, l'adresse de livraison, l'adresse électronique et les numéros de téléphone. . Les données financières comprennent les détails des comptes bancaires et des cartes de paiement.
	Informations collectées lors de l'utilisation du site web Money Fellows	. Les données de transaction comprennent les détails sur les paiements à destination et provenant de l'utilisateur et d'autres informations sur les produits et services qu'il a achetés chez nous. . Les données techniques comprennent l'adresse de protocole Internet (IP), les données de connexion, le type et la version du navigateur, le réglage du fuseau horaire et la localisation, les types et versions de plug-in du navigateur, le système d'exploitation et la plate-forme et d'autres technologies sur les appareils utilisés pour accéder à ce site web. Les données de profil comprennent votre nom d'utilisateur et votre mot de passe ainsi que vos activités sur le site web, vos intérêts, vos préférences, vos commentaires et vos réponses aux enquêtes. Les données d'utilisation comprennent des informations sur la façon dont vous utilisez notre site web, nos produits et nos services. Les données de marketing et de communication comportent vos préférences pour recevoir des informations marketing de la part de nos tiers et de nous-mêmes, ainsi que vos préférences en matière de communication. Lorsque les utilisateurs utilisent le site web de MoneyFellows, etc., les données techniques de navigation du terminal de l'utilisateur sont automatiquement collectées. Ces données sont collectées à l'aide de cookies et d'autres technologies similaires. D'autres données techniques sur les

	Informations reçues de tiers	Les données personnelles sont également reçues de différentes sources tierces [et publiques] comme indiqué ci-dessous. Données techniques des sources suivantes : fournisseurs d'analyses, réseaux publicitaires et fournisseurs d'informations de recherche. Contact, données financières et de transaction des fournisseurs de services techniques, de paiement et de livraison.
	Utilisation des informations de l'utilisateur par l'application	La politique de confidentialité de MoneyFellows indique qu'elle collecte les données des utilisateurs aux fins suivantes : . Vérification de l'identité d'un utilisateur . Traitement des transactions des utilisateurs . Evaluation du crédit et création de modèles de crédit . Analyse du comportement de l'emprunteur . Décaissement des prêts et recouvrement des paiements . Responsabilités de MoneyFellows envers les utilisateurs . Respect des réglementations applicables en matière de KYC "Know Your Customer", lutte contre le blanchiment d'argent (AML) et lutte contre le financement du terrorisme (CFT). . Communications promotionnelles et services de marketing
	Informations partagées avec des tiers Durée de l'accès des données aux tiers	MoneyFellows partage les informations des utilisateurs avec : . Ses filiales, sa société mère et d'autres filiales de notre société mère (« son groupe »). . Toute personne agissant au nom d'un utilisateur . Les fournisseurs de portefeuilles mobiles, les assurances, les bureaux d'information sur le crédit ou d'autres institutions financières . Les autorités chargées de l'application de la loi, les agences internationales ou gouvernementales qui aident à détecter, prévenir et enquêter sur les activités criminelles ou la fraude. . Les partenaires commerciaux et fournisseurs de services tiers La politique ne mentionne pas la durée pendant laquelle les tiers peuvent accéder aux informations personnelles des utilisateurs et les conserver

	Technologies de suivi / Cookies du site web	Le service de prêt des MoneyFellows utilise des « cookies » pour améliorer l'expérience des utilisateurs. MoneyFellows fait appel à des prestataires de services tiers, tels que des fournisseurs d'analyses ou des agences de marketing, qui peuvent choisir d'utiliser des cookies ou d'autres technologies de suivi mobile pour vous distinguer des autres utilisateurs de l'application ou du site Web.
	Stockage des informations sur l'utilisateur par l'application	Les données personnelles de Money Fellows sont enregistrées sur des serveurs en Egypte, mais elles peuvent être transférées et sauvegardées vers une destination hors de l'Egypte. Elles peuvent également être traitées par du personnel situé hors d'Égypte et travaillant pour MoneyFellows ou l'un de ses fournisseurs. Ces membres du personnel peuvent être engagés dans le traitement des demandes des utilisateurs. Vous acceptez ce transfert, ce stockage ou ce traitement des données en soumettant vos données. MoneyFellows souligne qu'elle prend toutes les mesures appropriées pour s'assurer que les données des utilisateurs sont traitées en toute sécurité et conformément à sa politique de confidentialité. Les informations essentielles des utilisateurs (y compris les coordonnées, l'identité, les données financières et commerciales) sont conservées pendant cinq (5) ans après qu'ils ont cessé d'être des clients à des fins fiscales.

Étude de cas : L'application Halan et la question du traitement des données des applications multiservices.

Avec son slogan "Une application pour tous vos besoins", Halan regroupe cinq services : E-Commerce & BNPL, Bill Micro Finance, Paiements, Livraison, Epicerie, Portefeuille & Carte. En plus de leurs sous-composantes, les services prennent en charge une grande masse de données collectées auprès des utilisateurs dans le monde entier, sans nécessairement tenir compte du service recherché par l'utilisateur. Ainsi, la politique de confidentialité de Halan ne fait pas de différence entre les données collectées par un utilisateur qui cherche un prêt et un autre qui attend la livraison de ses courses. Une situation qui nécessite que le Centre de protection des données (« CPD ») en Égypte dispose d'un outil en temps réel pour contrôler le traitement des données collectées par Halan Apps.

Analyse des pratiques de protection des données des applications de prêt numérique au regard de la loi sur la protection des données personnelles

La loi égyptienne sur la protection des données personnelles a clairement défini les obligations légales en matière de protection de la vie privée applicables à tout traitement, automatique ou non[88]. Ainsi, les demandes de prêts numériques y sont soumises. Cependant, l'analyse du système de traitement des données de ce dernier montre que les dispositions relatives à la protection de la vie privée ne sont pas strictement respectées. La présente section met en évidence les dispositions pertinentes de la loi afin d'établir si ces applications sont conformes à ces dispositions.

88 Article 1 et 2, chapitre I de la loi n° 151 du 15 juillet 2020.

Droit à la vie privée

La loi sur la protection des données exige que les responsables du traitement et les gestionnaires des données (dans ce cas, les applications de prêt numérique) traitent les données personnelles de manière à respecter le droit à la vie privée de la personne concernée[89]. Les applications étudiées violent ce droit et traitent des données de manière intrusive et sans rapport avec l'objectif de la collecte de données. Par exemple, ces applications collectent des informations telles que les contacts enregistrés sur l'appareil d'un emprunteur, les informations de connexion des plateformes de médias sociaux et la localisation précise en temps réel, ce qui constitue une collecte de données intrusive et excessive.

Légalité, équité et transparence

La loi sur la protection des données exige que ces applications traitent les données de manière légitime et légale[90]. Les applications doivent s'assurer que les personnes concernées sont informées au moyen d'informations claires et concises de la manière dont leurs données sont traitées et que tous les paramètres de la loi sont respectés dans cet exercice[91].

Les applications doivent alors informer les utilisateurs des raisons pour lesquelles leurs données sont collectées, de la manière dont elles seront utilisées et, si elles sont partagées avec des tiers, des personnes avec lesquelles elles seront partagées et de la durée de conservation des données. Les applications étudiées peuvent être transparentes quant aux raisons pour lesquelles elles collectent les données des utilisateurs et avec qui elles les partagent. Cependant, elles n'indiquent pas combien de temps les tiers ont accès aux données et combien de temps elles les conservent [92].

Restriction de l'objectif, pertinence et adéquation

Les applications de prêt numérique sont tenues, en vertu de la loi sur la protection des données, de traiter les données personnelles après leur collecte[93]. Cela signifie qu'elles ne doivent collecter des données que dans les limites du prêt numérique et non des données excessives. Les applications sont également tenues de ne collecter que des données pertinentes, adéquates et limitées à ce qui est nécessaire pour la collecte des données[94]. Les applications examinées collectent des informations personnelles non pertinentes et contraires à l'objectif de la collecte de données. Elles collectent des informations sur les emprunteurs, telles que leurs associations professionnelles, leurs numéros de carte de crédit, leurs accès aux comptes des réseaux sociaux, leurs contacts sur les médias sociaux, leurs contacts téléphoniques, leurs photos et leurs vidéos, qui ne sont pas pertinentes dans le cadre du prêt numérique.

Partage des informations avec des tiers

La loi sur la protection des données stipule que les entreprises doivent informer les utilisateurs des tiers avec lesquels leurs données seront partagées, y compris des détails adoptés pour protéger leurs données avant de les collecter.[95]

Les applications examinées partagent les informations relatives aux utilisateurs/emprunteurs avec plusieurs tiers (partenaires commerciaux, conseillers professionnels, organismes gouvernementaux et organismes chargés de l'application de la loi) et n'indiquent pas les mesures de protection adoptées pour protéger les données des emprunteurs. Les

89 Article 1 chapitre I de la loi n° 151 du 15 juillet 2020
90 Article 6 du chapitre II de la loi n° 151 du 15 juillet 2020.
91 Article 2 et 3 du chapitre II de la loi n° 151 du 15 juillet 2020.
92 Article 5 du chapitre II de la loi n° 151 du 15 juillet 2020.
93 Article 5 du chapitre II de la loi n° 151 du 15 juillet 2020
94 Article 5 et 6 du chapitre II de la loi n° 151 du 15 juillet 2020
95 Article 4,5 et 6 du chapitre II de la loi n° 151 du 15 juillet 2020

applications n'indiquent pas non plus pendant combien de temps ces parties auront accès aux données et combien de temps elles les conserveront.

Confidentialité par conception et par défaut

La loi prévoit que le responsable du traitement doit prendre toutes les dispositions pour traiter les données des utilisateurs [96]. Les applications disposent de mesures de cryptage pour protéger les communications et les contenus privés de leurs utilisateurs. Un niveau de sécurité est nécessaire pour protéger les données des utilisateurs. Toutefois, le niveau de protection inclus ne peut empêcher le fournisseur d'applications de collecter des informations excessives.

Droit d'accès et de suppression des données personnelles

Les utilisateurs des applications[97] d'emprunt ont le droit d'accéder à leurs données détenues par ces applications et de demander la suppression ou la destruction de leurs données que les applications ne sont plus autorisées à conserver, ou qui sont non pertinentes, excessives ou obtenues illégalement[98]. Les fournisseurs d'applications ont mis en place des services dédiés pour recevoir les demandes des utilisateurs à ce sujet.

Mobilité des données

La loi donne aux personnes concernées le droit de recevoir leurs données dans un format structuré et lisible par machine[99]. Elle leur donne également le droit, lorsque c'est techniquement possible, de faire transmettre les données directement à d'autres responsables du traitement des données ou à des gestionnaires du traitement des données[100]. Les applications étudiées ont intégré ces dispositions pertinentes dans leur politique de confidentialité, mais rien ne garantit que les utilisateurs puissent récupérer toutes les données collectées à leur sujet

96 Article 4, et 6 du chapitre II de la loi n° 151 du 15 juillet 2020.
97 Article 2 et 5 du chapitre II de la loi n° 151 du 15 juillet 2020
98 Article 6 du chapitre II de la loi n° 151 du 15 juillet 2020
99 Article 2 du chapitre II de la loi n° 151 du 15 juillet 2020
100 Article 2 et 6 du chapitre II de la loi n° 151 du 15 juillet 2020

Eswatini

Profil du pays

Situé en Afrique australe, Eswatini ou Swaziland (forme longue : Royaume du Swaziland) comptait 1 104 479 habitants en 2020. Il partage une frontière avec l'Afrique du Sud et le Mozambique et n'a pas d'accès à la mer. Son PIB est estimé à 4,472 milliards USD (2019) et pratique une monarchie absolue [101].

101 Les pouvoirs exécutif, législatif et judiciaire sont concentrés entre les mains du roi (le Ngwenyama) qui est assisté d'un conseil des ministres et d'un parlement (avec deux chambres : la Chambre d'assemblée (chambre basse) et le Sénat (chambre haute).

Protection des données en Eswatini

Il n'existe actuellement aucune loi promulguée en Eswatini qui recueille et traite spécifiquement de la protection de la vie privée et des données personnelles. Toutefois, deux propositions de loi, à savoir : la proposition de loi 2020 sur la criminalité informatique et la cybercriminalité et la proposition de loi 2020 sur la protection des données (« la proposition de loi 2020 »), sont censées traiter en profondeur de la protection des données et des personnes concernées. Le projet de loi sur la protection des données n° 21/2017 («le projet de loi sur la protection des données ») vise à rassembler toutes les lois existantes sur la protection des données, mais il n'a pas encore été promulgué. En attendant la promulgation de ses différents textes et selon la plupart des juridictions modernes, Eswatini reconnaît et protège le droit des personnes concernées sur leurs informations personnelles[102]. Par conséquent, le traitement (collecte, utilisation et divulgation) d'informations concernant une personne morale, qu'il s'agisse d'un traitement informatique ou autre, ne peut être effectué qu'avec le consentement exprès de la personne concernée. La collecte et le traitement non autorisés de données personnelles et leur divulgation à des tiers sont interdits et ne peuvent être effectués que dans des cas spécifiques.

102 La section 14 du règlement sur la protection des consommateurs prévoit que tout fournisseur de services numériques doit respecter la vie privée d'un consommateur lorsqu'il collecte et traite des données personnelles. Un fournisseur ne peut collecter, rassembler, traiter ou divulguer des données personnelles d'un consommateur que si : le consommateur y consent ; cela est nécessaire à la conclusion ou à l'exécution d'un contrat auquel le consommateur adhère ; le fournisseur est tenu par la loi de collecter, rassembler, traiter ou divulguer des données personnelles ; cela protège l'intérêt légitime du consommateur ; cela est nécessaire à la bonne exécution d'une obligation de droit public envers un organisme public ; ou cela est nécessaire à la poursuite de l'intérêt légitime du fournisseur d'un tiers auquel les informations sont fournies. Un prestataire en possession légitime des informations personnelles d'une personne concernée est tenu de conserver ces données de manière sécurisée, tant que les données personnelles sont utilisées et pendant une période d'au moins un an par la suite.

Introduction

Si la téléphonie mobile connaît sans aucun doute un essor colossal en Afrique subsaharienne, cette dernière connaît cependant un développement plus lent dans d'autres zones géographiques. En effet, largement bancarisée et disposant de liquidités, l'Afrique australe reste peu intéressée par les transferts et le paiement par téléphonie mobile. Cette sous-région ne compte que trois millions (3) d'utilisateurs actifs, contre 102 millions en Afrique de l'Est, 56 millions en Afrique de l'Ouest et 20 millions en Afrique centrale en 2020, selon le rapport de la GSMA.

Sur ces trois millions (3) d'utilisateurs actifs, une grande partie se trouve en Afrique du Sud, au Mozambique et en Eswatini (Swaziland). L'accès et l'utilisation de l'argent mobile ont contribué au développement de l'Eswatini au cours des dernières années. Selon l'enquête FinScope 2018 auprès des consommateurs, le taux d'utilisation du mobile money a augmenté de 42% (de 28% à 70%) entre 2014 et 2018. Cette augmentation de l'argent mobile est portée par la numérisation des services bancaires mobiles classiques, aux entreprises de téléphonie mobile et aux fintechs. Ces différents services permettent d'effectuer des transferts d'argent mobile et de souscrire à des offres de prêt. Les offres de prêt consistent en des services de crédit numérique mobile en vogue en Afrique de l'Est.

La première offre de crédit numérique a été lancée à Eswanti par Old Mutual Limited et Swazi MTN en octobre 2017 grâce à la recommandation de Likhandlela Insurance[103]. Une offre qui permet aux abonnés MTN d'obtenir une assistance funéraire pour la famille de l'utilisateur qui a souscrit à l'offre. Dans le prolongement de cette offre, MTN Eswatini, en partenariat avec Letshego, a lancé une nouvelle offre de prêt le 26 janvier 2021, à travers son service Momo Quick Loans[104]. En plus de cette offre, plusieurs autres (E-Mali[105] par Eswatini Mobile, Instant Pay Day Loans[106] par Standard Bank, et Nifty Credit[107] par GetBucks et Nifty Credit) sont proposées aux populations via des applications mobiles. L'objectif est d'attirer un marché potentiel dans un pays où seulement 52% de la population a accès aux services financiers (FinScope Swaziland 2018).

Ces offres collectent les données personnelles de leurs clients par le biais d'applications mobiles qui servent d'interfaces utilisateurs. Cette pratique peut porter atteinte à la vie privée des utilisateurs ; elle doit donc être remise en question de manière impartiale. Ce type de service de prêt est basé sur des applications mobiles en toute liberté en Eswatini, où il n'y a pas de loi spécifique sur la protection des données personnelles et peuvent donc conduire à des abus.

Les pratiques de traitement des données de ces applications, telles que définies dans leurs politiques et conditions d'utilisation, tiennent-elles compte de la réglementation sur la protection de la vie privée ? Cette étude vise à analyser les politiques de confidentialité et les conditions d'utilisation de ces applications et à examiner les risques potentiels en Eswatini. La première partie comprend un aperçu des données collectées par ces applications, et la deuxième partie examine leurs activités de traitement en fonction de la loi sur la protection des données personnelles. La dernière partie se termine en indiquant si ces applications respectent ou non la loi sur la protection des données personnelles.

---

103 Les montants de couverture de l'assurance Ikhandlela vont de 500 à 2000 SZL (acronyme de la monnaie du Swaziland : Lilangeni). La couverture peut être réclamée jusqu'à 12 mois.

104 Cette offre propose des prêts entre 50 et 200 SZL par le service MTN Eswatini Mobile Money (MoMo).

105 L'offre E-Mali d'Eswatini Mobile permet d'obtenir des prêts à court terme entre 50 et 800 SZL remboursables en 30 jours*

106 L'offre Instant Payday Loans de Standard Bank permet à un Estwanien de recevoir moins de 33% de son salaire mensuel pour lui fournir une aide financière en cas d'urgence. Ce prêt sans intérêt est conçu pour répondre aux besoins des clients qui ont besoin d'un financement à court terme. Le montant prêté est compris entre 500 et 5000 SZL avec un taux forfaitaire de 8% min de 40 SZL. En outre, le client peut accéder à l'offre mensuellement en fonction de la gestion du compte. Elle est accessible sur l'application mobile Standard Bank App.

107 Nifty Credit est une application de crédit numérique proposée par GetBucks qui permet aux habitants d'Eswatini d'obtenir des prêts flexibles jusqu'à R8000. Les prêts sont accordés sur la base du profil du client et de sa capacité de remboursement.

Aperçu des données collectées par les applications de prêt numérique

MTN MoMo[108] Lien de téléchargement : Google Play Store et Apple Store	Les informations collectées et traitées par l'application	
	Autorisations demandées	Au démarrage de l'application, MTN MoMo demande à. Accéder aux contacts de l'utilisateur . Accéder à l'agenda pour ajouter ou modifier des événements et envoyer des e-mails aux invités à l'insu des propriétaires . Accéder à la localisation précise (GPS et réseau) de l'utilisateur . Accéder aux photos / médias / fichiers pour lire le contenu du stockage USB, modifier ou supprimer le contenu du stockage USB et d'autres contenus. . Accéder à l'appareil photo pour prendre des photos et des vidéos . Accéder aux informations sur la connexion Wi-Fi et afficher les connexions Wi-Fi. . Gérer d'autres éléments, recevoir des données d'Internet, afficher les connexions réseau, contrôler la lampe de poche, l'accès complet au réseau, contrôler les vibrations et empêcher l'appareil de se mettre en veille.
	Informations recueillies auprès de l'utilisateur	Lors de l'inscription, MTN MoMo collecte des informations afin d'identifier l'utilisateur : nom, adresse postale, adresse électronique, numéros de téléphone et numéro de carte de crédit.
	Informations recueillies sur le l'appareil de l'utilisateur Informations collectées lors de l'utilisation MTN Eswatini	Le site Web MTN MoMo collecte les informations suivantes à partir de l'appareil d'un utilisateur : Informations stockées dans l'appareil : liste de contacts, journaux d'appels, contacts de comptes de réseaux sociaux, photos, vidéos ou tout contenu numérique pertinent. Dès qu'un utilisateur utilise le site web de MTN Eswatini sur son téléphone mobile, MTN MoMo collecte automatiquement les informations d'identification personnelle de l'utilisateur : liste de contacts, journaux d'appels, contacts des comptes de médias sociaux, photos, vidéos ou tout contenu numérique pertinent.
	Informations reçues de tiers	Informations obtenues auprès d'autres entités de MTN Eswatini et du Groupe MTN (société mère et filiales) et de tiers ; Partenaires commerciaux.

108 Politique de confidentialité de MTN Momo

	Utilisation des informations de l'utilisateur par l'application	La politique de MTN MoMo en matière de protection de la vie privée stipule qu'elle collecte les données des utilisateurs aux fins suivantes : . Traiter les transactions d'un utilisateur . Vérification de l'identité de l'utilisateur . Décaissement des prêts et collecte des paiements . Analyse du comportement de l'emprunteur et profilage . Obligations de MTNMoMo aux utilisateurs . Conformité - Respect des lois, de la réglementation relatives à la connaissance du client et à la lutte contre le blanchiment d'argent. . Services de marketing
	Informations partagées avec des tiers Accès aux données de temps à des tiers	MTN MoMo partage les informations des utilisateurs avec : Ses membres, agents, entités de MTN Eswatini et du groupe MTN Eswatini et toute personne agissant au nom d'un utilisateur. Ses partenaires commerciaux Des fournisseurs de services tiers La politique ne mentionne pas la durée pendant laquelle les tiers peuvent accéder aux informations personnelles des utilisateurs et les conserver. MTN indique donc qu'elle n'est pas responsable des actions ou des politiques de traitement des données des tiers qui ne sont pas membres du groupe MTN.
	Technologies de suivi du site web/cookies	MTN MoMo ne fournit aucune information sur l'utilisation des cookies sur son site web.
	Stockage des informations sur l'utilisateur par l'application	L'application ne donne pas de détails sur le stockage et la période de conservation des données collectées par MTN MoMo.

e-Mali[109] Lien de téléchargement : Google Play Store	Les informations collectées et traitées par l'application

109 e-Mali n'a pas de politique de confidentialité

	Autorisations recherchées	Au démarrage de l'application e-Mali demande à: . Accéder aux dossiers Photos et Media pour lire le contenu du stockage USB, modifier ou supprimer le contenu du stockage USB et d'autres contenus. . Gérer d'autres éléments, télécharger des fichiers sans notification, recevoir des données d'Internet, afficher les connexions réseau, accès complet au réseau, exécuter au démarrage, contrôler les vibrations et empêcher l'appareil de se mettre en veille.
	Informations collectées auprès de l'utilisateur	Informations non disponibles
	Informations collectées sur l'appareil de l'utilisateur Informations collectées lors de l'utilisation du site web e-Mali	Informations non disponibles Informations non disponibles
	Informations reçues de tiers	Informations non disponibles
	Utilisation des informations de l'utilisateur par l'application	Informations non disponibles
	Informations partagées avec des tiers Durée de l'accès aux données par des tiers	Informations non disponibles Informations non disponibles
	Technologie de suivi / cookies de site web	Informations non disponibles
	Stockage des informations sur l'utilisateur par l'application	Informations non disponibles

Instant PayDay des prêts par Standard Bank[110] (Application Standard Bank) Lien de téléchargement : Google Play Store et Apple Store	Les informations collectées et traitées par l'application	
	Autorisations demandées	Au démarrage de l'application, la Standard Bank demande : . d'accéder aux contacts de l'utilisateur, les informations sur son appareil . d'accéder à l'ID de l'appareil et aux informations sur les appels . d'accéder aux Photos / Multimédia / Fichiers et stockage, modifier ou supprimer le contenu du stockage USB et lire le contenu du stockage USB . d'accéder à l'appareil photo pour prendre des photos et des vidéos . d'ccéder à la localisation de l'utilisateur pour connaître son emplacement approximatif (en fonction du réseau mobile utilisé), la localisation précise (GPS et réseau) . d'accéder aux informations sur la connexion Wi-Fi et visualiser les connexions Wi-Fi. . de gérer d'autres accès tels que : recevoir des données en provenance d'Internet, afficher les connexions réseau, s'exécuter au démarrage, lire la configuration du service Google, désactiver le verrouillage de l'écran, empêcher l'appareil de se mettre en veille, contrôler la lampe de poche, contrôler les vibrations, créer des comptes et définir des mots de passe, lancer une diffusion permanente, accéder à l'ensemble du réseau et . contrôler la communication en champ proche.

110 Politique de confidentialité de l'application Standard Bank

	Informations recueillies auprès de l'utilisateur	Lors de l'inscription, l'application Standard Bank collecte des informations sur une personne physique identifiable et/ou, le cas échéant, sur une personne morale, y compris, mais sans s'y limiter, des informations sur la race, le sexe, la grossesse, l'état civil, la nationalité, l'origine ethnique ou sociale, la couleur, l'orientation sexuelle, l'âge, la santé physique ou mentale, le bien-être ; le handicap ; la religion ; la prise de conscience ; la croyance ; la culture ; la langue ; la naissance ; l'éducation ; les antécédents médicaux, financiers, criminels ou professionnels ; tout numéro d'identification, symbole, email, adresse postale ou physique, numéro de téléphone ; site ; tout identifiant en ligne ; toute autre affectation propre à la personne ; les informations biométriques ; les opinions personnelles ; les points de vue ou les préférences de la personne ou les points de vue ou les opinions d'une autre personne sur la personne ; la correspondance envoyée par la personne qui est implicitement ou explicitement de nature privée ou confidentielle ; ou toute autre correspondance qui révélerait le contenu du message original ; et le nom de la personne s'il apparaît avec des informations personnelles supplémentaires la concernant ou si la divulgation du mot lui-même révèle des informations sur la personne.
	Informations collectées à partir de l'appareil de l'utilisateur Informations recueillies lors de l'utilisation du site web de la Standard Bank	L'application Standard Bank contient les informations pertinentes permettant d'identifier l'utilisateur à partir de son terminal (voir la section précédente). Dès qu'un usager utilise le site web de Standard Bank sur son téléphone mobile, l'application Standard Bank collecte les informations pertinentes permettant l'identification de l'usager (voir la section précédente).
	Informations reçues de tiers	Informations obtenues d'autres entités de la Standard Bank et du groupe Standard Bank (société mère et filiales) et de tiers ; Partenaires commerciaux

	Utilisation des informations de l'utilisateur par l'application	Politique de confidentialité La Standard Bank affirme qu'elle collecte les données des utilisateurs aux fins suivantes : . Traitement des transactions des utilisateurs . Vérification de l'identité d'un utilisateur . Décaissement des prêts et recouvrement des paiements . Analyse du comportement de l'emprunteur et profilage . Responsabilités de la Standard Bank à l'égard des utilisateurs . Respect des lois, réglementations et règles relatives à la connaissance du client et à la lutte contre le blanchiment d'argent. . Services de marketing
	Informations partagées avec des tiers Durée de l'accès des données à des tiers	MTN MoMo partage les informations des utilisateurs avec : Ses membres, ses agents, la Standard Bank et les entités du groupe Standard Bank. Toute personne agissant au nom d'un utilisateur Des partenaires commerciaux Des prestataires de services tiers La politique ne mentionne pas la durée pendant laquelle les tiers peuvent accéder aux informations personnelles des utilisateurs et les conserver. En outre, la Standard Bank indique qu'elle n'est pas responsable des actions ou des politiques de traitement des données des tiers qui ne sont pas membres du groupe Standard Bank.
	Technologies de suivi du site web/cookies	La Standard Bank ne fournit aucune information sur l'utilisation des cookies sur son site web.
	Stockage des informations sur l'utilisateur par l'application	Aucun détail n'est donné concernant le stockage et la durée de conservation des données collectées par la Standard Bank.

Nifty Credit[111] par GetBucks et Nifty Credit Co Lien de téléchargement : Google Play Store et Apple Store	Les informations collectées et traitées par l'application

111 Politique de confidentialité non trouvée

	Autorisations recherchées	Au démarrage, Nifty Credit demande à: Accéder aux dossiers photos / Media pour obtenir le contenu du stockage USB, modifier ou supprimer le contenu du stockage USB et d'autres contenus. . Accéder à la localisation précise (GPS et réseau) de l'utilisateur . Accéder à l'appareil photo pour prendre des photos et des vidéos . Accéder aux informations sur la connexion Wi-Fi et visualiser les connexions Wi-Fi. . Gérer d'autres éléments, recevoir des données Internet, afficher les connexions réseau, contrôler la lampe de poche, l'accès complet au réseau, contrôler les vibrations et empêcher l'appareil de se mettre en veille.
	Informations recueillies auprès d'un utilisateur	Informations non disponibles
	Informations collectées à partir de l'appareil de l'utilisateur Informations recueillies lors de l'utilisation du site web	Informations non disponibles Informations non disponibles
	Informations reçues de tiers	Informations non disponibles
	Utilisation des informations utilisées par l'application	Informations non disponibles
	Informations partagées avec des tiers Temps d'accès aux données pour le tiers	Informations non disponibles Informations non disponibles
	Technologies de suivi/cookies du site web	Informations non disponibles
	Stockage des informations sur l'utilisateur par l'application	Informations non disponibles

Étude de cas : L'absence d'une véritable politique de confidentialité des données personnelles sur les applications mobiles du groupe MTN.

Comme en Côte d'Ivoire avec l'application MyMTN, l'application MTN MOMO de MTN Eswatini

ne dispose pas de politique de confidentialité. La politique de confidentialité associée à ses applications est une politique générale qui ne traite pas des spécificités et de la nature des données collectées. Cette situation reflète la mauvaise volonté du groupe à œuvrer en faveur du respect des réglementations relatives à la protection des données personnelles.

En ce qui concerne plus particulièrement l'Eswatini, l'absence d'une loi-cadre sur la protection de la vie privée ne dispense pas MTN de ses obligations. Sa présence dans plus de 22 pays d'Afrique et du Moyen-Orient et son poids économique et financier devraient lui permettre d'associer à ses applications mobiles des politiques légales de confidentialité adaptées aux différents contextes nationaux.

Analyse des pratiques de protection des données des applications de prêt numérique par rapport à la loi sur la protection des données personnelles

L'absence d'une loi-cadre sur la protection de la vie privée en Eswatini constitue un risque pour ses résidents. Toutefois, les responsables du traitement des données des entreprises qui offrent des applications de prêt numérique restent soumis à la loi sur la protection des consommateurs. Dans son article 14, cette loi prévoit des dispositions relatives à la protection de la vie privée dans l'attente de la nouvelle loi et de la création de la Commission Eswatini de la communication ("ECC")[112]. Par ailleurs, le projet de loi sur la protection des données de 2020 (projet) prévoit des obligations légales en matière de protection de la vie privée, applicables à tout traitement automatisé ou non[113] . Les demandes de prêts numériques devront tomber sous le coup de ladite loi pour minimiser les risques sur la protection de la vie privée.

En ce qui concerne les dispositions pertinentes relatives au respect de la vie privée en Eswatini, il est bon de noter que les applications étudiées sont en totale violation des principes de base. Ces violations concernent le droit à la vie privée, l'égalité, l'équité et la transparence, le partage d'informations avec des tiers, la confidentialité par conception et par défaut, le droit d'accès et de suppression des données personnelles, et la mobilité des données. En outre, certains d'entre eux ne disposent pas de politiques de confidentialité pour les données qu'ils traitent.

Les pratiques de traitement des données des demandes de crédit numérique en Eswatini sont essentielles pour protéger la vie privée. Face à la dynamique attendue de ce type de développement de services, les autorités politiques et administratives du pays doivent œuvrer à la mise en place d'une Autorité de protection des données. Dès sa mise en place, cette dernière devra effectuer des audits de conformité des activités des responsables de traitement et devra être dotée des moyens matériels lui permettant de contrôler les données collectées par les applications mobiles.

112 L'organe statutaire a été créé et censé être responsable de la publication des lignes directrices sur les données.
113 Article 3 du projet de loi sur la protection des données, 2020

Ethiopie

Profil du pays

Située en Afrique du Nord-Est (c'est-à-dire dans la Corne de l'Afrique)[114], l'Éthiopie, également connue sous le nom de République fédérale démocratique d'Éthiopie, partage une frontière avec l'Érythrée, Djibouti, la Somalie, le Kenya, le Sud-Soudan et le Soudan[115]. Elle couvre une superficie de 1 112 000 km2 et compte une population d'environ 110,14 millions d'habitants[116]. Il comprend environ 80 groupes ethniques, dont la plupart sont des Amharas et des Oromo. Sa capitale est Addis-Abeba, qui est aussi sa plus grande ville[117].

114 À propos de l'Éthiopie https://ethiopianembassy.org/overview-about-ethiopia/
115 Éthiopie https://www.britannica.com/place/Ethiopia
116 À propos de l'Éthiopie https://ethiopianembassy.org/overview-about-ethiopia/
117 Ibid

Protection des données en Éthiopie

En Éthiopie, les applications de prêt ne sont actuellement pas régies par un cadre juridique. Le pays ne dispose pas non plus d'une loi sur la protection des données pour contrôler les pratiques de prêt de ces applications[118]. Toutefois, des dispositions relatives à la vie privée et à la protection des données figurent dans d'autres textes législatifs du pays, dont le principal est la Constitution de la République fédérale démocratique d'Éthiopie de 1995[119]. La Constitution garantit le droit à la vie privée et donne aux fonctionnaires le devoir de respecter et de protéger ce droit[120].

La déclaration de protection des données de l'Éthiopie est encore à l'état de projet. Cette étude examinera les politiques de confidentialité des applications de prêt (sélectionnées) en Éthiopie afin de déterminer si elles protègent le droit à la vie privée des utilisateurs de ces applications.

Aperçu des données collectées par les applications de prêt numérique

L'application Dashen Amole	Informations collectées et traitées par l'application

118 Éthiopie-Protection des données Aperçu La vie privée et la protection des données personnelles en Afrique : Une enquête sur la législation de huit pays basée sur les droits (mai 2021) pg. 27
119 Éthiopie - Aperçu de la protection des données, section 26, Constitution de la République fédérale démocratique d'Éthiopie https://www.refworld.org/docid/3ae6b5a84.html
120 La déclaration de protection des données de l'Éthiopie est encore à l'état de projet. Cette étude examinera les politiques de confidentialité des applications de prêt (sélectionnées) en Éthiopie afin de déterminer si elles protègent le droit à la vie privée des utilisateurs de ces applications.

	Autorisations demandées	Demandes d'accès : au courrier électronique, aux messages texte (SMS), aux plateformes de réseaux sociaux ou applications mobiles. Lorsqu'un utilisateur ne souhaite plus que l'application accède à ces informations, il peut contacter le service clientèle pour mettre fin à l'utilisation du service de l'application.
	Informations recueillies auprès de l'utilisateur	L'application recueille le nom, l'adresse, l'adresse électronique et le numéro de téléphone de l'utilisateur lors de son inscription.
	Informations collectées à partir de l'appareil de l'utilisateur	
	Utilisation des informations de l'utilisateur	Exécution des obligations envers l'utilisateur Suivre les instructions de l'utilisateur Ouverture et tenue du compte de l'utilisateur, facilitation des transactions, gestion des réclamations et des risques. Fins statistiques et analytiques Marketing Respect de la réglementation applicable
	Informations reçues de tiers	Les informations sont collectées auprès des tiers suivants : Rapports de solvabilité Agences gouvernementales Partage les informations avec : des personnes offrant des services d'assistance Ses filiales et sociétés affiliées
	Divulgation d'informations personnelles Durée de l'accès aux tiers	Divulgue les informations relatives aux utilisateurs dans les circonstances suivantes : Lorsque la loi l'exige à la demande de la banque nationale d'Ethiopie (National Bank of Ethiopia NBE) Dans le cadre de son obligation publique de divulguer l'information Lorsque l'intérêt légitime de l'utilisateur ou de l'entreprise exige la divulgation de l'information Lorsque l'utilisateur y consent Lorsqu'elle est ordonnée par un tribunal Non indiqué

	Technologies de suivi/ cookies de site web	Types de cookies utilisés : Cookies de session : Temporaires et n'existent que lorsqu'un utilisateur navigue sur le site. Cookies persistants : Permanents et stockés dans l'appareil de l'utilisateur jusqu'à leur expiration ou leur suppression par un utilisateur. Cookies de première partie : Appartenant et créés par Dashen Cookies tiers : Appartenant et conçus par les prestataires de services de Dashen.
	Stockage des informations sur l'utilisateur	

Application HelloCash	Informations collectées et traitées par l'application	
	Autorisations demandées	
	Données collectées auprès de l'utilisateur	Informations sur le contact Numéro de téléphone entre autres
	Données collectées auprès de l'appareil de l'utilisateur	L'adresse du protocole Internet (IP), le nom de l'appareil, le système d'exploitation, la configuration de l'application, l'heure et la date de l'utilisation des services par l'utilisateur.
	Utilisation des informations de l'utilisateur	Aucun détail explicite sur l'utilisation des informations données La politique indique seulement que les informations relatives aux utilisateurs seront partagées avec des tiers pour aider à l'identification des utilisateurs.
	Informations reçues de tiers	Identité des utilisateurs : L'application utilise des services tiers pour faciliter l'identification des utilisateurs.
	Utilisation des informations par des tiers/ Divulgation des informations Durée de l'accès aux informations par des tiers	Partage des informations avec des tiers aux fins suivantes : Facilitation des services de HelloCash Fourniture des services de HelloCash en son nom Analyse des services de HelloCash Les tiers sont tenus de ne pas divulguer ou utiliser les informations de l'utilisateur à d'autres fins. Non indiqué
	Technologies de suivi/ cookies de site web	La politique indique que l'application n'utilise pas de cookies (cela doit être confirmé). La politique indique également que l'application utilise des cookies de tiers.
	Stockage	Il ne garantit pas aux utilisateurs la sécurité de leurs données

Application de prêt de la Commercial Bank of Ethiopia	Les informations collectées et traitées par l'application	
	Autorisations demandées	Demande l'accès : aux contacts du téléphone mobile, et d'autres fonctions (la politique ne précise pas les fonctions
	Informations recueillies auprès d'un utilisateur	
	Informations recueillies dans l'appareil de l'utilisateur	L'application collecte des informations concernant l'appareil mobile de l'utilisateur (la politique ne précise pas de quelles informations il s'agit)
	Utilisation des informations de l'utilisateur	La politique n'indique pas comment les informations de l'utilisateur sont utilisées.
	Informations reçues de tiers	Aucune indication
	Utilisation des informations par des tiers/ divulgation des informations Durée de l'accès des informations à tiers	Le partage les informations relatives aux utilisateurs dans les circonstances suivantes : Lorsque le consentement de l'utilisateur a été obtenu Pour la réalisation de son intérêt légitime Pour l'exécution du contrat avec l'utilisateur Pour l'accomplissement d'obligations légales - c'est-à-dire le respect des lois, des demandes du gouvernement, des procédures judiciaires, des ordonnances du tribunal, des processus juridiques. Pour l'investigation et la prévention de la fraude ou des activités illégales Aucune indication
	Technologies de suivi / cookies du site web	Aucune indication
	Stockage d'informations sur l'utilisateur par l'application	Aucune indication
TeleBirr par EthioTelecom	Les informations collectées et traitées par l'application	

	Autorisations demandées	
	Informations recueillies auprès de l'utilisateur	Collecte les informations suivantes auprès des utilisateurs : Données contenues dans les commentaires des utilisateurs faits sur le site, y compris l'adresse IP et le navigateur de l'utilisateur.
	Informations collectées à partir de l'appareil de l'utilisateur	
	Informations reçues de tiers	Aucune indication
	Utilisation des informations de l'utilisateur par l'application	Aucune indication
	Informations partagées avec des tiers	Aucune indication
	Technologies de suivi/cookies de sites web	Lorsqu'ils font des commentaires sur le site, les utilisateurs peuvent enregistrer leurs informations dans les cookies du site, à savoir leur nom, leur adresse électronique, etc. Cookies temporaires : ils sont supprimés lorsque l'utilisateur ferme le navigateur. Cookies qui enregistrent les informations de connexion de l'utilisateur lorsqu'il se connecte au site. Cookies enregistrés dans le navigateur de l'utilisateur lors de l'édition ou de la publication d'articles sur le site
	Conservation des informations sur les utilisateurs	Aucune indication

Analyse des pratiques de protection des données de ces applications

L'Éthiopie ne dispose pas d'une loi unique sur la protection de la vie privée et des données permettant d'évaluer la conformité des applications dans le cadre de cette étude. Toutefois, le pays dispose du droit à la vie privée prévu par la Constitution, qui garantit à chacun le droit de ne pas être soumis à des fouilles de son domicile, de sa personne ou de ses biens. La Constitution garantit également aux individus le droit à la confidentialité de leurs communications effectuées par téléphone ou par télécommunication sur des appareils électroniques. Elle donne aux agents publics l'obligation de respecter et de protéger ce droit[121].

Cette recherche examinera les pratiques de traitement des données de ces applications par rapport aux normes requises pour la sécurisation de la vie privée et la protection des données personnelles.

121 Section 26, Constitution de la République fédérale démocratique d'Éthiopie https://www.refworld.org/docid/3ae6b5a84.html

Clarté sur les politiques de confidentialité

Les politiques de confidentialité étudiées ne sont pas suffisamment détaillées quant à leurs pratiques de traitement des données. Elles ne fournissent pas à l'utilisateur des informations adéquates sur les données collectées, la manière dont elles sont collectées et l'utilisation prévue. Elles ne précisent pas non plus quels tiers auront accès aux données et pendant combien de temps. Il est important de noter qu'il n'est pas fait mention des mesures de sauvegarde mises en place pour protéger les données partagées avec des tiers, de la durée de conservation de ces données et des mesures de sécurité mises en place pour protéger les données en leur possession. Une politique de confidentialité devrait au moins fournir des informations sur ces questions essentielles. Elle doit permettre à l'utilisateur de savoir comment l'entreprise (l'entité chargée de l'application de prêt) entend traiter et utiliser ses données, ainsi que ses droits d'accès et de rectification[122].

Les politiques de confidentialité des applications étudiées dans cette recherche peuvent susciter la crainte des utilisateurs en raison d'un manque de certitude sur la manière dont elles utilisent et conservent leurs données. Elles ne fournissent pas suffisamment d'informations pour permettre aux utilisateurs de prendre des décisions éclairées pour ce qui est de l'utilisation de leur application.

Contrôle de l'utilisateur

Les entités propriétaires d'applications de prêt devraient permettre aux utilisateurs de contrôler leurs données. Elles devraient leur donner la possibilité de refuser les messages marketing et leur permettre d'accéder à leurs données et d'en demander la correction et la suppression. L'accès aux données personnelles est essentiel car les personnes concernées ont des droits sur leurs données. Cependant, l'examen de ces applications indique que la plupart ne permettent pas aux utilisateurs de contrôler leurs données. Par exemple, l'application de prêt de la Commercial Bank of Ethiopia et l'application HelloCash ne prévoient aucun droit dans leurs politiques. Seules Ethio Telecom et DashenBank permettent aux utilisateurs d'accéder à leurs données et de demander la suppression et la correction de celles-ci. DashenBank va plus loin en permettant aux utilisateurs de ne pas recevoir de messages marketing.

Securité

La sécurité des données est cruciale, surtout lorsque de grandes quantités de données personnelles sont traitées. Les applications de prêt numérique, par exemple, sont très gourmandes en données, et l'accès à leurs services dépend des données des utilisateurs. Elles doivent mettre en place des mesures de sécurité solides pour éviter les violations et l'accès aux données des utilisateurs par des entités malveillantes. Certaines n'ont pas de clauses de sécurité indiquant les mesures de protection qu'elles entendent mettre en place.

Accès par des tiers

Ces applications n'indiquent pas quels sont les tiers qui ont accès aux données des utilisateurs, quelles sont les informations auxquelles ils accèdent, combien de temps ils y ont accès et quelles mesures ces applications ont mis en place pour garantir la sécurité des données auxquelles les tiers ont accès. L'application DashenBank est la seule à indiquer les tiers qui ont accès aux informations personnelles des utilisateurs.

Les applications étudiées n'indiquent pas combien de temps elles comptent conserver les données des utilisateurs et quels critères elles utilisent pour déterminer cette conservation. Elles laissent les utilisateurs dans l'incertitude quant à la durée pendant laquelle ces entités conserveront leurs données et si cette conservation se poursuivra même après la désinstallation des applications.

122 Centre d'inclusion financière pg.1

Objectif de la collecte des données

Une entité qui traite les données personnelles d'un utilisateur doit indiquer clairement le type de données collectées et l'objectif de la collecte. Les politiques de confidentialité des applications de cette étude n'indiquent pas aux utilisateurs la finalité de la collecte des données. La seule application qui fournit cette information est l'application Dashen Bank, qui énumère les informations collectées et les utilisations qui en sont faites[123].

123 Politique de confidentialité de la Dashen Bank : Clause de recouvrement https://dashenbanksc.com/privacy-and-security/

Gabon

Profil du pays

Le Gabon est un pays francophone situé en Afrique centrale qui compte 2 172 579 habitants[124] . Ce pays est traversé par l'équateur et a pour frontières la République du Congo, la Guinée équatoriale et le Cameroun. Pays membre de la Communauté Economique et Monétaire des États de l'Afrique centrale (CEMAC)[125], le Gabon a un PIB de 16,87 milliards USD (2019)[126] et est gouverné par un système semi-présidentiel[127].

124 https://fr.countryeconomy.com/pays/gabon
125 La Communauté économique et monétaire des États de l'Afrique centrale (CEMAC) est une organisation internationale regroupant plusieurs pays d'Afrique centrale, créée pour prendre le relais de l'Union douanière et économique de l'Afrique centrale (UDEAC). Son siège est à Bangui, en République centrafricaine. Elle regroupe les pays suivants : Cameroun, République centrafricaine, Congo-Brazzaville, Gabon, Guinée équatoriale et Tchad.
126 https://www.google.com/search?client = avast-a-1 & q = le + GDP + du + gabon & oq = le + PIB + du + gabon & aqs = avast..69i57j0l6.9968j0j4 & ie = UTF-8 (Source Banque Mondiale)
127 http://archive.ipu.org/parline-f/reports/CtrlParlementaire/1115_F.htm

Protection des données au Gabon

La protection des données personnelles au Gabon est régie par la loi 001/2011 du 25 septembre 2011[128]. La loi s'applique à tout traitement automatique ou non effectué sur le territoire du Gabon[129]. La Commission Nationale de Protection des Données Personnelles (CNPDCP) est l'APD du Gabon[130]. Elle a été créée par la loi 001/2011 du 25 septembre 2011 et est chargée de veiller à ce que le traitement des données personnelles respecte les libertés individuelles[131]. En parallèle, les transactions électroniques sont régies par l'ordonnance n° 00000014 / PR / 2018 du 23 février 2018.

Introduction

Selon le rapport conjoint "Stimulating Electronic Commerce in Central Africa: Role of Mobile Services and Policy Implications" du Groupement mondial des opérateurs de téléphonie mobile (Association GSM) et de la Commission économique pour l'Afrique (CEA), les pays d'Afrique centrale sont en retard par rapport à ceux des autres régions africaines en termes d'accès à l'internet mobile. En effet, les données de l'Intelligence GSMA indiquent que le taux de pénétration d'internet mobile au sein de la Communauté économique des États d'Afrique centrale (CEEAC) a atteint 23% en 2019, contre 43% en Afrique du Nord., 29% dans la Communauté économique des États d'Afrique de l'Ouest (CEDEAO), 26% dans la communauté d'Afrique australe et 21% en Afrique de l'Est. En outre, la sous-région est toujours confrontée à des défis importants tels que le manque de compétences en TIC et la

128 https://www.afapdp.org/wp-content/uploads/2012/01/Gabon-Loi-relative-%c3%a0-la-protection-des-donn%c3%a9es-personnelles-du-4-mai -2011.2.pdf
129 Article 2 et 4 de la loi 001/2011 du 25 septembre 2011
130 Pour plus d'informations : https://www.cnpdcp.ga/presentation/
131 Article 11 de la loi 001/2011 du 25 septembre 2011

faible capacité institutionnelle à soutenir les entreprises innovantes. Autant de choses qui ne facilitent pas le développement du Mobile Money. Pourtant, au sein de la CEEAC, le Gabon occupe la première place en termes de pénétration de l'internet, avec un taux de 38%. Aussi, la pénétration du mobile money a été extrême au Gabon (43% de la population de plus de 15 ans avait un compte en 2017 contre 6,7% en 2017) mais est restée supérieure à celle des autres pays de ladite région, 15% au Cameroun et au Tchad, et 6% au Congo et inférieure à celle du Kenya 73%.

Par ailleurs, le mobile money en Afrique centrale et au Gabon reste confiné à des services simples tels que les dépôts et les retraits d'argent sur les téléphones mobiles. Ce sont les sociétés de téléphonie mobile qui exercent ces activités : Airtel Mobile Gabon, Moov Africa Gabon, certaines banques (BGFI Bank, Ecobank Gabon, etc.) offrant des services numériques à leurs clients traditionnels et des FinTechs (E-Doley Finance, Fedha Finance, etc.) avec diverses solutions de monnaie électronique. Grâce à ces entreprises, les services de mobile money permettent de payer à distance son abonnement à un service de télévision, ses factures d'eau et d'électricité, ses frais scolaires et universitaires, mais aussi ses impôts, etc.

Malgré ces possibilités offertes aux populations, les activités de prêt et de crédit numérique ne sont pas encore très développées au Gabon comme en Afrique de l'Est. Seules deux offres de crédit numérique sont proposées au Gabon par des entreprises domiciliées en dehors dudit pays. Viva PS est qui propose la première offre de prêt Open Loans Gabon[132]. Cette offre permet d'obtenir directement des prêts personnels sans garantie et d'entrer en contact les emprunteurs et prêteurs domiciliés au Gabon.

Son objectif est de créer un marché de prêt efficace, opérationnel et instantané entre les populations au Gabon. Les prêts sont soumis à un taux d'intérêt compris entre 12 et 15%, à un remboursement minimum et à une période de remboursement de 90 jours et 365 jours, respectivement. Des offres sont également disponibles dans les pays africains comme le Ghana, le Kenya, le Nigeria et la Tanzanie. Spectro Coin propose la deuxième partie du mouvement des crypto-monnaies à travers les Crypto-Prêts sur son portefeuille Bitcoin par une application Crypto Loans sur son portefeuille Bitcoin par une application. Cette offre, lancée en 2013, permet aux détenteurs de comptes en crypto-monnaies (Bitcoin, Ethereum, etc.) au Gabon d'obtenir et de garantir des prêts convertibles dans différentes devises telles que l'euro (€) ou le dollar ($). Ces prêts vont de 25 à plus de 15 000 (€) (16 000 FCFA à plus de 9 000 000 FCFA). Avec l'adoption progressive des crypto-monnaies dans le monde, ce type d'offre va se généraliser. Bien qu'elles élèvent l'accès au financement pour les citoyens et surtout pour les emprunteurs privés, ces différences permettent aux fournisseurs de collecter des données sur leurs clients pour suivre les transactions et récupérer les fonds. Cette pratique peut porter atteinte à la vie privée des utilisateurs et doit être examinée de manière impartiale. Ce type de service de prêt basé sur des applications mobiles s'est développé après l'entrée en vigueur de la loi sur la protection des données au Gabon[133]. Les pratiques de traitement des données de ces applications, telles que définies dans leurs politiques et conditions d'utilisation, tiennent-elles compte de la réglementation sur la protection de la vie privée ?

Cette étude vise à analyser les politiques de confidentialité et les termes et conditions de ces applications et à examiner leur conformité avec la loi sur la protection des données au Gabon. La première partie comprend un aperçu des données collectées par ces applications. La deuxième partie examine leurs activités de traitement au regard de la loi sur la protection des données personnelles. La dernière partie se termine en indiquant si ces applications respectent ou non la loi sur la protection des données personnelles.

132 Open Loans Gabon a été lancé en Janvier 2018.
133 Loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel au Gabon.

Aperçu des données collectées par les applications de prêt numérique

Open Loans Gabon[134] Lien de téléchargement : Google Play Store[135]	Les informations collectées et traitées par l'application	
	Permissions demandées	Au démarrage, Open Loans Gabon App demande de : . gérer les appels des utilisateurs - accéder aux SMS d'un utilisateur : Elle affiche les SMS d'un utilisateur pour collecter des informations financières et des données transactionnelles afin de recueillir des informations sur l'historique financier d'un utilisateur et déterminer sa solvabilité. Accéder aux contacts de l'utilisateur accéder aux données de localisation, de l'appareil et d'utilisation : l'application Open Loans Gabon utilise la technologie GPS ou d'autres services de localisation pour déterminer l'emplacement actuel d'un utilisateur. . Accès au calendrier des utilisateurs, Open Loans Gabon App lire les événements du calendrier et les informations confidentielles, ajouter ou modifier les événements du calendrier et envoyer des e-mails aux invités à l'insu des propriétaires. . Accès Photos / Multimédia / Fichiers, peut lire le contenu de votre stockage USB, modifier ou supprimer le contenu de votre stockage USB. . Open Loans Gabon peut également recevoir des données Internet, afficher les connexions réseau, l'accès complet au réseau, s'exécuter au démarrage, prendre le dessus sur d'autres applications, contrôler les vibrations, empêcher les appareils de se mettre en veille et régler l'alarme.
	Informations recueillies auprès de l'utilisateur	Lors de l'inscription, Open Loans Gabon collecte les informations de l'utilisateur : adresse e-mail, nom et numéro de téléphone, informations financières et de paiement, authentification, contacts fournis activement par l'utilisateur, références de crédit et pays de résidence

134 Politique de confidentialité pour les prêts et le crédit
135 Politique de confidentialité pour les prêts et le crédit

	Informations recueillies sur l'appareil de l'utilisateur Informations collectées lors de l'utilisation	Le site de Open Loans Gabon collecte les informations suivantes à partir de l'appareil de l'utilisateur : Technique d'intelligence artificielle (IA) : modèle du téléphone mobile, numéro IMEI ou numéro de série de l'appareil, informations sur la carte SIM, informations sur le réseau mobile, système d'exploitation de l'appareil, type de navigateur, emplacement de l'appareil et réglage du fuseau horaire. Informations stockées dans l'appareil : liste de contacts, historique des appels, historique des SMS, contacts des comptes de réseaux sociaux, photos, vidéos ou tout contenu numérique pertinent. Dès qu'un utilisateur se connecte à Internet, les applications de données sont transmises par HTTPS. Ces informations sont ensuite regroupées à des fins d'analyse ou de marketing et mises à la disposition d'Orange Bank.
	Informations reçues de tiers	Open Loans Gabon reçoit des registres de prêteurs dans chaque pays où des applications similaires sont utilisées : Kenya, Ghana, Nigeria et Tanzanie, afin de donner aux emprunteurs un choix aussi large que possible d'opportunités lorsqu'ils recherchent un financement.
	Utilisation des informations de l'utilisateur par l'application	La politique de confidentialité d'Open Loans Gabon indique qu'elle recueille les données des utilisateurs pour les raisons suivantes . le traitement des transactions d'un utilisateur . vérification de l'identité d'un utilisateur . décaissements de prêts et évaluation du recouvrement des paiements . crédit et création de modèles de crédit . analyse du comportement de l'emprunteur . conformité à la reglémentation en vigueur relative à la "connaissance du client" et aux règles de lutte contre le blanchiment d'argent . prévention des fraudes, · Marketing services . Responsabilités de l'application Open Loans Gabon envers les utilisateurs Les données personnelles et sensibles de l'utilisateur collectées par l'application avec le consentement de l'utilisateur et protégées par cette politique sont limitées aux informations personnellement identifiables, aux informations financières et de paiement, aux informations d'authentification, aux contacts activement fournis par l'utilisateur, aux références de crédit et au pays de résidence.

	Informations partagées avec des tiers Durée de l'accès des données aux tiers	Open Loans Gabon partage les informations relatives aux utilisateurs avec des prêteurs tiers pour analyser le risque de crédit et prendre des décisions de prêt. Les informations concernant les visiteurs non identifiables personnellement peuvent être fournies à d'autres parties à des fins de marketing, de publicité ou autres. Ces parties acceptent de garder ces informations confidentielles et ne peuvent les divulguer. La politique ne précise pas combien de temps les tiers peuvent accéder aux informations personnelles des utilisateurs et les conserver. Lesdits tiers ne sont pas autorisés à suivre le comportement des utilisateurs.
	Technologies de suivi du site web/ cookies	Open Loans Gabon indique qu'il n'utilise pas de cookies pour les suivis. Pour les connexions sur ordinateur, l'utilisateur est averti de l'envoi d'un cookie. L'utilisateur a donc la possibilité de choisir ou de désactiver tous les cookies.
	Stockage des informations de l'utilisateur par l'application	Les informations personnelles des utilisateurs sont contenues dans des réseaux sécurisés. Elles ne sont accessibles qu'à un nombre limité de personnes qui ont des droits d'accès spéciaux à ces systèmes et qui doivent garder ces informations confidentielles. En outre, toutes les informations sensibles / informations de crédit transmises sont cryptées à l'aide de la technologie Secure Socket Layer (SSL). Toutes les transactions sont traitées par un fournisseur de passerelle et ne sont ni stockées ni traitées sur les serveurs de Open Loans Gabon. En outre, diverses mesures de sécurité sont mises en œuvre lorsqu'un utilisateur saisit, soumet ou accède à ses informations afin de préserver la sécurité de ses données.

Bitcoin Wallet par SpectroCoin[136] Lien de téléchargement : Google Play Store et Apple Store	Informations collectées et traitées par l'application

136 Politique de confidentialité de Bitcoin Wallet Apps

	Autorisations demandées	Au démarrage, Bitcoin Wallet demande à : . Gérer les informations d'identité de l'utilisateur, trouver des comptes sur l'appareil et ajouter ou supprimer des comptes. . Accéder aux contacts de l'utilisateur . Accéder aux Photos / Multimédia / Fichiers et autres contenus de l'utilisateur, accéder au contenu de votre stockage USB et modifier ou supprimer le contenu de votre stockage USB . Accédez à l'appareil photo pour prendre des photos et des vidéos et au microphone pour l'enregistrement audio. Accéder aux données de localisation, de l'appareil et d'utilisation : Bitcoin Wallet utilise la technologie GPS ou d'autres services de localisation pour déterminer l'emplacement actuel de l'utilisateur. . Il peut également afficher les connexions réseau, créer des comptes et définir des mots de passe, accéder à l'ensemble du réseau, modifier les paramètres audio de l'utilisateur et empêcher les appareils de se mettre en veille. . Des fonctionnalités peuvent être ajoutées automatiquement dans chaque groupe en cas de mise à jour de l'application Bitcoin Wallet de SpectroCoin.
	Informations recueillies auprès de l'utilisateur	Lors de l'inscription, Bitcoin Wallet collecte les informations suivantes sur les utilisateurs : (i) Données d'identification générales : prénom, second prénom, ancien nom, alias, nom de famille, sexe, date de naissance, adresse résidentielle, email, numéro de téléphone, selfie (avec la pièce d'identité), vidéo en temps réel ; (ii) Données relatives aux pièces d'identité : Type de pièce d'identité (passeport / carte d'identité / permis de séjour), sa copie, zone de lecture automatique (MRZ) numéro du document, date d'émission, date d'expiration ; (iii) Données relatives au profil de l'autre Client : type de profil, identifiant de membre, code de parrainage, statut de connexion, statut de confirmation par email, statut de confirmation par téléphone, informations sur les questions secrètes ; (iv) Données relatives aux réseaux sociaux : type de connexion aux réseaux sociaux, photo de profil de réseau social, nom, prénom, vos commentaires, émotions et autres actions exprimées via notre compte de réseau social, autres informations de votre profil de réseau social fournies par vous ; et (v) Informations sur la profession et les sources de revenus du client : profession spécifique, principaux secteurs de la profession du client, source de la richesse et des fonds dans le compte du client, source de revenus fixes, informations sur le pourcentage du chiffre d'affaires de l'activité du client susmentionné traité en espèces.

	Informations recueillies sur l'appareil de l'utilisateur Informations recueillies lors de l'utilisation du site web https:// spectrocoin. com website	Bitcoin Wallet collecte les informations suivantes à partir de l'appareil d'un utilisateur : Technique d'intelligence artificielle (IA) : modèle de l'appareil mobile, numéro IMEI ou numéro de série de l'appareil, informations sur la carte SIM, informations sur le réseau mobile, système d'exploitation de l'appareil, type de navigateur, localisation de l'appareil et réglage du fuseau horaire. Informations enregistrées dans l'appareil : liste de contacts, historiques d'appels, historiques de SMS, contacts de comptes de médias sociaux, photos, vidéos ou tout autre contenu numérique pertinent. Dès qu'un utilisateur utilise le site web de Spectro Coin, Bitcoin Wallet collecte automatiquement les informations suivantes et les stocke dans ses fichiers journaux : L'adresse IP de l'utilisateur, le type de navigateur, le fournisseur d'accès à Internet (FAI), les pages de référence/de sortie, le système d'exploitation, l'horodatage et le support de navigation. Ces données sont ensuite regroupées pour une analyse ou à des fins de marketing.
	Informations reçues de tiers	L'entreprise collecte vos données directement auprès de vous ou de tiers lorsque : vous utilisez ou consultez la plateforme ; vous vous inscrivez sur la plateforme ; vous utilisez nos services ; vous demandez de l'aide à nos services ; nous effectuons une vérification préalable du client ou une vérification préalable continue ; nous surveillons vos transactions ; nous vérifions si vous n'êtes pas lié à une activité frauduleuse ; nous recevons des requettes, des ordres, des décisions, etc. de tiers vous concernant. L'entreprise peut également collecter vos données auprès d'autres entreprises SpectroCoin, telles que définies dans les Conditions Générales de la plateforme lors du changement de l'entreprise SpectroCoin en tant que votre fournisseur de services.

	L'utilisation des informations de l'utilisateur par l'application	La politique de confidentialité de Bitcoin Wallet indique qu'elle collecte les données des utilisateurs à: . l'ouverture du compte de l'utilisateur ; . l'exécution des services (tels que la vente et l'achat, le retrait, le dépôt, les transactions d'échange) ; . la prévention du blanchiment d'argent et du financement du terrorisme (mise en œuvre du principe "Know Your Customer") ; . la prévention de la criminalité ; . le respect et la mise en œuvre des sanctions internationales ; . les services d'assistance ; . l'assurance qualité ; . Inscription sur la liste d'attente pour la fourniture des services ; . marketing direct et utilisation des comptes de médias sociaux de l'entreprise ; . le fonctionnement correct et sécurisé de la plateforme Bitcoin Wallet.
	Informations partagées avec des tiers Durée de l'accès aux données par des tiers	Bitcoin Wallet partage les informations des utilisateurs avec les autres entités du groupe Spectrocoin dans 40 pays pour favoriser le suivi des clients auprès des autorités internationales en charge de la lutte contre la cybercriminalité, le blanchiment d'argent, la protection des données personnelles, les bureaux de crédit, etc.... En fonction de la catégorie de données personnelles et de la finalité de leur traitement, la durée de conservation de vos données est applicable dans l'entreprise, conformément à la loi ou aux pratiques commerciales, afin de garantir la bonne exécution des services.
	Technologies de suivi / Cookies du site web	Bitcoin Wallet utilise une technologie de suivi mobile et des cookies pour distinguer les utilisateurs de l'application. La politique en matière de cookies (à partir de maintenant, la « politique en matière de cookies ») s'applique à l'accès au site web (https://spectrocoin.com) et à d'autres domaines/sous-domaines du groupe, tels que https://spectrocoin.com/crypto-loans/app, https://exchange.spectrocoin.com ou tout autre site web, page, fonctionnalité ou contenu et explique les types de cookies.

	Stockage des données de l'utilisateur par l'application	Bitcoin Wallet traite les données personnelles pour atteindre les objectifs indiqués dans cette politique. Pour fixer les durées de conservation des données collectées, l'entreprise s'est référée aux actes juridiques et aux recommandations publiques telles que le respect des délais de prescription légitimes et les pratiques commerciales courantes. L'entreprise utilise diverses technologies et procédures garantissant la sécurité afin de protéger vos données contre tout traitement non autorisé ou illégal, perte accidentelle, mauvaise utilisation, accès non autorisé, utilisation illégale, destruction, divulgation, dommages, etc. Cela comprend des mesures de sécurité juridiques, organisationnelles, techniques et physiques, telles que les systèmes de sécurité les plus récents, les mots de passe, la capacité à détecter les attaques de cybersécurité et autres menaces pour l'intégrité de la plate-forme, le fait de ne travailler qu'avec les services dignes de confiance des fournisseurs, etc. Toutefois, aucune transmission d'informations par courrier électronique ou par d'autres canaux de télécommunication, ni votre accès à la plate-forme ou aux services via l'internet ne peuvent être totalement sécurisés. Par conséquent, vous devez faire preuve de prudence lorsque vous accédez à la plateforme ou utilisez les services via Internet ou lorsque vous partagez des informations confidentielles par courrier électronique ou par d'autres canaux de télécommunications.

Étude de cas : La question du traitement automatisé des données réalisé hors du territoire du Gabon et la domiciliation des responsables de traitement

La loi du 25 septembre 2011, relative à la protection des données à caractère personnel dans ses articles 2, 3 et 4 stipule qu'elle s'applique à tous les traitements automatisés ou non de données à caractère personnel sur le territoire du Gabon. Dans le cas de ces deux applications, même si les entreprises qui les proposent sont domiciliées hors du Gabon, ladite loi leur est applicable. Or, les politiques de confidentialité fournies par ces deux entreprises ne stipulent aucune relation avec la Commission nationale de protection des données personnelles (CNPDCP). Cette situation remet en cause le contrôle du processus de traitement des données par les sociétés domiciliées hors du pays ou des données collectées.

Analyse des pratiques de protection des données des applications de prêt numérique au regard de la loi relative à la protection des données personnelles

La loi gabonaise sur la protection des données personnelles a clairement défini les obligations légales en matière de protection de la vie privée, applicables à tout traitement, automatique ou non[137]. Ainsi, les demandes de prêts numériques y sont soumises. Cependant, en raison de leur développement récent, les risques qu'elles présentent pour la protection de la vie privée sont courants. Cette section met en évidence les dispositions

137 Articles 2 et 4 de la loi 001/2011 du 25 septembre 2011

pertinentes de la loi afin d'établir si ces applications sont conformes à ces dispositions.

Droit à la vie privée

La loi sur la protection des données exige que les responsables du traitement et les gestionnaires des données (dans ce cas, les applications de prêt numérique) traitent les données personnelles en respectant le droit à la vie privée de la personne concernée[138]. Cette loi demande aux entreprises qui fournissent ces applications de veiller à ce que le droit à la vie privée des emprunteurs prime lors du traitement de leurs données. Les applications étudiées violent ce droit et traitent des données de manière intrusive et sans rapport avec l'objectif de la collecte des données. Par exemple, ces applications collectent des informations telles que les contacts enregistrés sur l'appareil d'un emprunteur, les informations de connexion des plateformes de médias sociaux, la localisation précise en temps réel, les photos/médias/fichiers des utilisateurs, etc. Comportement qui entraîne la violation de la réglementation sur la protection des données personnelles et des objectifs assignés à leur collecte.

Légalité, équité et transparence

La loi sur la protection des données exige que les applications collectent et traitent les données de manière équitable et légale[139]. Conformément à cette disposition, les entreprises doivent obtenir le consentement des utilisateurs. Les personnes concernées doivent être formellement informées de la manière dont leurs données seront utilisées et s'assurer que tous les paramètres de la loi sont respectés dans ce traitement[140].

En l'occurrence, les applications doivent informer les utilisateurs des raisons pour lesquelles leurs données sont collectées, de la manière dont elles seront utilisées et, si elles sont partagées avec des tiers, des personnes avec lesquelles elles seront partagées et de la durée de conservation des données. On peut dire que les applications étudiées sont transparentes quant aux raisons pour lesquelles elles collectent les données des utilisateurs et avec qui elles les partagent. Cependant, elles n'indiquent pas pendant combien de temps les tiers auront accès aux données et combien de temps elles les conserveront.

Limitation de l'objet, pertinence et adéquation

Les applications de prêt numérique sont tenues, en vertu de la loi sur la protection des données, de traiter les données personnelles après leur collecte[141]. Cela signifie qu'elles ne doivent collecter que des données dans les limites du prêt numérique et non des données superflues. Les applications sont également tenues de ne collecter que des données pertinentes, adéquates et limitées à ce qui est nécessaire pour la collecte des données[142].

Les applications examinées collectent des informations personnelles non pertinentes et contraires à l'objectif de la collecte de données. Elles collectent des informations sur les emprunteurs telles que leurs profils de médias sociaux, leurs contacts téléphoniques, leurs photos et leurs vidéos, qui ne sont pas pertinentes dans le cadre du prêt numérique.

Partage des informations avec des tiers

La loi sur la protection des données stipule que ces applications doivent informer les utilisateurs à propos des personnes tierces[143] avec lesquelles leurs données seront partagées, y compris les mesures adoptées pour protéger leurs données avant de

138 Articles 2,3 et 4 de la loi 001/2011 du 25 septembre 2011
139 Article 45 de la loi 001/2011 du 25 septembre 2011
140 Article 46 de la Loi 001/2011 du 25 septembre 2011
141 Articles 8, 66, 68, et 69 de la Loi 001/2011 du 25 septembre 2011
142 Article 45 de la loi 001/2011 du 25 septembre 2011
143 Article 13 de la Loi 001/2011 du 25 septembre 2011

les collecter[144]. L'absence d'une période fixe de traitement et de stockage des données constitue une violation du droit à la vie privée.

En matière de lutte contre le blanchiment d'argent et de protection, les applications examinées partagent les informations relatives aux utilisateurs/emprunteurs avec des tiers tels que des sociétés affiliées, des partenaires commerciaux et des organismes gouvernementaux et d'application de la loi, les données personnelles, etc. et n'indiquent pas les mesures de protection adoptées pour protéger les données des emprunteurs. Les applications n'indiquent pas non plus pendant combien de temps ces tiers auront accès aux données et pour combien de temps ils les conserveront. En plus, les règles de confidentialité des deux applications ne font pas référence à leur relation spécifique avec l'APD du Gabon.

Confidentialité par conception et par défaut

La loi prévoit que le responsable du traitement des données doit prendre toutes les dispositions pour traiter les données des utilisateurs [145]. Les applications disposent de mesures de cryptage pour protéger les communications et le contenu privé de leurs utilisateurs, un niveau de sécurité nécessaire pour protéger les données des utilisateurs. Toutefois, le niveau de protection inclus ne peut empêcher le fournisseur d'applications de collecter des informations superflues.

Droit d'accès et de suppression des données personnelles

Les utilisateurs des applications ont le droit d'accéder à leurs données détenues par ces applications et de demander l'effacement ou la destruction de leurs données que les applications ne sont plus autorisées à conserver, ou qui ne sont pas pertinentes, sont superflues ou obtenues illégalement [146]. Les fournisseurs d'applications ont mis en place des services dédiés pour recevoir les demandes des utilisateurs à ce sujet.

Mobilité des données

Elle leur donne également le droit, lorsque c'est techniquement possible, de faire transmettre les données directement à d'autres responsables du traitement des données ou à des gestionnaires de données[147]. Les applications examinées ne permettent pas aux utilisateurs d'exercer ce droit.

Les formalités préalables à la mise en œuvre d'un traitement de données personnelles

La loi prévoit que les traitements automatisés de données à caractère personnel doivent être déclarés à la Commission nationale de la protection des données à caractère personnel (CNPDCP) [148]. La loi a prévu la désignation d'un correspondant à la protection des données. Cette disposition est principalement due à la domiciliation des prestataires des applications étudiées [149]. Un bilan documentaire des recommandations du CNPDCP n'indique pas que les entreprises de cette étude aient obtenu ces autorisations.

Les pratiques de traitement des données des demandes de crédit numériques au Gabon sont réglementées par différents aspects de la loi en vigueur sur la protection de la vie privée. Des évaluations d'impact sur la protection des données (DPIA) doivent être réalisées par les responsables du traitement des demandes de crédit numériques. Cette évaluation permettra de respecter strictement les obligations légales. Par ailleurs, une révision de la

144 Article 14, 48, 60 et 66 de la Loi 001/2011 du 25 septembre 2011
145 Article 66, 68, 69, et 70 de la Loi 001/2011 du 25 septembre 2011
146 Article 7, 8, 9, 10, 11, 12, 13 et 14 de la loi 001/2011 du 25 septembre 2011.
147 Article 14 de la loi 001/2011 du 25 septembre 2011
148 Article 51 de la loi 001/2011 du 25 septembre 2011
149 Article 51 de la loi 001/2011 du 25 septembre 2011

loi n° 2013-50 du 19 juin 2013 relative à la protection des données personnelles doit être envisagée, compte tenu des nouveaux risques liés à la vie privée. Au-delà, il est également nécessaire que le CNPDCP se dote des moyens matériels et techniques pour contrôler le volume, la qualité et la quantité de données collectées par les responsables du traitement des applications mobiles. Sans oublier la nécessité pour le CNPDCP d'assurer une veille technologique permanente sur l'apparition de nouvelles entités dont l'activité principale nécessite la collecte et le traitement de données personnelles.

Ghana

Profil du pays

Le Ghana, également connu sous le nom de République du Ghana, est situé en Afrique occidentale[150]. Il s'étend sur le golfe de Guinée et l'océan Atlantique à son sud. Le Ghana partage une frontière avec la Côte d'Ivoire, le Burkina Faso et le Togo[151] et possède un beau relief qui comprend des plaines basses traversées par des collines, des rivières et le lac Volta, connu comme le plus grand lac artificiel du monde[152].

Le pays couvre une superficie de 238 533 km2[153] et compte plus de 31 millions d'habitants[154]. Sa capitale est Accra, et l'anglais est l'une des langues les plus parlées, suivie de l'akan et d'autres langues autochtones[155].

150 Ghana https://www.britannica.com/place/Ghana
151 Ghana https://www.nationsonline.org/oneworld/ghana.htm
152 Ghana https://www.nationsonline.org/oneworld/ghana.htm
153 Profil du pays Ghana https://www.bbc.com/news/world-africa-13433790
154 Worldometer https://www.worldometers.info/world-population/ghana-population/
155 Article 3 (1), Loi sur les systèmes et services de paiement, 2019

Protection des données au Ghana

Le prêt numérique au Ghana dispose d'un cadre réglementaire diversifié. Les plateformes de prêt sont réglementées par plusieurs organismes établis en vertu de diverses lois qui les régissent. La plus importante d'entre elles est la loi de 2019 sur les systèmes et services de paiement, qui donne à la Banque du Ghana le mandat de les superviser et de les réglementer[156]. En vertu de cette loi, les plateformes doivent demander leur enregistrement auprès de la Bank of Ghana [157], chargée de délivrer les licences [158]. Le fait de ne pas demander l'enregistrement constitue une infraction et rend la plate-forme passible, en cas de condamnation, d'une amende ou d'une peine d'emprisonnement d'une durée déterminée[159].

En raison de l'intensité de leurs données, les plateformes de prêt sont également réglementées par la Commission de protection des données établie en vertu de la loi sur la protection des données de 2012[160]. La loi met en place la Commission pour protéger la vie privée des individus et assurer la protection des données personnelles[161]. En vertu de la loi, les établissements de prêts numériques doivent s'enregistrer auprès de la Commission[162],

156 Article 3 (1), Loi sur les systèmes et services de paiement, 2019
157 Article 8 (1), Loi sur les systèmes et services de paiement, 2019
158 Article 3 (2)(l), Loi sur les systèmes et services de paiement, 2019
159 Article 9, Loi sur les systèmes et services de paiement, 2019
160 Article 2, Loi sur la protection des données, 2012
161 Article 2, Loi sur la protection des données, 2012
162 Article 27 (1), Loi sur la protection des données, 2012

qui est chargée de réglementer le traitement des informations personnelles[163]. La loi rend obligatoire l'enregistrement des plateformes, faute de quoi elles sont passibles, en cas de condamnation, d'une amende ou d'une peine d'emprisonnement d'une durée déterminée. Troisièmement, en raison des menaces que représentent les systèmes informatiques, les plateformes relèvent également de la réglementation de l'Autorité de cybersécurité établie en vertu de la loi sur la cybersécurité de 2020[164]. L'Autorité réglemente les activités de cybersécurité dans le pays et réagit aux menaces et incidents de cybersécurité[165]. L'un de ses objectifs essentiels est de tenir pour responsables les propriétaires d'infrastructures d'information sensibles en termes d'activités de cybersécurité, les prestataires de services de cybersécurité et les professionnels du Ghana[166].

Quatrièmement, les plateformes sont soumises à la loi de 2020 sur la lutte contre le blanchiment d'argent, qui leur interdit de mener des activités de blanchiment d'argent. Cette loi crée le centre de renseignement financier, qui identifie efficacement le produit d'activités illicites et lutte contre le blanchiment de capitaux et le financement d'activités terroristes[167]. Enfin, les plateformes sont soumises à la loi sur les transactions électroniques, qui vise à supprimer et prévenir les incidents au commerce électronique et à développer un environnement sûr, sécurisé et efficace pour que les consommateurs, les entreprises et le gouvernement puissent effectuer et utiliser des transactions électroniques[168]. Cette loi vise à créer un climat de sécurité pour les plateformes de prêt[169].
La présente étude se concentre sur la réglementation de ces plateformes au regard de leurs activités de traitement des données. Elle examine le cadre réglementaire entourant ces plateformes pour la protection des données. Elle commence par examiner la nature des données traitées par ces plateformes et analyse ensuite si leurs activités de traitement sont conformes à la loi sur la protection des données. La recherche se concentre sur quatre plateformes de prêt clés au Ghana, à savoir Airtel Money Bosea, MTN Qwik Loan, FIDO Micro Finance et EcoBank Mobile Money.

Aperçu des données collectées par les applications de prêt numérique

Airtel Money Bosea -Termes et conditions non disponibles -Politique de confidentialité non disponible	Informations collectées et traitées par l'application	
	Autorisations demandées	
	Informations recueillies auprès de l'utilisateur	
	Informations recueillies dans l'appareil de l'utilisateur	
	Informations reçues de tiers	.
	Utilisation des informations de l'utilisateur par l'application	

163 Article 2 (a), Loi sur la protection des données, 2012
164 Article 2, Loi sur la cybersécurité, 2020 (Loi 1038)
165 Article 3 (a)&(b), Loi de 2020 sur la cybersécurité (Loi 1038)
166 Article 3 (c) Loi sur la cybersécurité, 2020 (Loi 1038)
167 Article 7 (a)(b)(i)(ii), Loi sur la cybersécurité, 2020 (Loi 1038)
168 Article 1, Loi sur les transactions électroniques, 2008 (Loi 772)
169 Law and Practice: Fintech Market (2.2 Regulatory Regime) https://practiceguides.chambers.com/practice-guides/comparison/626/6478/10265-10267-10280-10284-10289-10292-10295-10305-10310-10314-10317-10320-10329

	Informations partagées avec des tiers Durée de l'accès aux informations par des tiers	
	Stockage des informations de l'utilisateur par l'application	

MTN Qwik Loan	Informations collectées et traitées par l'application	
	Autorisations demandées	La seule politique disponible est la politique de confidentialité générale du groupe MTN[170].
	Informations recueillies auprès de l'utilisateur	
	Informations recueillies dans l'appareil de l'utilisateur	
	Informations reçues de tiers	
	Utilisation des informations de l'utilisateur par l'application	
	Informations partagées avec des tiers Durée de l'accès des informations aux tiers	
	Stockage des informations sur l'utilisateur par l'application	
	Suivi et cookies	.

170 Politique de confidentialité du groupe MTN https://www.mtn.com/privacy-policy/

FIDO Micro Credit[171]	Informations collectées et traitées par l'application	
	Autorisations demandées	Demande l'autorisation d'accéder : au compte du réseau social de l'utilisateur
	Informations recueillies auprès de l'utilisateur	FIDO collecte les informations suivantes sur les utilisateurs de son application et de son site web : Informations personnelles : informations de souscription, de facturation, les informations générées par la communication de l'utilisateur. Les informations relatives à l'appareil sont collectées automatiquement par l'application et le site web : données de connexion, données d'utilisation du produit, applications installées (sur l'appareil de l'utilisateur), historiques de SMS, liste de contacts, adresse e-mail, compte de tiers et numéro de téléphone de l'appareil. Les personnes tierces (partageant les informations avec la FIDO) : Bureaux de référence de crédit et registres d'identification, comptes de réseaux sociaux et fournisseurs de données tiers.
	Informations collectées à partir de l'appareil de l'utilisateur	Informations sur l'appareil recueillies par l'application et le site web : données de journal, données d'utilisation du produit, applications installées, historiques SMS, liste de contacts, adresse électronique, compte de tiers et numéro de téléphone de l'appareil.
	Informations reçues de tiers	FIDO reçoit des informations des tiers suivants : Bureaux de référence de crédit et registres d'identification, comptes de réseaux sociaux et fournisseurs de données tiers.
	Utilisation des informations de l'utilisateur par l'application	Amélioration des produits et services de prêt de FIDO et de l'expérience utilisateur Recherche et développement Facturation et recouvrement Contact avec l'utilisateur Marketing Support client Analyse de crédit Vérification de l'identité de l'utilisateur Respect des exigences légales ou des demandes des autorités Poursuite ou défense des droits de FIDO dans le cadre de procédures judiciaires Transmission d'informations à des tiers autorisés

171 Politique de confidentialité de FIDO Micro Credit https://www.fidocredit.com/privacy.html

	Informations partagées avec des tiers Durée de l'accès des informations aux tiers	Partage des informations avec les tiers suivants : Les associés de FIDO, c'est-à-dire les administrateurs, les dirigeants, les employés et les actionnaires. les vendeurs, entrepreneurs, fournisseurs, agents, prestataires de services et de paiement de FIDO Les personnes agissant au nom des utilisateurs, telles que les récipiendaires de paiement, les bénéficiaires, les comptes de prête-nom, les intermédiaires, les correspondants et les banques agents. les personnes recommandées par FIDO les partenaires commerciaux en cas de vente, de fusion, de transfert ou d'acquisition. Bureaux d'information sur le crédit Organismes d'application de la loi, tribunaux ou fonctionnaires Non indiqué
	Stockage des informations sur l'utilisateur par l'application Cookies et technologies de suivi	Un protocole sécurisé de cryptage protège les informations personnelles de l'utilisateur transmises par l'application.
EcoBank Mobile App[172]	Informations collectées et traitées par l'application	
	Autorisations demandées	
	Informations recueillies auprès de l'utilisateur	Collecte des informations suivantes auprès des utilisateurs lors de leur inscription : Nom adresse e-mail Numéro de téléphone Date de naissance Sexe Adresse de résidence Numéro d'identification ID de l'appareil Localisation de l'appareil

172 Avis de confidentialité de l'application mobile EcoBank https://www.ecobank.com/privacy-centre/personal-banking-privacy-notice/mobile-app

	Informations collectées à partir de l'appareil de l'utilisateur	Adresse IP Informations sur les cookies Identifiants de l'appareil mobile et de la publicité Version du navigateur Type de système d'exploitation et version Informations sur le réseau mobile Paramètres de l'appareil, et Données du logiciel Collecte également des informations sur l'utilisateur auprès de tiers pour vérifier le compte et l'appareil de l'utilisateur.
	Informations reçues de tiers	
	Utilisation des informations de l'utilisateur par l'application	Authentification et autorisation de l'accès de l'utilisateur aux services de l'application. Communication avec l'utilisateur, c'est-à-dire par le biais de courriels, de SMS, d'appels téléphoniques, etc, Diffusion de publicités aux utilisateurs Commercialisation de ses produits Enquêter et résoudre les plaintes des clients Enquête sur les fraudes et les violations de la politique de confidentialité
	Informations partagées avec des tiers/ Partage d'informations personnelles	EcoBank peut partager les informations des utilisateurs avec les tiers suivants : Ses sociétés affiliées ou partenaires Ses filiales technologiques et de sécurité Ses prestataires de services et partenaires marketing
	Stockage des informations sur l'utilisateur par l'application Cookies et technologies de suivi	Les informations sont conservées aussi longtemps que le compte de l'utilisateur est actif ou nécessaire pour fournir des services ExpressPay, se conformer aux obligations légales, résoudre les litiges et appliquer ledit accord.

Analyse des pratiques de protection des données des applications de prêt numérique par rapport à la loi sur la protection des données de 2012

La loi sur la protection des données au Ghana contient des dispositions clés, des sections 18 à 24, qui sont essentielles pour les pratiques de protection des données des applications de prêt numérique opérant au Ghana. La loi définit les principes qui doivent être observés par ces applications et leurs obligations en matière de confidentialité et de protection des informations personnelles des emprunteurs. Cette section met en évidence les dispositions pertinentes de la loi afin d'établir si les applications sont conformes à ces dispositions.

Manque (indisponibilité) de politiques de confidentialité

Les politiques de confidentialité sont cruciales pour les plateformes de prêt numérique en raison de l'intensité de leurs données. Elles fournissent des informations essentielles aux utilisateurs sur les données traitées par les plateformes, leur utilisation, l'accès des

données aux tiers, la période de conservation des données, le stockage des données, et si les données seront transférées en dehors de la juridiction de l'utilisateur. Elles permettent aux utilisateurs de savoir comment les plateformes de prêt ont l'intention de traiter leurs données et s'ils exercent un contrôle sur leurs données, c'est-à-dire un droit d'accès, de rectification, de suppression ou de transfert des données personnelles[173].
Deux des principales plateformes de prêt étudiées, à savoir Airtel Money Bosea et MTN Qwik Loan, n'ont pas de politique de confidentialité. Ce défaut est contraire à l'obligation qui leur incombe en vertu de la loi sur la protection des données de 2012, qui les oblige à informer les utilisateurs sur les aspects suivants :

- la nature des données traitées,
- le nom et l'adresse de la plateforme de prêt,
- la finalité de la collecte des données, que cette collecte soit discrétionnaire ou obligatoire,
- les conséquences en cas de manque de communication des données,
- les destinataires des données, et le droit de la personne concernée à accéder aux données et,
- demande de rectification des données avant leur collecte.[174]

Contrôle de l'utilisateur

Les plateformes de prêt doivent permettre aux utilisateurs d'exercer un contrôle sur leurs données en leur donnant la possibilité d'y accéder, de les corriger et de les transférer à d'autres fournisseurs.[175] Ce droit doit être prioritaire car les utilisateurs sont les garants de leurs données. La loi sur la protection des données énonce cette exigence et fournit des orientations complètes sur la manière dont ces plateformes peuvent faciliter le droit d'accès des utilisateurs.[176]

Les plateformes de prêt telles que Airtel Money Bosea et MTN Qwik Loan refusent aux utilisateurs le contrôle de leurs données en raison de l'absence de politiques de confidentialité permettant aux utilisateurs de savoir comment exercer ces droits. La FIDO et EcoBank Mobile Money fournissent des canaux permettant aux utilisateurs d'exercer ces droits. EcoBank Mobile Money ne permet pas aux utilisateurs de demander la mobilité de leurs informations personnelles.

Objectif de la collecte de données

Les plateformes de prêt en ligne devraient se limiter à collecter et à utiliser les données des utilisateurs en conformité avec les services de prêt.[177] Elles doivent tenir compte de la vie privée de l'utilisateur[178] et s'assurer que le traitement des données personnelles est nécessaire, pertinent et non abusif.[179] La collecte des informations d'un utilisateur telles que les données de connexion, les applications installées, l'historique des SMS, les listes de contacts et les actualités des comptes de médias sociaux ne cadre pas avec l'objectif du prêt en ligne.[180]

Ces informations sont intrusives et portent atteinte à la vie privée des utilisateurs. On s'inquiète du fait que les données des utilisateurs, telles que les informations obtenues à partir de leurs plateformes de réseaux sociaux pour l'évaluation du crédit, puissent être utilisées ou vendues de manière inappropriée sans leur consentement.[181] Les créanciers doivent s'assurer que les données sont utilisées dans le meilleur intérêt du client et non

173 Centre d'inclusion financière pg.1
174 Article 27, Loi sur la protection des données, 2012
175 [Focus on Making Data Work for the Poor] pg. 2
176 Article 32-35, Loi sur la protection des données, 2012.
177 [Focus on Making Data Work for the Poor] pg.10
178 Article 17 (c) de la loi sur la protection des données, 2012
179 Article 19, Loi sur la protection des données, 2012.
180 Politique de confidentialité de FIDO - 'Information We Collect' https://www.fidocredit.com/privacy.html
181 John Owens, Responsible Digital Credit: What Does Responsible Digital Credit Look Like? (July 2018) pg 25 https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/1970/01/Responsible_Digital_Credit_FINAL_2018.07.18.pdf

d'une manière qui lui porte préjudice.[182]

Automatisation de la prise de décision

Les plateformes de prêts numériques emploient des modèles de notation de crédit alternatifs qui s'appuient sur l'IA pour déterminer la solvabilité d'un utilisateur. Les systèmes d'IA accèdent au contenu stocké dans l'appareil d'un utilisateur, comme l'appareil photo, les contacts, le stockage, entre autres, pour créer le score de crédit de l'utilisateur.[183] Les scores créés par ces systèmes basés sur l'évaluation des données d'un utilisateur peuvent parfois être injustes. Les entités de prêt devraient concevoir ces systèmes de manière à garantir l'équité et l'absence de préjugés.[184] Pour ce faire, les entités devraient employer du personnel qui surveille et évalue constamment les décisions prises par les systèmes d'IA afin de s'assurer que les systèmes ne provoquent pas d'inégalités financières.[185]

Mesures de sécurité

En vertu de la loi sur la protection des données, les plateformes de prêt numérique sont tenues de prendre les mesures nécessaires pour garantir la sécurité des données en leur possession en adoptant des mesures appropriées, raisonnables, techniques et organisationnelles.[186] Cette protection est nécessaire pour protéger les données contre la perte, l'accès et le traitement illicites.[187] Pour ce faire, les applications doivent d'abord identifier tout risque raisonnablement prévisible pour les données personnelles. Ensuite, elles doivent établir et maintenir des garanties appropriées contre les risques identifiés et vérifier régulièrement que les garanties sont effectivement mises en œuvre. Enfin, elles sont tenues de s'assurer que les garanties sont continuellement mises à jour en réponse aux nouvelles menaces.[188]

En raison de la quantité importante de données traitées par les plateformes de prêt numériques, le respect strict de cette disposition est nécessaire pour garantir la sécurité des données. Les applications étudiées suscitent de nombreuses inquiétudes quant à leurs mesures de sécurité. Certaines, notamment Airtel Money Bosea et MTN Qwik Loan, n'ont pas de politique de confidentialité, ce qui est un point essentiel en l'espèce pour indiquer aux utilisateurs les mesures de sécurité adoptées par les plateformes. D'autres, comme FIDO Microcredit, n'ont pas de clauses sur les mesures de sécurité, laissant ainsi les utilisateurs sans aucune information sur la manière dont la plateforme stockera leurs données.
Traitement des données provenant des bureaux de crédit

Les applications de prêt numérique accèdent aux données de tiers, tels que les bureaux de d'information sur le crédit, aux fins de l'évaluation de la solvabilité d'un emprunteur. Les applications, si elles ne sont pas limitées, peuvent accéder à des données personnelles superflues, ce qui est contraire à l'objectif du prêt numérique. Dans ce cas, la loi limite la portée des données auxquelles ces applications peuvent accéder à partir des bureaux de référence de crédit afin d'empêcher la violation. Elle indique que les données des bureaux de crédit auxquelles ces applications ont accès doivent être limitées à la situation financière et à l'historique de la personne concernée pour la période qui précède les 12 mois suivant l'obtention du prêt.[189]

182 [Focus on Making Data Work for the Poor] pg.2
183 L'analyse des risques par l'IA va-t-elle vraiment élargir l'accès au crédit en Afrique ?
184 [Focus on Making Data Work for the Poor] pg.2
185 [Focus on Making Data Work for the Poor] pg.3
186 Article 28 (1), Loi sur la protection des données, 2012
187 Article 28 (1), Loi sur la protection des données, 2012
188 Article 28 (2), Loi sur la protection des données, 2012
189 Article 36 (2), Loi sur la protection des données, 2012

Kenya

Profil du pays

Le Kenya est un pays situé dans la région de l'Afrique de l'Est.[190] Il a une superficie de 580 000 km2[191] et a pour frontières la Somalie, l'Éthiopie et le Soudan au nord et l'Ouganda et la Tanzanie à l'ouest et au sud.[192] Sa capitale est Nairobi, qui est le comté le plus développé. Selon le rapport du recensement national de 2019, le Kenya a une population de 47 000 000 millions d'habitants.[193]

190 À propos du Kenya https://www.britannica.com/place/Kenya
191 https://www.nationsonline.org/oneworld/kenya.htm
192 https://www.un.int/kenya/kenya/general-information-about-kenya
193 Recensement de la population et des logements au Kenya en 2019 Volume I : Population par comté et sous-comté https://www.knbs.or.ke/?wpdmpro=2019-kenya-population-and-housing-census-volume-i-population-by-county-and-sub-county

Protection des données au Kenya

Les applications de prêt numériques ont fourni aux Kenyans un moyen pratique d'accéder à des prêts rapides et à court terme. Elles rendent les prêts facilement accessibles aux personnes qui, autrement, ne disposent pas de comptes bancaires et de sources de revenus classiques nécessaires pour emprunter auprès d'institutions financières.[194] Leur fonctionnalité leur a permis de gagner en popularité au Kenya. Une étude menée par FSD Kenya indique que plus de 6 millions de Kenyans ont accédé à des prêts grâce à ces applications au cours des dernières années.[195]

Cependant, ces applications restent essentiellement non réglementées, ce qui leur permet de pratiquer des taux d'intérêt élevés et de mettre en œuvre des pratiques qui violent les droits des utilisateurs. Le gouvernement tente de remédier à cette situation par le biais du projet de loi de la Central Bank of Kenya, (amendement) de 2021, qui est en cours d'examen au Parlement.[196] Ce projet de loi, une fois adopté, soumettra effectivement les applications de prêt à la Central Bank of Kenya (CBK) et exigera qu'elles obtiennent une licence de la Banque.[197] Le projet de loi obligera la CBK de superviser les activités de ces applications[198] et lui donnera, entre autres, le pouvoir de définir des règlementations sur: l'enregistrement des applications, leur gestion, les activités autorisées et interdites, le partage d'informations avec les bureaux de référence de crédit, leurs activités de protection des données, la

194 Le Kenya se prépare à sévir contre un flot d'applications de prêts à taux d'intérêt élevé. <https://qz.com/africa/1975202/kenya-prepares-to-crack-down-on-high-interest-loan-apps/> Consulté le 26/7/2021
195 Fsd Kenya, Rapport d'audit sur le crédit numérique : Évaluation de la conduite et des pratiques des applications de prêt numériques au Kenya (septembre 2019) pg iv.
196 Projet de loi 2021 de la Central Bank of Kenya http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2021/TheCentralBankofKenya_Amendment_Bill_2021.pdf
197 Article 33 (S) (1), Central Bank of Kenya (amendement) projet de loi 2021.
198 Article 3 (da), Central Bank of Kenya (amendement) projet de loi 2021

protection des consommateurs et leurs exigences en matière de reporting.[199]
Il convient de noter qu'une fois le projet de loi adopté, les applications partageront et recevront des informations des bureaux d'information sur le crédit Ce n'était pas le cas l'année dernière lorsque le gouvernement les a effectivement exclues des systèmes de référence des bureaux de crédit lors de la pandémie de COVID-19.[200]

En ce moment, les applications collectent beaucoup d'informations personnelles lors de l'octroi de ces prêts. La quantité de données collectées par la plupart d'entre elles est excessive par rapport à l'objectif du traitement, ce qui entraîne une violation de la vie privée des utilisateurs. La loi sur la protection des données de 2019 énonce d'importantes dispositions qui sont cruciales pour les activités de traitement de ces applications.
Cette étude vise à analyser les politiques de confidentialité et les conditions générales de ces applications et à examiner leur conformité avec la loi sur la protection des données. La première partie comprend un aperçu des données collectées par ces apps. La deuxième partie examine leurs activités de traitement au regard de la loi sur la protection des données. La dernière partie conclut en indiquant si ces applications sont conformes ou non à la loi sur la protection des données.

Aperçu des données collectées par les applications de prêt numérique

Tala[201]	Informations collectées et traitées par l'application	
	Autorisations demandées	Gérer les appels des utilisateurs Accès aux SMS de l'utilisateur Accès aux contacts de l'utilisateur Accès à la localisation de l'utilisateur (en utilisant la technologie GPS) et aux données de l'utilisateur
	Informations recueillies auprès de l'utilisateur	le nom, l'adresse, l'adresse électronique et le numéro de téléphone de l'utilisateur, le numéro de téléphone de l'appareil, la carte SIM, l'âge, le nom d'utilisateur, le mot de passe, les informations financières et de crédit, la description personnelle et la photographie, ainsi que d'autres informations de souscription.
	Informations collectées à partir de l'appareil de l'utilisateur Informations recueillies lors de l'utilisation du site web de Tala	Données techniques : Modèle de l'appareil mobile, IMEI ou numéro de série de l'appareil, informations sur la carte SIM, informations sur le réseau mobile, système d'exploitation de l'appareil, type de navigateur, localisation de l'appareil et réglage du fuseau horaire. Informations stockées dans l'appareil : liste de contacts, historique des appels, historique des SMS, contacts des comptes de réseaux sociaux, photos, vidéos ou tout autre contenu numérique pertinent. L'adresse IP de l'utilisateur, le type de navigateur, le fournisseur d'accès à Internet (FAI), les pages de renvoi/de sortie, le système d'exploitation, l'horodatage et le média clickstream. Ces informations sont stockées dans les fichiers journaux de Tala et utilisées pour des analyses ou du marketing.
	Informations reçues de tiers	Réception d'informations provenant d'agences d'évaluation du crédit, de fournisseurs de réseaux mobiles et d'agences de recouvrement.

199 Article 6 (3), Central Bank of Kenya (amendement) projet de loi 2021
200 624 sociétés de prêt numérique interdis de partager les données de leurs clients avec les organismes de contrôle du crédit https://www.businessdailyafrica.com/bd/markets/market-news/624-digital-loan-from-sharing-client-data-with-crbs-3416546
201 Politique de confidentialité de Tala https://tala.co.ke/privacy-policy-ke/

	Utilisation des informations de l'utilisateur par l'application	Traitement des transactions Vérification Déboursement du prêt Evaluation du crédit Analyse du comportement de l'emprunteur Respect des obligations du prêteur Conformité aux règles KYC (Know Your Customer Requirements) et anti-blanchiment d'argent Prévention de la fraude Marketing
	Informations partagées avec des tiers Durée de l'accès des tiers	Partage des informations relatives aux utilisateurs avec les entités suivantes : Ses membres, agents, prestataires de services, et toute personne sous-traitée par elle. Les personnes agissant au nom d'un utilisateur Institutions financières, bureaux d'information sur le crédit Partenaires commerciaux en cas de transfert d'entreprise, de cession, de fusion et d'acquisition, etc. Prestataires de services tiers Organismes chargés de l'application de la loi, fonctionnaires gouvernementaux, sur la base : d'une demande formelle ou ordonnance du tribunal du respect de la loi ou signalement d'une activité illégale présumée Non indiqué
	Technologies de suivi / cookies du site web	La technologie de suivi mobile et les cookies du site web sont utilisés pour distinguer les utilisateurs de l'application.
	Stockage d'informations sur les utilisateurs	Les informations des utilisateurs se trouvant hors du Kenya et traitées par le personnel opérant hors du Kenya.

Branch[202]	Informations collectées et traitées par l'application	
	Autorisations demandées	Accès aux: contacts SMS appels téléphoniques données de localisation : Utilisation de la technologie GPS
	Informations recueillies auprès d'un utilisateur	Nom, adresse, adresse électronique et numéro de téléphone, détails de la carte SIM, âge, nom d'utilisateur, mot de passe, informations financières et de crédit et autres informations de souscription.

202 Politique de confidentialité de Branch https://branch.co.ke/pp

	Informations collectées à partir de l'appareil de l'utilisateur	Informations techniques : Modèle de l'appareil mobile, IMEI ou numéro de série de l'appareil, informations sur la carte SIM, informations sur le réseau mobile, système d'exploitation de l'appareil, type de navigateur utilisé par un utilisateur, emplacement de l'appareil et réglage du fuseau horaire. Informations stockées dans l'appareil : liste de contacts, historique des appels, historique des SMS, contacts de comptes des réseaux sociaux, photos, vidéos ou tout autre contenu numérique pertinent. les données provenant de toute application tierce utilisée par un utilisateur sur l'appareil.
	Informations reçues de tiers	Les informations sont reçues de tiers tels que les agences d'évaluation du crédit, les fournisseurs de réseaux mobiles et les agences de recouvrement.
	Utilisation des informations de l'utilisateur par l'application	Vérification de la solvabilité Sa politique indique également qu'elle ne partage les informations relatives aux utilisateurs que dans le cadre d'une ordonnance d'un tribunal, d'une commission arbitrale, d'un tribunal, d'une prescription ou d'une ordonnance réglementaire, ou de toute autre obligation légale ou réglementaire.
	Informations partagées avec des tiers Durée de l'accès des données par des tiers	Partage les informations sur les utilisateurs avec les organismes suivants : agence d'évaluation de crédit Ses membres, c'est-à-dire ses filiales, ses sociétés affiliées, ses sociétés de holding Des partenaires commerciaux lors de la vente d'actifs Les administrations en conformité avec les obligations légales ou réglementaires Non indiqué
	Stockage des informations sur les utilisateurs	It stores user information outside Kenya, where its staff is processed outside the country.
	Suivi et cookies	Mobile tracking technologies/ website cookies are used to distinguish users of the App.
LionCash[203]	Informations collectées et traitées par l'application	
	Autorisations demandées	Accès aux : SMSs Données de localisation : Utilise des informations précises de localisation en temps réel Téléphone : Pour obtenir l'état et l'identité du téléphone Contacts

203 Politique de confidentialité de LionCash http://lioncash.co/privacy-policy/

	Informations recueillies auprès de l'utilisateur	Nom de l'utilisateur, titre du poste, nom de l'entreprise, adresse, adresse électronique, numéro de téléphone, sexe, âge, date de naissance, nationalité, associations professionnelles et numéros d'enregistrement, informations sur l'utilisation des produits LionCash par les utilisateurs, relevés d'argent mobile, informations bancaires ou de compte, informations de connexion des comptes de réseaux sociaux des utilisateurs, contacts téléphoniques dans l'appareil de l'utilisateur.
	Informations collectées à partir de l'appareil de l'utilisateur	Informations techniques : Type d'appareil mobile, adresse IP, système d'exploitation de l'appareil et identifiant de l'appareil. Ces informations sont collectées automatiquement à partir de l'appareil et des navigateurs web d'un utilisateur par le biais de cookies. Utilisation de l'application par l'utilisateur et consommation de la publicité numérique. Données de localisation : Collecte de la localisation précise en temps réel à partir de l'appareil d'un utilisateur.
	Informations reçues de tiers	Réception d'informations de la part de ses partenaires commerciaux, telles que le nom de l'utilisateur, le nom de l'entreprise, le titre du poste, l'adresse, l'adresse électronique et le numéro de téléphone, à des fins de vérification. Peut également recueillir des informations publiques ou commerciales auprès de tiers.
	Utilisation des informations de l'utilisateur par l'application	Fourniture de services Fourniture d'informations sur les produits et services Amélioration du site, de l'application, des produits et des services Marketing Défense contre des poursuites judiciaires, respect des lois et des décisions de justice, et prévention de la fraude.
	Informations partagées avec des tiers Durée de l'accès des tiers	Partage des informations sur les utilisateurs avec : Des prestataires de services Des partenaires commerciaux qui les aident à fournir des produits et services aux utilisateurs Les administrations, dans le cadre du respect des lois, des règlements et des ordonnances judiciaires, et de la prévention de la fraude Des partenaires commerciaux en cas de fusion, liquidation, dissolution, etc., Non indiqué
	Stockage des informations sur les utilisateurs	Stockage des informations sur les utilisateurs dans des bases de données et des serveurs situés hors du Kenya.
Timiza[204]	Informations collectées et traitées par l'application	

204 Conditions générales du compte Absa Timiza https://www.absabank.co.ke/content/dam/kenya/absa/pdf/Terms-of-use/timiza-account-terms-and-conditions.pdf

	Autorisations demandées	Demande l'accès aux : Données de localisation - pour accéder aux informations de localisation en temps réel Téléphone - pour obtenir l'état et l'identité du téléphone Contacts
	Informations recueillies auprès d'un utilisateur	
	Informations collectées à partir de l'appareil de l'utilisateur	
	Informations reçues de tiers	Obtient des informations auprès des organismes suivants : Safaricom : Y compris le numéro de téléphone de l'utilisateur, son nom, sa date de naissance, son numéro d'identité/de passeport, et toute autre information pertinente. Accède aux informations sur l'utilisation des services MPESA et des services Safaricom par l'utilisateur. Le système IPRS du gouvernement. Agence d'évaluation du crédit et partage des informations de crédit de l'utilisateur avec les agences.
	Utilisation des informations de l'utilisateur par l'application	Prestation de services Objectifs de marketing Amélioration du site, de l'application, des produits et des services Défense des revendications juridiques, respect de la loi et des ordonnances judiciaires, et prévention de la fraude
	Informations partagées avec des tiers/ Partage des informations personnelles	Les informations sur les utilisateurs sont partagées avec : leurs fournisseurs de services, concessionnaires et agents leurs conseillers professionnels, y compris les avocats et les auditeurs Pour Safaricom en ce qui concerne les services MPESA Les organismes d'application de la loi et les agences gouvernementales locales et internationales dans le cadre de la prévention de la fraude et de la poursuite d'activités criminelles.
	Stockage des informations de l'utilisateur par l'application	
O-Kash[205]	Informations collectées et traitées par l'application	

205 Politique de confidentialité de O-Kash https://ke.o-kash.com/kenya/en/privacy-policy/

	Autorisations demandées	Demande l'accès : - aux photos et médias sur l'appareil de l'utilisateur - à la localisation de l'appareil Numéro MPESA, numéro de téléphone, nom de l'emprunteur, âge, adresse électronique et autres informations de contact. Les coordonnées des contacts d'urgence peuvent être utilisées pour vérifier l'identité de l'utilisateur.
	Informations recueillies auprès de l'utilisateur	
	Les informations sont collectées auprès de l'utilisateur	La marque et le modèle de l'appareil, le système d'exploitation, les applications logicielles et un identifiant utilisateur unique. Les contacts du courrier électronique et du répertoire téléphonique, les historiques d'appels, les SMS et les informations de localisation GPS.
	Informations reçues de tiers	Collecte d'informations auprès des agences d'évaluation du crédit et des institutions financières.
	Utilisation des informations de l'utilisateur	Vérification et évaluation du crédit
	Informations partagées avec des tiers	Partage des informations des utilisateurs avec : l'agence d'évaluation du crédit Agences de recouvrement Organismes gouvernementaux et organismes chargés de l'application de la loi des conseillers professionnels des partenaires commerciaux lors de fusions, d'acquisitions et d'insolvabilités. Transfert des données des utilisateurs vers d'autres pays, y compris des pays qui n'ont pas de lois sur la protection des données.
	Stockage des informations sur l'utilisateur par l'application	

Étude de cas : O-Kash : L'humiliation subit à la suite des emprunts

O-Kash est connu pour avoir fait honte aux emprunteurs sur sa plateforme. L'application s'appuie sur les contacts de l'appareil de l'emprunteur et sur les coordonnées de la personne à contacter en cas d'urgence ou du référent de l'emprunteur.[206] Lors de son installation, l'application demande l'accès aux contacts de l'emprunteur et exige que celui-ci fournisse un contact d'urgence dès qu'il demande un prêt.[207]

Ses conditions générales prévoient que l'emprunteur consent expressément à ce que son référent soit contacté en cas de défaut de paiement de sa dette.[208] Sur cette base, l'application a appelé de manière agressive les référents et les contacts des emprunteurs

206 Politique de confidentialité de O-Kash https://ke.o-kash.com/kenya/en/privacy-policy/
207 Politique de confidentialité de O-Kash https://ke.o-kash.com/kenya/en/privacy-policy/
208 Article 8, Conditions générales d'O-Kash https://ke.o-kash.com/kenya/en/Terms-for-Kenya/

et, dans certains cas, les a menacés de payer leur dette.[209]

De tels actes constituent des violations de la vie privée de l'emprunteur. Ils sont contraires aux dispositions de la loi sur la protection des données, qui exige que les données personnelles des personnes concernées soient traitées dans le respect de leur droit à la vie privée.[210]

Analyse des pratiques de protection des données des applications de prêt numérique par rapport à la loi sur la protection des données, 2019.

La loi kenyane sur la protection des données contient des dispositions essentielles pour les pratiques de protection des données des applications de prêt numérique opérant au Kenya. La loi établit les principes qui doivent être observés par ces applications et leurs obligations concernant la vie privée et la protection des informations personnelles des emprunteurs. Cette section met en évidence les dispositions pertinentes de la loi afin d'établir si les applications sont conformes à ces dispositions.

Droit à la vie privée

La loi sur la protection des données exige que les responsables du traitement et les gestionnaires des données (dans ce cas, les applications de prêt numérique) traitent les données personnelles d'une manière qui respecte le droit à la vie privée de la personne concernée.[211] Dans ce cas, la loi impose aux applications de donner la priorité au droit à la vie privée des emprunteurs lors du traitement de leurs données.

Les applications de l'étude violent ce droit et traitent des données qui sont de nature intrusive et sans rapport avec la collecte de données. Par exemple, ces applications collectent des informations telles que les contacts stockés dans l'appareil d'un emprunteur, les informations de connexion aux plateformes de médias sociaux, la localisation précise en temps réel, entre autres, qui sont intrusives et excessives en ce qui concerne la finalité de la collecte des données. application telle qu'O-Kash est connue pour faire payer les emprunteurs pour leur dette en appelant et en harcelant leurs garants et en contactant les personnes répertoriées dans leurs appareils pour les obliger à payer leur dette. De tels actes portent atteinte à la vie privée des emprunteurs.

Légalité, équité et transparence

La loi sur la protection des données exige que ces applications traitent les données de manière licite, juste et transparente.[212] Cela signifie que les applications garantissent que les personnes concernées sont informées de manière claire et concise de la manière dont leurs données seront utilisées et que tous les paramètres de la loi sont respectés lors de ce traitement.[213] La loi exige également que les applications s'assurent que le consentement des emprunteurs a été obtenu avant de traiter leurs données.[214]

Dans ce cas, les applications doivent informer les utilisateurs des raisons pour lesquelles leurs données sont collectées, de la manière dont elles seront utilisées et, en cas de partage par des tiers, de l'identité des personnes avec lesquelles les données seront partagées et de la durée de conservation des données. Les applications étudiées peuvent être transparentes quant à la collecte des données des utilisateurs et à leur partage. Cependant, elles n'indiquent pas combien de temps les tiers auront accès aux données et combien de temps elles les conserveront.

209 Cette application de prêt vous fait honte publiquement lorsque vous êtes en retard dans le paiement de votre prêt https://restofworld.org/2020/okash-microlending-public-shaming/
210 Section 25 (a) de la loi sur la protection des données, 2019
211 Article 25 (a) de la loi sur la protection des données, 2019
212 Article 25 (b) de la loi sur la protection des données, 2019
213 Guide de protection des données de Privacy International
214 Article 30 (1), Loi sur la protection des données 2019

Limites de la finalité, pertinence et adéquation

Les applications de prêt numérique sont tenues, en vertu de la loi sur la protection des données, de traiter les données à caractère personnel conformément à la collecte des données. Ce qui signifie qu'elles ne doivent collecter des données que dans les limites du prêt numérique et non des données excessives. Les applications sont également tenues de collecter des données pertinentes, adéquates et uniquement nécessaires à la collecte des données.[215]

Les apps examinées collectent des informations non pertinentes et intrusives telles que ; les contacts des emprunteurs, les numéros de carte de crédit, les détails de connexion et les coordonnées des réseaux sociaux, les photos et les vidéos.

Partage des informations avec des tiers

La loi sur la protection des données stipule que ces applications doivent informer les utilisateurs sur le partage de leurs données avec des tiers, y compris les mesures de protection adoptées avant la collecte de ces données. [216]
Les applications examinées partagent des informations sur les utilisateurs/emprunteurs avec des agences d'évaluation du crédit, des partenaires commerciaux, des conseillers professionnels, des sociétés de télécommunications comme Safaricom, des organismes gouvernementaux et des organismes chargés de l'application de la loi, etc. et n'indiquent pas les mesures de sauvegarde adoptées pour protéger les données des emprunteurs. Les applications ne précisent pas non plus combien de temps ces parties auront accès aux données et combien de temps elles les conserveront.

Transfert de données personnelles hors du Kenya

La loi sur la protection des données prévoit que ces applications doivent veiller à ce que les données personnelles ne soient pas transférées hors du Kenya, sauf si des garanties adéquates pour la protection des données ont été mises en place et si le consentement de la personne concernée a été obtenu.[217] Elle stipule également que ces applications ne peuvent transférer des données que vers d'autres pays où elles ont apporté la preuve au commissaire indépendant à la protection de la vie privée que les garanties appropriées en matière de sécurité et de protection des données à caractère personnel ont été mises en place.[218] La loi stipule en outre que les applications ne peuvent transférer des données personnelles que vers d'autres pays où elles ont fourni au commissaire aux données la preuve des garanties de sécurité et de la protection des données personnelles et des garanties appropriées, y compris des juridictions ayant des lois de protection des données proportionnelles.[219]

La plupart des entreprises propriétaires des applications examinées sont établies hors du Kenya et disposent de bases de données et de serveurs stockant les informations personnelles des emprunteurs hors du Kenya. Cela crée un risque de sécurité pour les emprunteurs concernant leurs données. Par exemple, Tala, Branch et O-Kash ont leur siège hors du pays et stockent les informations personnelles des emprunteurs dans des serveurs situés hors du pays.[220]

Certaines applications stockent des données dans des pays qui n'ont pas de lois de protection des données comparables à celles du Kenya. O-Kash, par exemple, transfère

215 Article 25 (d), Loi sur la protection des données, 2019
216 Article 29 (d), Loi sur la protection des données 2019
217 Article 25 (h), Loi sur la protection des données 2019
218 Article 48 (a) de la loi sur la protection des données, 2019.
219 Article 48 (b), Loi sur la protection des données 2019
220 Politique de confidentialité de Tala : https://tala.co.ke/privacy-policy-ke/; Politique de confidentialité de Branch : https://branch.co.ke/pp; Politique de confidentialité de O-Kash : https://ke.o-kash.com/kenya/en/privacy-policy/

des données personnelles vers des pays qui n'ont pas le même niveau de protection des données que le Kenya.[221]

Protection de la vie privée dès la conception et par défaut

La loi sur la protection des données exige que ces apps mettent en œuvre des mesures techniques et organisationnelles appropriées conçues pour appliquer efficacement les principes de protection des données et intégrer les garanties nécessaires au traitement.[222] La loi prévoit en outre que ces applications doivent mettre en œuvre des mesures techniques et organisationnelles qui garantissent, par défaut, que seules les données personnelles nécessaires sont traitées.[223] La loi stipule que les applications doivent prendre en compte la quantité de données personnelles collectées, l'étendue du traitement, la période de stockage, l'accessibilité des données, ainsi que le coût du traitement des données et des technologies utilisées.[224]
Les applications étudiées auraient dû être conçues pour empêcher de collecter des informations superflues et se limiter à collecter uniquement ce qui est nécessaire pour les besoins du prêt numérique.

Droit d'accès et de suppression des données personnelles

Les emprunteurs ont le droit d'accéder à leurs données détenues par ces applications[225] et le droit de demander la suppression ou la destruction de leurs données que les applications ne sont plus autorisées à conserver, ou qui sont non pertinentes, excessives ou obtenues illégalement.[226]

Les applications, cependant, ne créent pas un espace où les emprunteurs peuvent exercer ces droits. Tala, par exemple, conserve les informations de l'utilisateur même après que celui-ci a désinstallé l'application.[227]

Mobilité des données

La loi donne aux personnes concernées le droit de recevoir leurs données dans un format structuré et lisible en machine.[228] Elle leur donne également le droit, lorsque cela est techniquement possible, de faire transmettre directement les données à d'autres responsables du traitement ou à des gestionnaires de données.[229] Les applications étudiées ne fournissent pas aux utilisateurs un moyen permettant de faire valoir ce droit.

Évaluation d'impact sur la protection des données (DPIA)

La loi exige qu'une évaluation d'impact sur la protection des données (AIPD) soit réalisée lorsque le traitement de données personnelles est susceptible d'entraîner un risque élevé pour les droits et libertés de la personne concernée.[230] Aucune des applications étudiées n'a réalisé une DPIA malgré la quantité importante de données.

Les applications de prêt numérique au Kenya peuvent traiter des données en contradiction avec la loi sur la protection des données de 2019. Leurs pratiques, par conséquent, portent atteinte à la vie privée des utilisateurs et à leur droit à la protection de leurs données. Le gouvernement devrait obliger ces applications à réviser leurs politiques de confidentialité pour se conformer à la loi sur la protection des données.

221 Politique de confidentialité de O-Kash, clause C
222 Article 41 (a) & (b), Loi sur la protection des données, 2019
223 Article 41 (3), Loi sur la protection des données, 2019
224 Ibid
225 Article 26 (b), Loi sur la protection des données, 2019
226 Politique de confidentialité de Tala https://tala.co.ke/privacy-policy-ke/
227 Politique de confidentialité de Tala https://tala.co.ke/privacy-policy-ke/
228 Article 38 (1), Loi sur la protection des données, 2019
229 Article 38 (3), Loi sur la protection des données, 2019
230 Article 31 (1), Loi sur la protection des données, 2019

Mali

Profile du pays

Pays francophone enclavé d'Afrique de l'Ouest, la République du Mali a pour frontières la Mauritanie, l'Algérie, le Niger, le Burkina-Faso, la Côte d'Ivoire, la Guinée et le Sénégal. Comptant plus de 19 millions d'habitants, elle a un PIB de 17,28 milliards USD (2019) et est soutenue par un régime semi-présidentiel.[231] En mai 2013, le gouvernement malien a promulgué la loi n° 2013-015 relative à la protection des données personnelles en République du Mali.[232] La loi s'applique aux traitements automatisés ou non automatisés réalisés en tout ou partie sur le territoire du Mali.[233] L'Autorité de Protection des Données à Caractère Personnel (APDP) est l'APD du Mali.[234] Sa mission principale est de protéger les données personnelles et de réguler le secteur numérique de la République du Mali.

231 La constitution du 25 février 1992 indique que le Mali repose sur un régime semi-présidentiel. En effet, ladite constitution consacre la séparation des pouvoirs et la responsabilité du Gouvernement devant l'Assemblée nationale (article 54, 78 et 79). Cf : https://mjp.univ-perp.fr/constit/ml1992.htm#3

232 Loi no 2013-015 du 21 mai 2013 relative à la protection des données personnelles https://apdp.ml//wp-content/uploads/pdf/Loi-sur-la-protection-des-donnees-personnelles-du-21-mai-2013.pdf 2 mai 2021.

233 Article 4 de la loi n° 2013-015

234 Site web : https://apdp.ml/

Protection des données au Mali

Avec le développement du transfert de données de mobile à mobile et la transaction de données, de nouveaux services, jusqu'alors inexploités, ont vu le jour. L'un de ces nouveaux services est le crédit numérique, qui fait partie des services financiers numériques de deuxième génération. Il permet de fournir aux individus des prêts instantanés pour leurs besoins particuliers - une alternative au crédit traditionnel qui connaît un grand succès dans les pays anglophones d'Afrique.

Dans les pays francophones, notamment en Afrique de l'Ouest, les premières expériences de crédit digital ont débuté en 2018 avec l'offre « Momo Kash » de MTN & Bridge Bank en Côte d'Ivoire et au Mali avec Singa Ni Mara[235] de la Première Agence de Microfinance (PAMF-M) et Orange au Mali. Conscient de la flexibilité potentielle de ce type d'offre, un autre

235 SINGA NI MARA est une offre d'épargne et de pico / micro-crédit aux particuliers, en partenariat avec l'institution de microfinance PAMF (Première Agence de Microfinance) lancée le mercredi 13 juin 2018. Elle permet aux personnes de bénéficier instantanément de produits de crédit et d'épargne, les aidant ainsi à gérer rapidement et facilement les dépenses imprévues ou à épargner. Elle est accessible via un code USSD pour les clients Orange Money d'Orange Mali et passe par son application mobile Orange Mali Sugu.

service de micro-assurance va se développer entre la start-up OKO[236][237] et Orange Mali. Cette offre s'appuie sur des données satellitaires et des services de transfert d'argent mobile pour concevoir des produits d'assurance automatisés pour les agriculteurs. Comme pour l'offre Singa Ni Mara, l'offre Oko est accessible sur les téléphones mobiles des populations à l'aide d'un code USSD et sur l'application mobile Orange Money Mali : Orange Mali Sugu. Une application mobile qui en plus des données collectées avec les comptes Orange Money Mali associés également à ceux d'Oko et de Singa Ni Mara, offre un grand volume de données, dont le traitement peut comporter des risques potentiels pour le respect de la vie privée de ces utilisateurs et qui doit être analysé. Surtout, ce type de traitement de données basé sur des applications mobiles a commencé après l'adoption de la loi sur la protection des données personnelles au Mali. Par conséquent, il est essentiel de savoir si les pratiques de traitement des données de l'application mobile Orange Mali Sugu, telles que définies dans sa politique et ses conditions d'utilisation, tiennent compte de la réglementation sur la protection de la vie privée.

Cette étude vise à analyser les politiques de confidentialité et les termes et conditions de ces applications et à examiner leur conformité avec la loi sur la protection des données au Mali. La première partie comprend un aperçu des données collectées par ces applications. La deuxième partie examine leurs activités de traitement au regard de la loi sur la protection des données personnelles. La dernière partie se termine en indiquant si ces applications sont conformes ou non à la loi sur la protection des données personnelles.

Aperçu des données collectées par les applications de prêt numérique

Orange Mali Sugu[238] Lien de téléchargement : Google Play Store et Apple Store	Informations collectées et traitées par l'application	
	Autorisations demandées	Au démarrage, Orange Mali Sugu demande : - de gérer les appels des utilisateurs - d'accéder aux SMS d'un utilisateur : Il affiche les SMS d'un utilisateur pour collecter des informations financières et des données de transaction afin de recueillir des informations sur l'historique financier d'un utilisateur et de déterminer sa solvabilité. Accéder aux contacts de l'utilisateur Accéder aux données de localisation, d'appareil et d'utilisation : Orange Mali Sugu utilise la technologie GPS ou d'autres services de localisation pour déterminer l'emplacement actuel d'un utilisateur.
	Informations recueillies auprès de l'utilisateur	During registration, Orange Mali Sugu collects the user's information: name, address, email address and phone number, device phone number, SIM card, age, username, password, financial and credit data, descript personal ion and photograph, and other registration

236 https://fr.oko.finance/mali
237 L'offre d'assurance agricole OKO a été lancée le mardi 21 janvier 2020

238 L'application Orange Money Sugu ne dispose pas d'une politique de confidentialité des données personnelles. Ne sont disponibles, que les conditions d'utilisation Orange Money Mali qui abordent au point 12 la question du traitement des données.

	Informations collectées à partir de l'appareil de l'utilisateur Informations collectées lors de l'utilisation du site web Orange Mali website	Orange Mali Sugu collecte les informations suivantes à partir de l'appareil de l'utilisateur : Technique d'intelligence artificielle (IA) : modèle d'appareil mobile, numéro IMEI ou numéro de série de l'appareil, informations sur la carte SIM, informations sur le réseau mobile, système d'exploitation de l'appareil, type de navigateur, emplacement de l'appareil et réglage du fuseau horaire. Informations stockées dans l'appareil : liste de contacts, historique des appels, historique des SMS, contacts des comptes de médias sociaux, photos, vidéos ou tout contenu numérique pertinent. Dès qu'un utilisateur utilise le site Web d'Orange Mali sur son téléphone mobile, Orange Mali Sugu collecte automatiquement les informations suivantes et les stocke dans ses fichiers Journaux : L'adresse IP de l'utilisateur, le type de navigateur, le fournisseur d'accès à Internet (FAI), les pages de renvoi/de sortie, le système d'exploitation, l'horodatage et le support de navigation. Ces informations sont ensuite regroupées pour des raisons d'analyse ou de marketing et sont mises à la disposition d'Orange Money Mali, d'Oko Israël et de PAMF.
	Informations reçues de tiers	Des informations ont été obtenues auprès d'autres entités du groupe Orange : Orange Money Mali et Orange Finances Mobile Mali, Bureaux d'information de crédit (BIC), fournisseurs de réseaux mobiles et agences de recouvrement.
	Utilisation des informations de l'utilisateur par l'application	Les conditions d'utilisation d'Orange indiquent qu'elle collecte les données des utilisateurs aux fins suivantes : . le traitement des transactions d'un utilisateur . Vérification de l'identité d'un utilisateur . Décaissements de prêts et collecte de paiements scoring . Crédit et création de modèles de crédit . analyse du comportement de l'emprunteur . Responsabilités de l'application Orange Mali Sugu envers les utilisateurs . respect des lois et règlementation relatives à la connaissance du client et à la lutte contre le blanchiment d'argent. . prévention des fraudes, . Services de marketing

	Informations partagées avec des tiers	Orange Mali Sugu partage les informations des utilisateurs avec : Ses membres, agents, prestataires de services, les entités du groupe Orange Money, et les entités qui sous-traitent les données collectées. - Toute personne agissant pour le compte d'un utilisateur - les institutions financières, les bureaux d'information sur le crédit et les agences (BIC) - Des partenaires commerciaux en cas de transfert d'entreprise, de cession, de fusion et d'acquisition, etc. Prestataires de services tiers Organismes chargés de l'application de la loi (l'Autorité pour la protection des données personnelles (APDP)), fonctionnaires du gouvernement, sur la base de : Une demande ou une décision formelle de la justice Respect de la loi ou signalement d'une activité illégale présumée
	Durée de l'accès aux données par des tiers	La politique ne donne aucune indication sur la durée pendant laquelle les tiers peuvent accéder aux informations personnelles des utilisateurs et les conserver.
	Technologies de suivi / Cookies du site web	Orange Mali Sugu utilise une technologie de suivi mobile et des cookies de site web pour distinguer les utilisateurs de l'application.
	Stockage des informations sur l'utilisateur par l'application	Orange Mali Sugu stocke les informations relatives aux utilisateurs hors du Mali. Les données peuvent également être traitées par Orange Money Mali, le personnel d'Orange Mali. Aucune précision n'est également donnée concernant la durée de conservation des données par Orange Mali.

Étude de cas : Orange Mali Sugu (La question de la durée de conservation des données des utilisateurs)

Les conditions d'utilisation des comptes Orange Money Mali associés aux applications Orange Mali Sugu ne détaillent pas la durée de conservation des données des utilisateurs. Ce défaut constitue une violation de la loi relative à la protection des données au Mali, qui exige que les données soient collectées pour une durée déterminée.[239] En outre, l'application Orange Mali Sugu ne dispose pas d'une politique de confidentialité spécifique.

Analyse des pratiques de protection des données des applications de prêts numériques au regard de la loi relative à la protection des données personnelles.

La loi malienne sur la protection des données personnelles a clairement défini les obligations en matière de lois sur la vie privée, applicables à tout traitement, qu'il soit automatique ou non[240]. Par là même, les applications numériques de prêts. Cependant, en raison de leur développement récent, les risques pour la protection de la vie privée sont actuels. Cette section met en évidence les dispositions pertinentes de la loi afin d'établir si ces applications sont conformes à ces dispositions.

239 Article 15 de la loi n° 2013-015
240 Article 5 et 6 de la loi n° 2013-015

Droit à la vie privée

La loi sur la protection des données exige que les responsables du traitement et les gestionnaires des données (dans ce cas, les applications de prêt numérique) traitent les données personnelles d'une manière qui respecte le droit à la vie privée.[241] En l'occurrence, la loi demande aux applications de veiller à ce que le droit à la vie privée des emprunteurs soit prioritaire lors du traitement de leurs données. Les applications étudiées violent ce droit et traitent les données de manière intrusive et sans rapport avec l'objectif de la collecte des données. Par exemple, ces applications collectent des informations telles que les contacts stockés sur l'appareil d'un emprunteur, les informations de connexion des plateformes de médias sociaux et la localisation précise en temps réel, ce qui est intrusif et excessif concernant la collecte de données.

Légalité, équité et transparence

La législation sur la protection des données exige que ces applications traitent les données de manière légale, loyale et transparente.[242] Cela implique que les applications veilleront à ce que les personnes concernées soient informées clairement de la manière dont leurs données seront utilisées et que tous les paramètres de la loi soient respectés dans ce traitement.[243]

Dans ce cas, les applications devraient informer les utilisateurs des raisons pour lesquelles leurs données sont collectées, de la manière dont elles seront utilisées et, si elles sont partagées avec des tiers, des personnes avec lesquelles elles seront partagées et de la durée de conservation des données. On peut dire que les applications étudiées sont transparentes quant aux raisons pour lesquelles elles collectent les données des utilisateurs et avec qui elles les partagent. Cependant, elles n'indiquent pas pendant combien de temps les tiers auront accès aux données et combien de temps elles les conserveront.

Limitation de l'objectif, pertinence et adéquation

Les applications de prêt numérique sont tenues, en vertu de la loi sur la protection des données, de traiter les données personnelles après leur collecte.[244] Cela signifie qu'elles ne doivent collecter que des données qui ne concernent que le prêt numérique et non des données excessives. Les applications ne doivent collecter que des données pertinentes, adéquates et limitées à la collecte de données.[245]
Orange Mali Sugu collecte des informations personnelles qui ne sont pas pertinentes pour l'objectif de la collecte de données. Elles contiennent des informations sur les emprunteurs telles que des numéros de carte de crédit, des transactions financières, des informations sur les comptes de connexion aux réseaux sociaux, des contacts sur les réseaux sociaux, des contacts téléphoniques, des photos et des vidéos, etc. qui ne sont pas pertinentes dans le cadre du prêt numérique.

Partage d'informations avec des tiers

La loi malienne sur la protection des données stipule que ces applications doivent informer les utilisateurs des tiers avec lesquels leurs données seront partagées, y compris les mesures adoptées pour protéger leurs données avant leur collecte.[246] Dans le cas spécifique de l'application Orange Mali Sugu, l'absence de durée déterminée pour le traitement des données constitue une violation du droit à la vie privée.[247]

241 Article 8 de la loi n° 2013-015
242 Article 7 de la loi n° 2013-015
243 Article 15 de la loi n° 2013-015
244 Article 15 de la loi n° 2013-015
245 Article 15 de la loi n° 2013-015
246 Article 11 et 15 de la loi n° 2013-015
247 Article 8 de la loi n° 2013-015

Les avis de l'application Orange Mali Sugu partagent les informations relatives à l'utilisateur/emprunteur avec le bureau d'information sur le crédit (BIC), les partenaires commerciaux, les conseillers professionnels, le gouvernement et les organismes d'application de la loi, etc. Elles n'indiquent pas les mesures de protection adoptées pour protéger les données des emprunteurs. Elles n'indiquent pas non plus combien de temps ces parties auront accès aux données et combien de temps elles les conserveront.

Mali Transfert de données personnelles hors du Mali

Disposition respectée par les différents fournisseurs d'applications

Confidentialité par conception et par défaut

La loi prévoit que le responsable du traitement doit prendre toutes les dispositions pour traiter les données des utilisateurs[248]. L'application Orange Mali Sugu dispose de mesures de cryptage pour protéger les communications et le contenu privé de ses utilisateurs. Un niveau de sécurité est nécessaire pour protéger les données des utilisateurs. Cependant, le niveau de protection inclus ne peut empêcher le fournisseur d'application de collecter des informations superflues.

Droit d'accès et de suppression des données personnelles

Les utilisateurs des applications Orange Mali Sugu ont le droit d'accéder à leurs données détenues par ces applications[249] et ont le droit de demander l'effacement ou la destruction de leurs données que les applications ne sont plus autorisées à conserver. Les utilisateurs ont également le droit de demander la suppression des données non pertinentes, superflues ou obtenues illégalement.[250]

Mobilité des données

La loi donne aux personnes concernées le droit de recevoir leurs données dans un format structuré et lisible en machine[251]. Il leur donne également le droit, lorsque cela est techniquement possible, de faire transmettre les données directement à d'autres responsables de traitement ou gestionnaires de données.[252] L'application Orange Mali Sugu ci-dessus examinée ne fournit pas aux utilisateurs un moyen d'exercer ce droit.
Évaluation d'impact sur la protection des données (DPIA)
La loi exige qu'un rapport sur le processus de traitement des données soit produit annuellement et envoyé à l'Autorité de protection des données personnelles (APDP).
En outre, les autorisations de transfert de données ont indiqué la nécessité pour les contrôleurs de données d'effectuer une évaluation d'impact sur la protection des données (DPIA). Cependant, Orange Mali Sugu n'a pas produit ou mis à disposition leurs rapports.

Conclusion

Les pratiques de traitement des données des demandes de crédit numérique au Mali ne respectent pas les principes de base de la loi sur la protection de la vie privée. Des évaluations d'impact sur la protection des données (EIPD) doivent être exigées pour contraindre les responsables du traitement de ces applications à respecter strictement les obligations légales en la matière. Par ailleurs, une révision de la loi n° 2013-015 du 21 mai 2013 relative à la protection des données personnelles doit être envisagée, compte tenu des risques potentiels pour la vie privée. Au-delà, il est également nécessaire que l'APDP du Mali se dote d'une expertise et d'un équipement technique pour contrôler en temps réel le volume, la qualité et la quantité de données collectées par ces gestionnaires de données pour le traitement des applications mobiles.

248 Article 8 de la loi n°. 2013-015
249 Article 12,13,14,18 et 18 de la loi n° 2013-015
250 Articles 12, 13, 14, 18 et 18 de la loi n° 2013-015.
251 Article 12 de la loi n° 2013-015
252 L'article 12 de la loi n° 2013-015

Maroc

Profil du pays

Le Royaume du Maroc est situé au nord-ouest de l'Afrique et compte une population de plus de 37 millions[253] d'habitants avec un PIB estimé à 117 milliards de dollars US en 2021.[254] Le pays pratique un système de gouvernement monarchique unitaire avec un parlement élu. Selon la Banque africaine de développement (2018), l'économie marocaine est considérée comme la plus robuste d'Afrique. Le secteur des services domine l'économie marocaine, contribuant à environ 55 % du PIB.[255]

253 Atlas monde https://www.atlas-monde.net/afrique/maroc/ consulté le 23 août 2021.
254 Trading Economics https://tradingeconomics.com/morocco/gdp consulté le 25 août 2021.
255 https://thefintechtimes.com/fintech-africa-morocco/ > consulté le 25 août 2021.

Protection des données au Maroc

Selon Freedom House (2020), la liberté d'Internet au Maroc se caractérise par son caractère précaire, alors que la répression à l'encontre des journalistes en ligne couvrant les manifestations se poursuit et que les sites d'information pro-gouvernementaux publient de fausses informations sur les militants et les journalistes. Alors que l'accès à Internet augmente globalement, le gouvernement maintient des systèmes de surveillance sophistiqués.[256]

La loi marocaine sur la protection des données a été promulguée le 18 février 2009.[257] Elle s'applique au traitement des données à caractère personnel effectué en tout ou en partie par des moyens automatisés et au traitement non automatisé des données à caractère personnel contenues ou destinées à être contenues dans des fichiers manuels.[258] Le pays dispose d'une agence de protection des données - la APD - la Commission nationale de supervision de la protection des données personnelles (CNPD)[259] a été créée par décret le 21 mai 2009.

Système financier et Fintech au Maroc

Les banques placées sous la responsabilité de la Banque centrale du Maroc (Bank Al Maghreb - BAM),[260] représentent près de la moitié du système financier du pays.[261] Sur les 19 banques, les trois premières sont responsables de plus des deux tiers de tous les

256 Freedom House 2020 https://freedomhouse.org/country/morocco/freedom-net/2020 consulté le 25 août 2021.
257 Loi 09-08 du 18 février 2009 https://www.cndp.ma/images/lois/Loi-09-08-Fr.pdf consulté le 10 mai 2021.
258 Loi 09-08 du 18 février 2009, chapitre I, section 1, art.2.
259 https://www.cndp.ma/fr/ consulté le 24 août 2021.
260 https://www.bkam.ma/ > consulté le 24 août 2021.
261 https://thefintechtimes.com/fintech-africa-morocco/ > consulté le 22 août 2021.

actifs et dépôts bancaires. Depuis 2007, la BAM a fait des efforts notables pour améliorer l'inclusion financière.[262]

En 2014, un nouveau cadre a été élaboré (n° 103-12) publié au Journal Officiel en mars 2017 (loi bancaire).[263] Il s'applique aux institutions (y compris les banques islamiques participantes) : recevant des fonds du public, effectuant des opérations de crédit, mettant à la disposition de la clientèle de tout moyen de paiement ou de gestion.

La loi crée deux catégories de prestataires financiers, ce qui accroît la concurrence dans le domaine des services de paiement. Un nouveau type, vaguement traduit par "banque participative", permet aux institutions non bancaires d'offrir des services de paiement permettant des transferts de fonds et des retraits de comptes de paiement.

Selon Fintechnews Middle East (avril 2021)[264], le Maroc est le troisième pôle fintech du monde arabe, accueillant 13% des 400 solutions fintech actives, soit environ 40 solutions fintech. Maroc s'élevait à seulement 28,6% en 2017, et que l'économie reste principalement basée sur le cash, avec environ 80% des transactions effectuées en espèces.

Un niveau élevé de couverture mobile soutiendrait l'écosystème Fintech du Maroc. Fintech News Middle East a d'abord rapporté que sur les 40 solutions Fintech actives au Maroc, les systèmes de paiement, de transfert de fonds et de point de vente (POS) constituent le segment le plus développé.[265] Parmi les autres formes de Fintech qui gagnent en popularité figurent le crowdfunding, les services financiers personnels, les plateformes de prêt et l'analyse avancée des données. Par exemple, Cotizi serait la première plateforme de crowdfunding du pays.[266]

Wafacash/Jibi : L'application mobile de prêt d'argent

Jibi[267] est une application d'argent mobile disponible 24 heures sur 24 et 7 jours sur 7 qui permet aux clients d'effectuer des transactions à partir d'Internet ou du mobile de l'utilisateur. Avec Jibi, les clients peuvent : régler leurs achats à l'aide de leur téléphone mobile auprès d'un vaste réseau de commerçants ; déposer et retirer de l'argent où et quand ils le souhaitent grâce à notre vaste réseau d'agences Wafacash et d'agents de détail dans tout le Maroc.

Il permet également d'envoyer de l'argent depuis son téléphone vers un compte mobile Jibi, un compte bancaire ou une agence Wafacash. Il est également possible de recevoir un transfert d'argent depuis l'une des agences Wafacash, de payer des factures ou de faire des achats en ligne sans avoir à communiquer ses coordonnées bancaires ou à recharger son téléphone portable.

En partenariat avec Wafasalaf, Wafacash propose un crédit à la consommation qui permet de financer à court terme tout projet ou dépense. Wafacash propose des solutions pour répondre aux besoins de ses clients, allant du crédit au microcrédit en collaboration avec Wafasalaf et Al Amana Micro Finances - elle agit comme une application de prêt.[268]

---

262 Idem

263 Loi n° 103-12 - relative aux établissements de crédit et organismes assimilés (loi bancaire) https://dfsobservatory.com/sites/default/files/Parliament%20of%20Morocco%20-%20Law%20No.%20103-12%20-%20On%20Credit%20Institutions%20and%20Similar%20Business%20%28Banking%20Law%29.pdf > consulté le 22 août 2021.

264 Article https://www.moroccoworldnews.com/2021/01/331921/cmi-chief-moroccos-2020-e-commerce-transactions-rose-43/ consulté le 22 août 2021.

265 Article https://www.crowdfundinsider.com/2021/04/174365-morocco-is-now-home-to-many-fintech-services-crowdfunding-lending-advanced-data-analytics-platforms-report/ consulté le 22 août 2021.

266 http://www.cotizi.com/ consulté le 22 août 2021.

267 Disponible sur Google Play - https://play.google.com/store/apps/details?id=com.b3g.wafacash.jibi&hl=fr&gl=US et iOs - https://apps.apple.com/fr/app/jibi-pro/id1371478054

268 https://www.wafacash.com/cr%C3%A9dit-micro-cr%C3%A9dit / https://www.alamana.org.ma/fr/alamana/tout-savoir-sur-le-micro-credit > consulté le 23 août 2021.

Aperçu des données collectées par les applications de prêt numérique

Wafacash/Jibi[269]	Aperçu des données collectées par les applications de prêt numérique[270]	
	Autorisations demandées	Trouver des comptes sur l'appareil Trouver des comptes sur l'appareil Prendre des photos et des vidéos Afficher les connexions Wi-Fi Lire le statut et l'identité du téléphone Lire le contenu de la mémoire USB du client Modifier ou supprimer le contenu de la mémoire USB du client.
	Informations recueillies auprès de l'utilisateur	Données personnelles : titre, nom, prénom Numéro de téléphone Opérateur téléphonique Adresse électronique
	Informations recueillies à partir de l'appareil de l'utilisateur	Localisation approximative (sur réseau) Localisation précise (GPS et réseau) Lire l'état et les informations sur le modèle du telephone La responsabilité du client est de protéger adéquatement son appareil mobile, de sauvegarder ses données et son matériel, et de prendre des précautions adéquates et raisonnables pour détecter les virus et autres éléments destructeurs. Wafacash ne sera pas responsable des pertes que le client pourrait subir en raison des événements ci-dessus. Toutes les opérations effectuées par le client via l'Application Mobile Jibi et le Site Internet Jibi, qui ont été authentifiés, sont considérées comme effectuées par le client. Le client accepte expressément et s'engage à ne pas contester.

269 https://www.wafacash.com/mentions-legales > consulté le 22 août 2021.
270 Conditions générales (adoptées le 4 juillet 2018) https://www.jibi.co.ma/DocReadme/CG_JIBI_VF_04072018_Valide.pdf /

	Informations recueillies lors de l'utilisation du site web de Jibi	L'accès au site www.wafacash.com est illimité et ouvert à tous. Wafacash se réserve le droit, en raison de l'évolution permanente de l'internet et des produits et tarifs, de modifier ou de supprimer, à tout moment et sans préavis, les conditions d'utilisation proposées et les informations présentes sur le site www.wafacash.com. Suite à la loi 09-08 relative à la protection des personnes par rapport au traitement des données à caractère personnel, il est porté à l'attention de l'utilisateur qu'en acceptant les conditions générales, l'utilisateur du site reconnaît que ses données feront l'objet d'un traitement informatique. En tout état de cause, wafacash ne collecte des informations personnelles relatives à l'utilisateur que pour le besoin de certains services proposés par le site www.wafacash.com. L'utilisateur fournit ces informations en toute connaissance de cause lorsqu'il les saisit.
	Informations reçues de tiers	Les informations recueillies font l'objet d'un traitement informatique. Elles sont destinées à Wafacash, son groupe et leurs filiales respectives, qui, de convention expresse, sont autorisées à procéder à leur traitement automatisé ou non, à les communiquer aux personnes morales de leur groupe, à leurs partenaires, et à leurs prestataires de services. Wafacash, son groupe et leurs filiales respectives s'engagent à n'utiliser les informations recueillies que pour satisfaire aux obligations légales et réglementaires. Elles pourront également être utilisées pour tenir le client informé des nouvelles offres, événements, actions ou publications susceptibles de l'intéresser.
	Utilisation des informations de l'utilisateur par l'application	Recevoir des données de l'internet Simuler des sources de localisation pour les tests Visualiser les connexions réseau Accès complet au réseau Empêcher l'appareil de passer en mode veille Lire la configuration des services Google

	Informations partagées avec des tiers	Les informations personnelles collectées sont destinées aux services de Wafacash chargés de répondre aux demandes des clients pour la gestion des demandes RH, des plaintes et réclamations, et des demandes de partenariat. Elles sont utilisées par Wafacash, le Groupe[271] Attijariwafa Bank et leurs partenaires et pourront être communiquées à toute autorité administrative ou judiciaire ayant le droit de les transmettre.
	Durée de l'accès des tiers	Les conditions générales sont établies pour une durée indéterminée. Elles entrent en vigueur à partir du moment où le client signe la convention de compte. Wafacash se réserve le droit de modifier les conditions générales, d'en ajouter ou d'en supprimer, pour mieux répondre à la satisfaction des clients et aux évolutions législatives, réglementaires et techniques.
	Technologies de suivi/ cookies de site web	L'utilisation des fonctionnalités du site www.wafacash.com peut nécessiter l'utilisation de cookies. Le site www.wafacash.com utilise des cookies pour mémoriser les préférences choisies par un utilisateur lors de sa visite du site pour recueillir des statistiques et de mesures d'audience.

Conclusion

Le Maroc est l'un des pays qui a connu une expansion rapide des plateformes numériques dans le secteur financier et des transactions. Notre recherche note que le contexte du pays dispose d'un cadre juridique suffisamment organisé et clair sur la manière dont ces services/applications numériques doivent fonctionner. En fait, depuis 2007, la Banque centrale du Maroc (Bank Al Maghreb - BAM) a fait des efforts notables pour améliorer l'inclusion financière. En 2014, elle a élaboré un nouveau cadre (n° 103-12), publié en mars 2017 (loi bancaire).

L'une des principales conclusions est liée à l'existence d'applications numériques qui, dans leur majorité, ne sont pas initialement réglementées au Maroc, puisque des entreprises étrangères en font la création. D'autre part, on note l'absence de cas concrets. L'Agence de protection des données a déjà agi pour sauvegarder les droits des utilisateurs, même après avoir annoncé des cas de vol de données de clients sur Internet en juillet de cette année.[272]

271 https://www.attijariwafabank.com/fr consulté le 25 août 2021.
272 Article https://www.zdnet.fr/actualites/un-pirate-accuse-de-fraude-bancaire-arrete-au-maroc-39925899.htm > consulté le 25 août 2021.

Mozambique

Profil du pays

Maputo est la capitale du Mozambique. Le pays compte plus de 30 millions d'habitants, et le portugais est la langue officielle.[273] Le Mozambique est situé en Afrique australe, et l'Eswatini le lie au sud.[274] Selon les modèles macroéconomiques mondiaux de Trading Economics et les prévisions des analystes, le PIB devrait atteindre 14,30 milliards USD d'ici la fin de l'année 2021.[275]

273 http://www.ine.gov.mz/iv-rgph-2017/mocambique/censo-2017-brochura-dos-resultados-definitivos-do-iv-rgph-nacional.pdf/view > consulté le 15 juillet 2021.
274 https://www.britannica.com/place/Mozambique consulté le 17 juillet 2021.
275 https://tradingeconomics.com/mozambique/gdp consulté le 17 juillet 2021.

Protection des données au Mozambique

Le préambule de la Constitution mozambicaine de 2004, telle que modifiée, souligne la nécessité du pluralisme d'opinion, du respect et de la garantie des droits fondamentaux de l'homme.[276] L'article 48 prévoit le droit à la liberté d'expression, à la presse et à l'accès à l'information qui ne doit pas être censuré. L'Inclusive Internet Index 2020[277], qui évalue la disponibilité, l'accessibilité, la pertinence et l'état de préparation de l'internet, classe le Mozambique 94e sur 100 pays. Selon l'indice, les faibles scores du Mozambique sur les quatre critères d'évaluation sont dus à un faible niveau d'alphabétisation, à un approvisionnement en électricité et à une infrastructure de réseau inadéquats.[278]

.Le Mozambique est actuellement classé 45e sur 61 pays en matière d'accessibilité à l'internet.[279] Il n'existe toujours pas de législation spécifique sur la protection des données et de la vie privée. Les principes directeurs sont fournis par la constitution, le code civil et plusieurs textes de loi sectoriels qui réglementent la protection des données dans des secteurs spécifiques. En 2020, de nouveaux amendements[280] au code pénal mozambicain[281] ont été introduits pour protéger la vie privée. The Media Le Media Institute of Southern Africa (MISA) Mozambique a rencontré le gouvernement mozambicain pour discuter des efforts de collaboration en matière de cybersécurité et de protection des données au cours

276 https://cdn.accf-francophonie.org/2019/03/mozambique_const-en.pdf > consulté le 19 juillet 2021.
277 https://theinclusiveinternet.eiu.com/ > consulté le 22 juillet 2021
278 https://theinclusiveinternet.eiu.com/explore/countries/MZ/?category=affordability > consulté le 24 juillet 2021.
279 https://a4ai.org/affordability-report/report/2019/#annexes > consulté le 25 juillet 2021.
280 https://advox.globalvoices.org/2020/01/17/new-privacy-law-in-mozambique-threatens-freedom-of-expression-activists-say/ consulté le 26 juillet 2021.
281 https://acjr.org.za/news/mozambique-promulgates-new-penal-code consulté le 27 juillet 2021.

de cette période.[282]

Le 26 juin 2018, le Mozambique a signé la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel[283] ("la Convention de l'UA"). Le Mozambique n'a pas encore ratifié la Convention de l'UA, ce qui pourrait indiquer une tendance générale quant à la manière dont un cadre de protection des données pourrait se développer dans la juridiction.[284]

Système financier et Fintech au Mozambique

Le secteur financier au Mozambique est réglementé par la Banque centrale (Banco de Moçambique).[285] La loi n° 14/2013 du 12 août établit[286] le régime juridique de prévention et de répression de l'utilisation du système financier pour la pratique d'actes de blanchiment de capitaux, de biens, de produits ou de droits dérivés d'activités criminelles définies par cette loi, et cela s'applique aux applications mobiles Money Leading. L'article 17 de la loi stipule que les institutions financières et les entités financières couvertes par la loi sont tenues de conserver les documents d'identification et de transaction pendant 15 ans à compter de la date de clôture des comptes des clients respectifs ou de la résiliation du contrat.
La même loi est réglementée par le décret 66/2014 du 29 octobre. Dans son article 2, le décret stipule que toutes les institutions financières, banques ou entités d'application mobile, doivent exiger au moins l'identification des clients, qui est attestée par la carte d'identité ou un document équivalent au Mozambique.[287] En 2020, le Mozambique a adopté la loi n° 20/2020 du 31 décembre, qui établit les établissements de crédit et les sociétés financières.[288] La loi sur les transactions électroniques (loi n° 03/2017, du 9 janvier), par exemple, prévoit des exigences liées au commerce électronique.[289]

M-Pesa : L'application mobile de prêt d'argent

M-Pesa[290] est le plus grand service financier mobile du Mozambique. Il permet aux clients de transférer et de retirer de l'argent, d'acheter du crédit, de payer l'électricité et d'effectuer des transactions pour des services par le biais de téléphones mobiles.[291] It was established on 16 January 2013 and is subject to regulation by the Bank of Mozambique. C'est Vodafone M-Pesa SA qui a créé ce service.[292] Il a été créé le 16 janvier 2013 et est soumis à la réglementation de la Banque du Mozambique. On ne sait pas exactement combien de clients utilisent l'application. Récemment, M-Pesa a lancé un service appelé "Txuna", qui sera au centre de nos recherches. Txuna M-Pesa est un service financier - une application mobile de prêt d'argent qui permet aux clients d'emprunter de l'argent à la banque et de recevoir de l'argent mobile via M-Pesa sans avoir besoin d'un compte bancaire. Le service est offert à tous les clients de Vodacom qui possèdent un compte M-Pesa actif depuis trois mois.
Pour demander un prêt, le client doit accéder au menu M-Pesa en utilisant *150# ou choisir l'option "Txuna M-Pesa" via l'application, puis suivre les étapes. Les prêts peuvent être remboursés en 7 jours (avec 10% de frais de service), 14 jours (avec 12% de frais de service) et 30 jours (avec 15% de frais de service). Le service fonctionne avec deux banques

282 Rapport des médias https://www.misa.org.mz/index.php/destaques/noticias/85-government-and-misa-mozambique-explore-synergies-for-cyber-security > consulté le 27 juillet 2021.
283 https://platform.dataguidance.com/legal-research/african-union-convention-cyber-security-and-personal-data-protection-27-june-2014-0 consulté le 25 juillet 2021.
284 https://www.dataguidance.com/jurisdiction/mozambique, consulté le 26 juillet 2021.
285 https://www.salcaldeira.com/index.php/pt/component/docman/cat_view/32-legislacao/77-bancario, consulté le 24 juillet 2021.
286 http://www.minec.gov.mz/index.php/documentos/legislacao/131-lei-14-2013-lei-de-branqueamento-de-capitais/file, consulté le 24 juillet 2021.
287 Loi n°66/2014, du 29 octobre
288 https://www.salcaldeira.com/index.php/pt/publicacoes/artigoss/doc_download/1205-lei-n-20-2020-de-31-de-dezembro-de-2020-lei-das-instituicoes-de-credito-e-sociedades-financeiras-e-revoga-as-leis-n-15-99-de-1-de-novembro-e-n-9-2004-de-21-de-julho, consulté le 23 juillet 2021.
289 http://www.oam.org.mz/wp-content/uploads/2017/07/Lei-das-Transac%C3%A7%C3%B5es-eletr%C3%B3nicas.pdf, consulté le 23 juillet 2021.
290 https://www.vm.co.mz/M-Pesa2 > consulté le 23 juillet 2021.
291 Téléchargement iOS https://apps.apple.com/pt/app/meu-m-pesa-mo%C3%A7ambique/id1442121355; Téléchargement Google Play
292 https://www.vm.co.mz/, consulté le 23 juillet 2021.

mozambicaines, ABC[293] (African Banking Corporation) et MozaBanco.[294]

Aperçu des données collectées par les applications de prêt numérique

Txuna M-Pesa[295]	Informations collectées et traitées par l'application	
	Autorisations demandées	Les termes et conditions (T&C) indiquent que le contrat définit les règles et les responsabilités entre le client, M-Pesa, MozaBanco et BancABC pendant la durée du prêt. Il n'y a pas de date de la dernière mise à jour des termes et conditions auprès des deux banques. En acceptant ces T&C, le client autorise BancABC à accéder aux données de son numéro Vodacom et du compte M-Pesa pour définir le niveau d'éligibilité.
	Informations recueillies auprès de l'utilisateur	Txuna M-Pesa s'engage à collecter les informations personnelles essentielles autorisées et limitées. Elle peut obtenir les informations personnelles du client s'il faut : Acheter ou acquérir un produit ou un service auprès de M-Pesa (y compris l'achat de produits en ligne, par téléphone ou dans une boutique Vodacom ou un autre établissement). S'inscrire à un produit ou service (y compris lorsque le client enregistre son nom et ses coordonnées ou crée un compte d'adresse e-mail avec Vodacom). S'abonner à des bulletins d'information, des alertes ou d'autres services de Vodacom. Demander des informations supplémentaires sur un produit ou un service, ou contacter Vodacom pour toute question ou plainte. Participer à un concours, une loterie ou une enquête. Utiliser les produits et services de M-Pesa. Avec votre permission ou votre consentement et dans la mesure permise par la loi, collecter également des informations vous concernant. Il s'agit notamment d'agences de prévention de la fraude, d'agences anti-fraude, d'annuaires professionnels, d'agences de référence de crédit et d'autres sociétés.
	Accès et correction des informations personnelles	Dans les conditions prévues par la loi, le client a le droit d'accéder, de corriger, de modifier, de supprimer ses informations personnelles ou de refuser qu'elles soient traitées. Dès réception de la demande écrite et d'informations suffisantes pour permettre à M-Pesa d'identifier les informations personnelles, ils divulgueront toutes les informations que M-Pesa détient sur les utilisateurs. Ils peuvent facturer le client, comme le permet la loi en vigueur.

293 https://www.bancabc.co.mz/en/index.html, consulté le 23 juillet 2021.
294 https://www.mozabanco.co.mz/, consulté le 23 juillet 2021.
295 Politique de confidentialité - https://www.vm.co.mz/M-Pesa2/Termos-e-Condicoes/Politica-de-Privacidade, consulté le 4 août 2021. Il est intéressant de noter que sur le site Web de M-Pesa, il existe une adresse électronique pour les commentaires et les réclamations : M-PESA.Privacy@vm.co.mz.

	Informations recueillies à partir de l'appareil de l'utilisateur	Les informations de l'entreprise sur les utilisateurs dépendent des produits et services M-Pesa que les clients utilisent et auxquels ils souscrivent. Cela comprend (sans s'y limiter) les éléments suivants : Le nom du client, sa date de naissance, le type et le numéro de sa pièce d'identité, son lieu de naissance et sa nationalité, sa filiation, son état civil et son régime matrimonial, son adresse, les informations relatives à son compte d'abonné et son adresse électronique et la nature de ses revenus. Les préférences du client pour des produits, services ou activités particuliers signalés par le client - ou lorsque Vodacom suppose ce qu'elles sont, en fonction de la façon dont le client utilise ces produits et services. Les communications du client avec M-Pesa - telles que les notes ou les enregistrements des appels que le client a passés avec l'un des centres de contact de Vodacom, les e-mails ou les lettres envoyés à Vodacom, ou tout autre enregistrement des contacts que le client a établis avec Vodacom. Les informations sur le compte du client comprennent les numéros de téléphone des utilisateurs, les dates des transferts et des paiements effectués ou reçus, ou toute autre information connexe. Shopping Achats Informations financières Informations sur les contacts Contacts Mot de passe Identifiants Données d'utilisation Diagnostics
	Informations recueillies lors de l'utilisation du site Internet de M-Pesa	Les cookies internes proviennent du même domaine que le site Web que vous êtes en train de visiter (dans ce cas, vodafone.com). Les cookies tiers proviennent d'un domaine différent du site Web visité. Par exemple, lorsque les clients visitent le site Web de M-Pesa, ils peuvent établir un lien avec le site Web d'une autre société - comme leur compte Facebook ou Twitter ou une vidéo de leur page YouTube. Ainsi, lorsque le client " aime " ou " tweet " un élément du site Web de M-Pesa, ces sites peuvent parfois placer des cookies sur l'ordinateur de l'utilisateur. M-Pesa déclare qu'elle ne contrôle pas ses cookies, et suggère donc aux utilisateurs de consulter son site Web pour savoir comment ils les utilisent et comment les gérer.

	Informations reçues de tiers	Les sociétés affiliées du groupe Vodafone ayant un nom de domaine différent peuvent également placer des cookies sur leur site web pour montrer aux utilisateurs des publicités ou des pages d'autres sociétés du groupe Vodafone susceptibles de vous intéresser. Les détails concernant ces sociétés affiliées - et la manière de les exclure - figurent sur le site web.
	Utilisation des informations de l'utilisateur par l'application	Informations financières ID - documents personnels (passeport ou document local) Contacts
	Informations partagées avec des tiers	Informations financières Pièce d'identité (la Banque oblige les clients à fournir une copie de leurs documents) Les informations peuvent être partagées avec : Les sociétés du groupe Vodacom (Vodafone Group Plc et toute autre société dont Vodafone Group Plc détient plus de 15% du capital social). des partenaires ou agents impliqués dans la fourniture des services que vous avez demandés ou utilisés Partenaires ou agents chargés de la satisfaction de la clientèle enquêtes sur les produits et services qui vous sont fournis Les sociétés engagées dans la fourniture de services pour le compte de Vodacom (Pty) Ltd, y compris Vodafone Limited ou d'autres sociétés du groupe Vodafone. Le cas échéant, les agences de référence de crédit, les agences de prévention des fraudes, les agences d'évaluation des entreprises ou d'autres agences d'évaluation de crédit. Sociétés de recouvrement de créances ou autres sociétés de recouvrement de créances Si la loi l'exige ou le permet, les autorités chargées du maintien de l'ordre, les régulateurs, les tribunaux ou d'autres autorités publiques. Services d'urgence (si le client passe un appel d'urgence) La société divulgue des informations dans les limites du possible pour la protection contre la fraude, pour défendre les droits ou la propriété de M-Pesa ou pour protéger les intérêts des clients. Si Vodafone M-Pesa est réorganisé ou acquis par une autre société ou un autre groupe, les informations personnelles sur les clients pourront être transférées à cette société ou ce groupe.
	Durée de l'accès des informations aux tiers	La manière dont ces données sont utilisées et la durabilité de leur utilisation en cas de résiliation du contrat entre la Banque, M-Pesa Txuna et le client ne sont pas claires.

	Technologies de suivi / cookies de site web	M-Pesa Txuna déclare que ses cookies ne contiennent pas d'informations personnelles telles que le nom. M-Pesa permet aux utilisateurs de trouver des informations une fois qu'ils sont connectés ou de relier leurs informations de navigation à leurs données lorsque les clients choisissent de s'inscrire à un service, un livre blanc ou une lettre d'information.
	Stockage des informations sur l'utilisateur par l'application	Informations financières Informations sur les contacts

Les prêts peuvent commencer à partir de 70 Meticais (MT) jusqu'à 3 500 MT (environ 1 à 60 $). Les montants peuvent changer en fonction du niveau d'éligibilité du client et de ses antécédents. Les conditions générales de la banque ABC ne sont pas rédigées[296] avec professionnalisme. Il ne semble pas s'agir d'un document contractuel entre deux entités. Le document définit ce que l'on entend par données client, c'est-à-dire les informations fournies par M-Pesa à la banque et à NANO (Global Holdings Limited) pour permettre le profilage du client et la fourniture de ce service.

Le même document indique que NANO est l'entreprise technologique qui fournit la plateforme technique pour le profilage de l'éligibilité des clients à l'utilisation du service. Il est dit que si les conditions générales sont acceptées, le client : a) confirme que toutes les informations (y compris les documents) fournies à Vodafone M-Pesa SA sont correctes, complètes et conformes à la réalité ; et b) autorise Vodafone M-Pesa SA à divulguer, vérifier et échanger toute information relative à l'identité et aux transactions avec l'institution financière chargée de fournir le service de prêt et les tiers fournissant l'infrastructure technique et les autorités réglementaires.

Nous constatons qu'entre les deux banques, ABC et MozaBanco, il y a une certaine différence dans la manière d'expliquer les termes et conditions. Par exemple, MozaBanco[297] utilise un système de gestion des données différent, FICO, une entreprise/entité partenaire qui s'occupe de services de crédit/financiers, d'analyse, de critères et de services associés. Cependant, le système d'autorisation des données/informations personnelles est le même entre les deux banques.

Nous avons également constaté que le document « Foire aux questions - Q&A »[298] disponible sur le site web ne précise pas la date de sa dernière mise à jour. Ce même document ne mentionne rien sur la protection des données ou l'utilisation des informations. Les questions posées profitent principalement à l'application mobile de prêt d'argent pour promouvoir son service et pas nécessairement aux clients. Cependant, l'un des aspects positifs que nous avons pu trouver est que M-Pesa publie[299] ses rapports financiers annuels, et que le dernier date de décembre 2020.

Le 7 mars 2019, Nous avons constaté que Vodafone M-Pesa, S.A. s'est vu infliger[300] une amende d'un montant de 10 millions de MT (environ 157 240 $) par la Banque centrale du Mozambique, suite à une violation de la réglementation sur la lutte contre le blanchiment

296 http://www.vm.co.mz/content/download/106232/706643/version/1/file/Termos+e+Condicoes+Txuna+M-Pesa+BancABC.pdf, consulté le 23 juillet 2021.
297 Consulté http://www.vm.co.mz/content/download/106233/706647/version/1/file/Termos+e+Condicoes+Txuna+M-Pesa+Moza+Banco.pdf > consulté le 25 juillet 2021.
298 http://www.vm.co.mz/content/download/106095/705913/version/1/file/Perguntas+Frequentes+Txuna+M-Pesa.pdf > consulté le 24 juillet 2021.
299 https://www.vm.co.mz/M-Pesa2/Relatorios-Financeiros, consulté le 24 juillet 2021.
300 Report http://www.vm.co.mz/content/download/103501/690546/version/1/file/M-Pesa+-+Relat%C3%B3rio+Disciplina+de+Mercado_Junho_2019.pdf > consulté le 24 juillet 2021.

d'argent - article 77 de la loi 14/2013. L'infraction était due à une limitation du système qui a maintenant été résolue. La nature de l'erreur système n'est pas claire[301]. On comprend néanmoins qu'il s'agissait d'une violation qui a exposé les données des utilisateurs à des tiers qui pouvaient avoir accès aux données personnelles et causer des fraudes financières par le biais de l'application.

Étude de cas : Deux utilisateurs de M-Pesa

Gilberto Manhiça[302] utilise M-Pesa depuis 2017. Tout d'abord, il a donné ses données (identification/identification personnelle) à la société de téléphonie mobile lorsqu'il a enregistré son compte et a mis à jour ses informations personnelles pour augmenter le montant autorisé sur le compte. En ce qui concerne la confidentialité des données, il note que Txuna est devenu sécurisé en 2020 lorsque M-Pesa a changé les règles pour cacher le nom du client pendant le processus de transfert. En tant que client de Txuna, il n'est pas sûr de la sécurité de ses données. Pourtant, même s'il était au courant de ses données, il ne doute pas que si les entités de la justice (police) veulent ses informations, elles y auront toujours accès auprès de l'entreprise de téléphonie mobile. Gilberto n'a jamais lu les conditions générales mais se souvient d'un contrat avec la banque ABC qui autorise Vodacom et Txuna M-Pesa à partager ses données avec la banque. Il considère qu'il s'agit d'une certaine sécurité mais note qu'il « fait confiance à la banque, plus qu'à Vodacom ». Nous avons également parlé à Justino Mabuiango[303] , qui a commencé à utiliser M-Pesa en 2016. Pour lui, l'application M-Pesa est sûre car ses "données ne sont exposées à personne". Comme Gilberto, il a mentionné que le changement substantiel s'est produit en 2020 lorsque M-Pesa a adopté un système selon lequel, en cas de transfert, l'application ne montre que les initiales du client. Le client a déclaré qu'il n'utilisait pas Txuna régulièrement car « il n'est pas bon d'avoir des dettes. » Tout ce qu'il sait sur les données personnelles est dû à sa propre expérience en tant qu'utilisateur et a noté qu'il n'a jamais lu aucun document pour adhérer au service ; il y a une garantie de sécurité.

Conclusion

L'application M-Pesa Txuna révèle que, bien que le service soit présent au Mozambique depuis plus de cinq ans, son expansion à d'autres banques est encore limitée si l'on considère que le Mozambique compte plus de dix banques commerciales. Le fait qu'il ne fonctionne qu'avec deux banques peut soulever certaines questions qui nécessitent une analyse plus approfondie. En outre, malgré la mise à disposition des conditions d'utilisation de la plateforme, l'absence de mise à jour de ces documents reste une question sans réponse. La politique de confidentialité n'est pas publiée de manière visible pour les clients, ce qui fait qu'il existe des cas d'omission, comme cela a été constaté tout au long des entretiens où un utilisateur a mentionné avoir utilisé le service sans jamais avoir lu aucun document auparavant. En conclusion, il y a des omissions sur la façon dont M-Pesa travaille avec la Banque centrale pour demander les données personnelles des clients.

301 http://www.vm.co.mz/content/download/103501/690546/version/1/file/M-Pesa+-+Relat%C3%B3rio+Disciplina+de+Mercado_Junho_2019.pdf, consulté le 24 juillet 2021.
302 Entretien du 22 juillet 2021, Maputo (Mozambique, via zoom).
303 Entretien du 27 juillet 2021, Maputo (Mozambique, via zoom).

Namibie

Profil du pays

Située sur la côte sud-ouest de l'Afrique, la Namibie partage une frontière avec l'Angola au nord et l'Afrique du Sud au sud. Après 106 ans de domination allemande et sud-africaine, la Namibie est devenue indépendante le 21 mars 1990, en vertu d'une constitution démocratique multipartite.[304] La capitale du pays est Windhoek. Sa population est estimée à environ 2 millions d'habitants[305] et son PIB à 10,56 milliards d'euros en 2020.[306]

304 https://www.britannica.com/place/Namibia > consulté le 6 septembre 2021.
305 https://www.worldometers.info/world-population/namibia-population/ > consulté le 5 septembre 2021.
306 https://www.statista.com/statistics/510122/gross-domestic-product-gdp-in-namibia/ > accessed on 5 September 2021.

Protection des données en Namibie

La Namibie n'a pas adopté de législation sur la protection des données.[307] Le pays est conscient que la vie privée est un droit de l'homme fondamental, conformément à l'article 13 de la Constitution namibienne.[308] Cet article stipule que nul ne sera soumis à une ingérence dans la vie privée de son domicile, de sa correspondance ou de ses communications. La loi prévoit une exception pour les ingérences prévues par la loi, dans l'intérêt de la sécurité nationale, de la sûreté publique ou du bien-être économique du pays, pour la protection de la santé ou de la moralité, pour la prévention des troubles ou des crimes, ou pour la protection des droits ou des libertés d'autrui

La Namibie a ratifié le Convention internationale sur les droits civils et politiques ('ICCPR').[309] Cela renforce l'article 12 de la DUDH, qui prévoit que « nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation ».

Système financier et Fintech en Namibie

Le cadre juridique du système national de paiement a été établi à partir de la loi sur la gestion du système de paiement de 2003 (loi n° 18 de 2003)[310] et des règlements publiés en vertu de la loi sur la gestion du système de paiement, telle que modifiée.[311] La Bank

307 https://www.dlapiperdataprotection.com/index.html?t=law&c=NA > consulté le 6 septembre 2021.
308 http://www.kas.de/upload/auslandshomepages/namibia/constitution/const_en_contents.pdf > consulté le 5 septembre 2021.
309 https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx > consulté le 5 septembre 2021.
310 https://www.bon.com.na/Bank/Payments-and-Settlements/Legal-Framework/Payment-System-Management-Act.aspx > consulté le 3 septembre 2021.
311 https://www.bon.com.na/Bank/Payments-and-Settlements/Legal-Framework/Payment-System-Management-Amended-Act.aspx > consulté le 3 septembre 2021.

of Namibia compte cinq émetteurs de monnaie électronique agréés : Magnet Payment Solutions ; Nam-mic Payment Solutions ; NamPost ; Virtual Technology Services, et Vivo Energy Namibia.[312]

En février 2021, il a été signalé[313] qu'au cours de la seule année 2020, plus de 40 milliards de dollars[314] namibiens ont été transférés par le biais de plateformes de monnaie électronique telles que eWallet, easyWallet et Blue Wallet et d'autres services bancaires similaires. Un an avant 2019, cette valeur n'était que de 14,8 milliards de dollars namibiens, ce qui a augmenté de 177%, soit plus que la croissance de la valeur poussée par les cartes bancaires et les transferts électroniques.

En avril dernier, la Banque de Namibie (BON) a appelé le secteur bancaire à envisager la technologie financière pour améliorer l'accès et l'inclusion financière.[315] Dans son rapport annuel,[316] la banque centrale a déclaré que plus les options d'accès aux produits et services bancaires seraient nombreuses, plus le nombre de clients serait élevé. Il est à noter que la Namibie compte encore de nombreux particuliers et entreprises qui ne sont pas enregistrés auprès des banques et préfèrent effectuer leurs transactions en espèces. Les transactions mobiles ont également augmenté de façon spectaculaire, passant de moins de 10 millions en 2015 à plus de 65 millions en 2020.[317] La BON a également lancé la vision et la stratégie du système national de paiement de la Namibie pour 2021-2025, qui prévoit de rendre les paiements multiplateformes plus conviviaux.[318] « En outre, la Bank of Namibia (BON) est en passe de terminer son étude[319] sur les crypto-monnaies d'ici avril 2022 », a récemment confirmé le gouverneur de la banque centrale, Johannes Gawaxab.[320] Toutefois, le gouverneur a réaffirmé que les crypto-monnaies n'ont pas cours légal, car les lois du pays ne prévoient pas actuellement l'utilisation de devises numériques.

PayToday : L'application mobile de prêt d'argent

PayToday[321] est une application d'argent mobile namibienne qui permet d'effectuer des paiements et des prêts par le biais de comptes bancaires pour les particuliers et les entreprises. Les clients doivent télécharger l'application PayToday à partir d'Apple Store ou Google Play Store et compléter le processus d'enregistrement pour utiliser l'application. Les clients doivent soumettre les détails de leur carte et de leur banque dans le cadre du processus d'inscription. Les détails de leur carte sont utilisés pour effectuer les paiements. Tout d'abord, l'application a été lancée sous le nom de StayToday, par Chris (expert-comptable) et Naude (ingénieur électrique/électronique) en 2013.[322] En 2017, elle a été introduite en Namibie. La solution est rendue possible grâce à un partenariat avec Nedbank Namibia. La plupart des cartes de débit ou de crédit de n'importe quelle banque namibienne peuvent être utilisées pour payer le carburant sur PayToday.[323]

Aperçu des données collectées par les applications de prêt numérique

312 Institutions de monnaie électronique https://www.bon.com.na/Bank/Payments-and-Settlements/E-Money-Institutions.aspx > consulté le 6 septembre 2021
313 Article https://allafrica.com/stories/202102240567.html > consulté le 3 septembre 2021.
314 Environ 2 800 581 200 $.
315 Article de presse https://afcacia.com/2021/04/17/namibian-banks-urged-to-embrace-fintech/> consulté le 3 septembre 2021.
316 https://www.bon.com.na/getattachment/7923760d-1805-4265-906a-b424abafdef8/.aspx > consulté le 3 septembre 2021.
317 Idem.
318 https://www.bon.com.na/getattachment/2183fe04-8b8f-44d0-add9-4629d7ec86a5/19-02-2021-Namibia-National-Payment-System-Vision.aspx > consulté le 3 septembre 2021.
319 Lois sur les crypto-monnaies en Namibie https://freemanlaw.com/cryptocurrency-blockchain/namibia/ > consulté le 6 septembre 2021
320 Article de presse https://news.bitcoin.com/namibia-central-bank-to-complete-crypto-study-by-april-2022-governor-says-current-laws-do-not-permit-use-of-digital-assets/ > consulté le 4 septembre 2021.
321 https://site.paytoday.com.na > consulté le 4 septembre 2021.
322 https://www.offerzen.com/companies/paytoday > consulté le 4 septembre 2021.
323 https://www.namibian.com.na/169678/archive-read/PayToday-introduces-mobile-fuel-payments > consulté le 4 septembre 2021.

PayToday[324]	Informations collectées et traitées par l'application	
	Autorisations demandées	L'application permet trois différents types de paramètres et d'autorisations de confidentialité :[325] Participants uniquement (paramètre de confidentialité strict) : Seules les personnes à qui les utilisateurs demandent ou envoient de l'argent seront informées de la transaction. Amis uniquement (paramètre de confidentialité modéré) : Les transactions ne seront partagées qu'avec les amis des utilisateurs. Tous les contacts des clients dans leur répertoire téléphonique définissent les amis des utilisateurs. Tout le monde (paramètre de confidentialité peu contraignant) : Les transactions (peer to peer et achats) seront partagées sur le fil de discussion en Namibie, le fil des amis et visibles par tous.
	Informations recueillies auprès de l'utilisateur	Nom ; Numéro de téléphone ; Adresse électronique ; Numéro de carte de crédit/débit et date d'expiration ; Coordonnées bancaires ; Numéros d'identification ; Noms de connexion ; Mots de passe ; Informations sur l'appareil ;
	Accès et correction des informations personnelles	Lire le contenu des clés USB des clients Modifier ou supprimer le contenu des clés USB des clients. Toutes les informations personnelles des clients que l'application collecte et conserve peuvent être consultées et modifiées par les utilisateurs à tout moment.
	Informations recueillies à partir de l'appareil de l'utilisateur	Les informations de localisation (uniquement lorsque le client a explicitement donné son autorisation) ; les coordonnées des clients dans votre répertoire téléphonique (uniquement si le client a explicitement donné son autorisation). PayToday fait correspondre les données de contact à la base de données des utilisateurs enregistrés pour effectuer des transactions avec d'autres utilisateurs enregistrés. Leurs données de contact sont stockées sur l'application dans une base de données interne pour la mise en cache, mais pas sur le serveur dorsal. Toutes les informations relatives à chaque transaction (le contenu du message, l'heure, la date, le destinataire et le montant de chaque transaction) ; Informations non personnelles identifiables ("NPPI") - il s'agit d'informations qui peuvent correspondre à une personne ou à un compte particulier mais qui, à elles seules, ne sont pas suffisantes pour identifier, contacter ou localiser une personne spécifique.

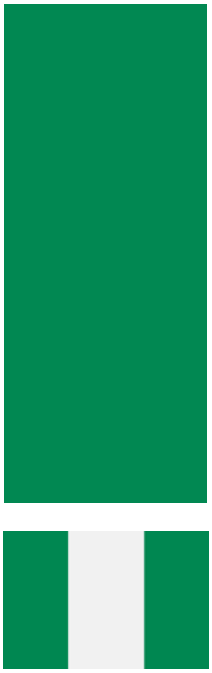
324 Foire aux question https://site.paytoday.com.na/need-help/#FAQs > consulté le 4 septembre 2021.
325 https://www.today.com.na/paytoday-privacy-policy > consulté le 3 septembre 2021.

	Informations recueillies lors de l'utilisation du site Internet de PayToday	Lorsque les utilisateurs se connectent à l'application PayToday ou accèdent au site web PayToday, ils peuvent transférer de petits fichiers de données appelés "cookies" sur leur ordinateur ou leur périphérique de connexion. Les sites web de PayToday utilisent ces « cookies » pour améliorer l'expérience des utilisateurs, qui sont libres de refuser ces « cookies ».
	Informations reçues de tiers	Aucune information
	Utilisation des informations de l'utilisateur par l'application	PayToday ou les entités liées ou leurs actifs respectifs pourraient être acquis par une autre entité commerciale ou fusionnés dans une telle entité. Si une telle fusion ou acquisition se produit, le client doit s'attendre à ce que PayToday partage une partie ou la totalité des informations personnelles d'identification des utilisateurs.
	Informations partagées avec des tiers	Dans le cadre de l'envoi et de la demande d'argent à d'autres utilisateurs de PayToday, les informations personnelles suivantes seront partagées avec les autres utilisateurs qui effectuent des transactions : détails de la transaction (montant, heure, date, autres participants, photo du profil du client et nom d'utilisateur).

Conclusion

Il semble que l'application détaille les informations nécessaires aux utilisateurs sur son site web. Cependant, l'absence d'une loi sur la protection des données ne permet pas une analyse cohérente garantissant la protection des données personnelles. Par exemple, dans les conditions de confidentialité de la politique, il n'est pas fait mention de l'intervention des organismes de réglementation pour les cas où les détenteurs de l'application violent les droits à la vie privée de leurs clients. Nous constatons également qu'il n'est pas fait mention de la relation entre l'application et ses partenaires (banques commerciales) dans le partage des informations avec des tiers. L'explication est vague et se concentre uniquement sur l'application elle-même et non sur d'autres entités.

Nigéria



Profil du pays

Situé en Afrique de l'Ouest,[326] le Nigeria, également connu sous le nom de République fédérale du Nigeria, partage une frontière avec le Niger, le Tchad, le Cameroun et le golfe de Guinée.[327] Il couvre une superficie de 923 768 km2[328] avec un climat allant de l'aride à l'équatorial humide[329]. Le Nigeria est le pays le plus peuplé d'Afrique, avec plus de 211 millions d'habitants.[330] Il compte environ 250 groupes ethniques divers, dont les langues les plus populaires sont le haoussa, l'igbo et le yoruba.[331] Sa capitale est Abuja, bien que Lagos reste la plus grande ville avec des activités économiques.[332]

326 Nigéria https://www.nationsonline.org/oneworld/nigeria.htm
327 Nigéria https://www.britannica.com/place/Nigeria
328 (n1)
329 (n2)
330 Bilan de la population mondiale Nigéria https://www.unfpa.org/data/world-population/NG
331 13 choses que vous devez savoir sur le Nigeria https://artsandculture.google.com/story/13-things-you-need-to-know-about-nigeria/_AJCyGgURLk8KA
332 (n1)

Protection des données au Nigeria

Au Nigeria, les particuliers et les PME ont principalement recours aux applications de prêt numériques en raison de leur processus de prêt simplifié et rapide, contrairement aux banques où l'obtention d'un prêt s'avère ardue.[333] L'utilisation de ces applications a augmenté, en particulier depuis la pandémie de coronavirus, qui a eu un impact considérable sur l'économie mondiale.[334] Contrairement aux banques, ces applications offrent un moyen pratique d'accéder à des prêts dans un court délai sans exiger de garantie. Cependant, elles s'appuient fortement sur les données de l'utilisateur pour évaluer le risque de crédit.

Les institutions qui possèdent ces applications doivent être enregistrées et obtenir une licence de la Banque centrale du Nigeria (CBN) en vertu de la loi 2020 sur les banques et autres institutions financières (BOFIA).[335] Cette loi place ces applications sous la supervision de la CBN et les classe dans la catégorie des « activités d'autres institutions financières », ce qui inclut les activités financières menées de manière numérique, virtuelle ou électronique.[336] Il convient de noter que ces entités (prêteurs) peuvent également s'inscrire dans le cadre des lois des États nigérians. Il convient de noter que ces entités (prêteurs)

333 L'intrusivité des applications de prêt mobiles au Nigeria https://aanoip.org/the-intrusiveness-of-money-lending-apps-in-nigeria/
334 Ibid
335 Section 57 (1), Loi 2020 sur les banques et autres institutions financières (BOFIA) https://www.cbn.gov.ng/Out/2021/CCD/BOFIA%202020.pdf
336 Article 57 (2)(j)(ix), Loi de 2020 sur les banques et autres institutions financières.

peuvent également s'inscrire dans le cadre des lois des États nigérians. Toutefois, cette option peut limiter les activités du prêteur. Le prêteur ne sera autorisé à opérer que dans les limites de l'État où l'enregistrement a eu lieu. Il sera également limité en termes de taux d'intérêt qu'il peut appliquer.[337]

Les activités de traitement des données de ces applications sont régies par le règlement sur la protection des données du Nigeria (NDPR), qui exige que ces applications préservent le droit à la vie privée des utilisateurs.[338] Le Règlement définit un cadre que les responsables du traitement des données doivent suivre pour garantir la sécurité des données des personnes concernées (dans ce cas, les emprunteurs).

Cette étude se concentre sur l'analyse de la conformité de ces applications avec les dispositions du RPDN. Elle commence par évaluer les données collectées par ces applications et analyse ensuite si ce traitement est conforme au RPDN

Aperçu des données collectées par les applications de prêt numérique

Carbon[339]	Informations collectées et traitées par l'application	
	Autorisations demandées	Demande la permission d'accéder : aux SMSs aux contacts aux applications installées historique du navigateur calendrier Localisation- Informations précises sur la localisation L'application peut également collecter ces informations en arrière-plan lorsque l'utilisateur ne l'utilise pas.
	Informations recueillies auprès de l'utilisateur	Informations demandées à l'utilisateur : nom, adresse, adresse électronique, numéro de téléphone, informations de connexion aux réseaux sociaux, informations financières/carte de crédit, description personnelle, emploi actuel et précédent, formation, noms des collègues, contacts et amis, photographies et liste des membres de la famille.
	Informations collectées à partir de l'appareil de l'utilisateur/ Utilisation du site web	Informations techniques : Adresse IP, informations de connexion, type de navigateur et version, réglage du fuseau horaire, types de plug-in des navigateurs et versions, système d'exploitation et plate-forme. Visite de l'utilisateur : Liens URL lors de la navigation sur le site ; produits consultés ou recherchés ; temps de réponse des pages, erreurs de téléchargement, durée des visites des pages du site, informations sur l'interaction des pages (défilement, clics, déplacements de la souris) ; méthodes utilisées pour naviguer ; numéro de téléphone utilisé pour appeler le service clientèle Données sur les remboursements

337 ICLG, Réglementation Fintech du Nigeria 2021 https://iclg.com/practice-areas/fintech-laws-and-regulations/nigeria
338 Règlement sur la protection des données au Nigeria 2019
339 Politique de Carbon https://getcarbon.co.ke/privacy-policy.html

	Mode de collecte des informations sur les utilisateurs	Lorsque vous remplissez des formulaires sur le site (par exemple, l'inscription et la demande de prêt dans l'application). Lors de l'autorisation d'accès aux plateformes de réseaux sociaux Lors de la correspondance, c'est-à-dire par courriel, par téléphone, etc,
	Informations reçues de tiers	Reçoit des informations : d'autres sites Web exploités par Carbon, utilisés par l'utilisateur. des plates-formes de réseaux sociaux sur lesquelles l'utilisateur se connecte via Carbon. de tiers, tels que des entrepreneurs, des sous-traitants, des services de paiement et de livraison, des sites de réseaux sociaux, des régies publicitaires, des agences d'évaluation du crédit et des fournisseurs de crédit, entre autres.
	Utilisation des informations de l'utilisateur par l'application	Exécution des obligations contractuelles avec l'utilisateur Notation de crédit Fourniture d'informations sur les biens et services de Carbon Marketing Notification de changements dans les services de Carbon Traitement ultérieur à des fins de recherche scientifique, statistique ou historique, conformément à l'intérêt public,
	Partage d'informations avec des tiers/ Divulgation d'informations Durée de l'accès des données aux tiers	Partage des informations avec les tiers suivants : Ses filiales, sa société holding. Ses partenaires commerciaux, fournisseurs et sous-traitants Annonceurs et réseaux publicitaires Fournisseurs de services d'analyse et de moteurs de recherche D'autres parties qui respectent une obligation légale ou appliquent ses conditions d'utilisation. Reçoit des informations sur l'utilisateur : Sociétés de commutation Fournisseurs de réseaux mobiles Sociétés d'électricité Agrégateurs Bureaux d'information sur le crédit Les plateformes de commerce électronique, et D'autres institutions financières. Pas d'indication
	Technologies de suivi/ cookies de site web	Les utilisateurs consentent à ce que des cookies soient placés dans leurs navigateurs et à ce que des courriels en HTML soient envoyés lorsqu'ils visitent le site.
	Transferts internationaux de données	Les données peuvent être transférées/partagées entre les pays dans lesquels Carbon opère.

	Stockage des informations sur l'utilisateur par l'application	Stocke les données sur ses serveurs en utilisant JWT

PalmCredit[340]	Informations collectées et traitées par l'application	
	Autorisations demandées	Demande la permission d'accéder à: la liste de contacts l'historique des appels l'historique des SMS Contacts Facebook la listes de contacts d'autres comptes de médias sociaux Photos, vidéos ou autres contenus numériques L'application appelle les contacts de la liste de contacts, des SMS ou de la liste d'appels d'un utilisateur pour vérifier l'identité de ce dernier.
	Informations recueillies auprès de l'utilisateur	Données personnelles : nom, âge, adresse électronique, numéro de téléphone, coordonnées physiques, description personnelle, photographie, nom d'utilisateur, mot de passe, informations financières - numéros de carte de crédit et de compte bancaire. Données transactionnelles : activités de l'utilisateur sur l'application. Correspondance : données recueillies dans le cadre de la correspondance avec l'utilisateur. Informations supplémentaires à des fins de vérification
	Informations recueillies à partir de l'appareil de l'utilisateur	ID du dispositif Type d'appareil Identifiants uniques de l'appareil ; informations de géolocalisation, ordinateur, système d'exploitation et informations de connexion Adresse IP Informations standard du journal Web
	Mode de collecte des informations sur les utilisateurs	Remplir des formulaires sur l'application Correspondre avec PalmCredit S'inscrire pour utiliser l'application S'abonner aux services PalmCredit Partage de données via les fonctions de médias sociaux de l'application Promotion, concours ou enquête Signaler des problèmes liés à l'application
	Informations reçues de tiers	Données démographiques et de navigation, Des informations sur les contrôles de crédit, et Informations provenant d'un bureau de crédit

340 Politique de confidentialité de PalmCredit http://web.palmcredit.loans/policy.html

	Utilisation des informations de l'utilisateur par l'application	Calcul de la limite de crédit Fourniture d'un accès à l'application Carbon Résolution des litiges Prévention de la criminalité et application des conditions générales de l'application. Personnalisation du contenu, de la publicité et des services Fourniture d'informations sur les services de l'application Marketing ciblé Vérification auprès de tiers Contact avec l'utilisateur
	Informations partagées avec des tiers Durée de l'accès des informations aux tiers	-L'application divulgue des informations sur les utilisateurs à : ses partenaires commerciaux lors de fusions et d'acquisitions ses partenaires commerciaux lors de la vente ou de l'achat d'une entreprise ou d'actifs des organismes d'application de la loi et des organismes gouvernementaux Ses filiales, sociétés holding, etc., des tiers dans le cadre de l'application de ses conditions générales ou de la publication des statistiques d'utilisation de l'application. Agence d'évaluation du crédit Des tiers lorsqu'il s'agit de se conformer à des ordres juridiques ou réglementaires ou d'appliquer ses politiques. Aucune indication
	Technologies de suivi/ cookies de site web	L'application possède : Des cookies de connexion qui sont supprimés du disque dur de l'utilisateur une fois que ce dernier a terminé sa session sur l'application. Des cookies de tiers qui proviennent principalement de ses fournisseurs de services. des cookies de tiers (n'appartenant pas à l'application) qu'un utilisateur rencontre lorsqu'il visite une autre page web sur l'application.

	Transferts internationaux de données/ Transferts transfrontaliers de données	Lorsque les données de l'utilisateur doivent être transférées vers un pays qui ne figure pas sur la liste blanche, l'application ne transfère les données que dans les circonstances suivantes : Lorsque le consentement de l'utilisateur a été obtenu. Lorsqu'un transfert est requis pour l'exécution d'un contrat entre l'utilisateur et l'application. Lorsqu'un transfert est nécessaire pour la conclusion d'un contrat entre l'application et un tiers dans l'intérêt de l'utilisateur. lorsqu'un transfert est nécessaire pour des raisons d'intérêt public lorsqu'un transfert est nécessaire pour l'établissement ou la défense de revendications légales.
	Stockage des informations sur l'utilisateur par l'application	Les données des utilisateurs peuvent être stockées ou transférées en hors du Nigeria. Elles peuvent également être traitées par du personnel opérant en dehors du Nigeria.

Branch	Informations collectées et traitées par l'application	
	Autorisations demandées	
	Informations recueillies auprès de l'utilisateur	Nom, date de naissance, numéro de téléphone, adresse mail, nationalité, numéro d'identification fiscale (ID), coordonnées bancaires, numéro de vérification bancaire, numéro d'identification, localisation, photographie, adresse IP, adresse MAC, numéro IMEI, numéro IMSI.[341]
	Informations recueillies auprès de l'appareil de l'utilisateur	
	Mode de collecte des informations par Branch	Par le biais de formulaires intégrés à l'application lors de la demande de prêt Par le biais de l'appareil de l'utilisateur Par la correspondance avec l'utilisateur, c'est-à-dire les courriels
	Informations reçues de tiers	
	Utilisation des informations de l'utilisateur	Évaluation du risque de crédit Exécution de la diligence raisonnable Respect de la réglementation Utilisation à des fins de marketing
	Informations partagées avec des tiers Durée de l'accès des informations aux tiers	

341 Politique de protection des données de la branche, pg 5 https://branch.co/documents/BranchDataProtectionPolicy-NG.pdf

	Technologies de suivi/ cookies de site web	
	Transferts internationaux de données	
	Stockage des informations sur les utilisateurs par l'application	

QuickCheck[342]	Informations collectées et traitées par l'application	
	Autorisations demandées	
	Informations recueillies auprès de l'utilisateur Mode de collecte des informations auprès des utilisateurs	Nom, adresse (y compris une ancienne adresse), courriel, numéro de téléphone, informations sur les médias sociaux, informations financières, informations sur le statut personnel, informations sur l'emploi, détails sur le niveau d'éducation, contacts et connaissances de la famille, applications, messages, adresse IP, type de navigateur.[343] Lorsque vous remplissez des formulaires dans l'application/le site Lors de l'octroi de l'accès aux comptes de réseaux sociaux par correspondance, c'est-à-dire par téléphone ou par courrier électronique par les commentaires des utilisateurs sur le site
	Informations collectées à partir de l'appareil de l'utilisateur	
	Informations reçues de tiers	
	Utilisation des informations de l'utilisateur par l'application	Personalisation of content Provision of products and services Credit scoring Notification of changes in products and services Correspondence, i.e., through email or phone
	Conservation des données de l'utilisateur	Indefinite retention of user comments on the site "Users can see, edit or delete their data at any time". However, "they cannot change their username".
	Informations partagées avec des tiers Durée de l'accès des informations aux tiers	

342 Politique de confidentialité de QuickCheck https://quickcheck.ng/privacy-policy/
343 Politique de confidentialité de QuickCheck https://quickcheck.ng/privacy-policy/

	Technologies de suivi/ cookies de site web	Type de cookies : Cookie temporaire- détermine l'acceptation des cookies par le navigateur de l'utilisateur lors de la connexion. Cookies de connexion- enregistre les informations de connexion de l'utilisateur Les cookies sont enregistrés dans les navigateurs des utilisateurs lorsqu'ils publient ou modifient des articles sur le site. -Les cookies sont utilisés à des fins de suivi.
	Transferts internationaux de données	
	Stockage des informations sur l'utilisateur par l'application	« Les informations personnelles des utilisateurs sont contenues dans des réseaux sécurisés et ne sont accessibles que par un nombre limité de personnes qui ont des droits d'accès spéciaux à ces systèmes et sont tenues de garder ces informations confidentielles. En outre, toutes les informations sensibles/de crédit fournies par les utilisateurs sont cryptées via le protocole Secure Socket Layer (SSL)... Toutes les transactions sont traitées par un fournisseur de passerelles et ne sont pas stockées ou traitées sur nos serveurs. »

Aella credit[344]	Informations collectées et traitées par l'application	
	Autorisations demandées	
	Informations recueillies auprès de l'utilisateur	Nom, adresse, adresse électronique, numéro de téléphone, IMEI, détails de la carte SIM, âge, nom d'utilisateur, mot de passe, informations financières et de crédit (y compris les détails du compte d'argent mobile de l'utilisateur, les détails du compte bancaire, le numéro de vérification de la banque), description personnelle et photographie.[345]
	Informations collectées à partir de l'appareil de l'utilisateur/ Utilisation du site web	Informations techniques : type d'appareil mobile, identifiants uniques (IMEI ou numéro de série), utilisation de la carte SIM, réseau mobile, système d'exploitation, type de navigateur, emplacement de l'appareil et réglage du fuseau horaire, informations stockées sur un appareil (contacts, journaux d'appels, SMS, photos, vidéos ou autres contenus numériques), informations sur l'utilisation d'une application tierce sur un appareil, détails de l'utilisation de l'application Aella (y compris les données de trafic et de localisation, les informations de connexion).[346] Informations de localisation grâce à la technologie GPS
	Informations reçues de tiers	Reçoit des informations de : D'agences d'évaluation du crédit Fournisseurs de réseaux mobiles
	Utilisation des informations de l'utilisateur	Ouverture de compte Respect des exigences en matière de respect de la vie privée (Know Your Customer) Évaluation de la solvabilité de l'utilisateur
	Mode de collecte des informations sur les utilisateurs	Remplir les formulaires lors de la demande de prêt sur l'application ou le site Correspondance avec Aella credit L'inscription pour l'utilisation du site Aella Le téléchargement de l'application L'abonnement aux services d'Aella Lors d'une recherche d'une application ou d'un service Connexion/ partage d'informations via les fonctions de médias sociaux d'aella credit Participation à des concours de l'application Lors de promotions ou d'enquêtes Lors de plaintes concernant l'application, les services ou le site.

344 Politique de confidentialité du crédit Aella https://aellaapp.com/privacy-policy
345 Politique de confidentialité du crédit d'Aella - Clause « Information requise » https://aellaapp.com/privacy-policy
346 Politique de confidentialité d'Aella Credit - Clause 3.2 Informations collectées

	Informations partagées avec des tiers/ Divulgation d'informations Durée de l'accès des informations aux tiers	Aella credit partage ses informations avec : des prestataires de services Des entreprises affiliées, c'est-à-dire sa société mère, ses filiales, etc, Des sociétés qu'elle a engagées pour commercialiser ses produits D'autres sociétés lors de fusions, acquisitions, ventes d'actifs, procédures de liquidation ou de faillite Les autorités dans le but de prévenir les dommages Organismes compétents dans le cadre de l'exécution d'une décision de justice, de la défense d'un droit ou du respect de la loi. les agences d'évaluation du crédit pour signaler les mauvais payeurs ou pour publier des statistiques sur l'utilisation de l'application. Aucune indication
	Technologies de suivi/ cookies de site web	Utilise des cookies et des technologies de suivi
	Transferts internationaux de données	
	Stockage des informations sur l'utilisateur par l'application	Les données des utilisateurs peuvent être stockées et transférées hors du Nigeria et traitées par du personnel travaillant hors du Nigeria.

Analyse des pratiques de protection des données des applications

Limitation de l'objectif

Les applications de prêt sont tenues, en vertu de la règlementation sur la protection des données du Nigeria (RPDN), de traiter les données à caractère personnel à des fins spécifiques, légitimes et licites, sous réserve du consentement de la personne concernée.[347] La règlementation prévoit également que le processus de traitement complémentaire des données personnelles par ces applications ne doit être effectué qu'à des fins d'archivage, de recherche scientifique, de recherche historique ou de statistiques dans l'intérêt du public.[348]

Les applications étudiées ci-dessus, indiquent la finalité de la collecte de données à caractère personnel, qui comprend, entre autres, la fourniture de services (c'est-à-dire des prêts), l'évaluation du crédit et le marketing. Toutefois, la question est de savoir si les données collectées sont pertinentes quant à l'objectif de la collecte de données. Une étude des politiques de confidentialité des applications (comme indiqué ci-dessus) montre qu'elles sont excessives et contraires à l'objectif du prêt numérique. Il s'agit notamment des données stockées dans l'appareil d'un utilisateur, telles que la liste des contacts, l'historique des appels, les photos et les vidéos ; les informations et les contacts sur les réseaux sociaux (y compris les informations de connexion) ; la description personnelle de l'utilisateur ; les informations financières et de crédit; les collègues; et la liste des membres de la famille. La collecte de ce type d'informations est intrusive et viole le droit à la vie privée de la personne concernée.

Ce type d'information n'est pas nécessaire pour les prêts numériques, et les applications

347 Article 2.1. (1) (a) RPDN
348 Article 2.1 (1) (a) (i) RPDN

doivent s'en tenir à la collecte des données personnelles nécessaires au prêt.

Conservation des données

Le RPDN exige que ces applications indiquent clairement la durée de conservation des données et les critères utilisés pour déterminer cette durée.[349] Le règlement précise en outre que ces applications ne doivent stocker les données personnelles des utilisateurs que pour la période pendant laquelle elles sont nécessaires. Le règlement précise en outre que ces applications ne doivent conserver les données personnelles des utilisateurs que pendant la période au cours de laquelle elles sont nécessaires.[350]

Les applications examinées ci-dessus ne respectent pas ce principe. Certaines applications permettent de supprimer les données après qu'elles ont été utilisées aux fins indiquées. Cependant, elles mettent toujours un avertissement contraire au principe de suppression. L'application Carbon, par exemple, indique que les données à caractère personnel sont supprimées après que leur objectif, à savoir le prêt, a été atteint.[351] Elle précise toutefois que, malgré la suppression des données, celles-ci seront toujours conservées sur leur support de sauvegarde ou d'archivage à des fins juridiques, fiscales ou réglementaires.[352] Cela signifie en définitive que Carbon disposera toujours des données d'un utilisateur malgré la suppression et la réalisation de son objectif. Il convient également de noter que Carbon n'indique pas les critères utilisés pour déterminer la période de conservation des données.[353]

Palm Credit, en revanche, fait un effort supplémentaire pour montrer les critères utilisés pendant la période de conservation des données.[354] Cependant, la politique de confidentialité de l'application indique que même si un utilisateur désinstalle l'application, celle-ci peut conserver les données de l'utilisateur sous une forme agrégée et anonyme.[355] La politique indique également que l'application peut toujours conserver les données d'un utilisateur afin de se conformer aux obligations légales, de résoudre les litiges et de faire respecter ses accords.[356] Ces éléments réunis indiquent que les données ne seront pas supprimées et qu'elles seront toujours en possession de l'application.

L'application Branch ne comporte pas de clause sur la conservation des données. QuickCheck, en revanche, permet aux utilisateurs de voir, modifier ou supprimer leurs données, à l'exception de leur nom d'utilisateur.[357] L'appli Aella indique que les données des utilisateurs ne seront pas conservées sous une forme permettant de les identifier plus longtemps que nécessaire pour la collecte des données.[358]
Sécurité des données

Le RPDN définit des mesures détaillées que ces applications doivent suivre pour garantir la sécurité des données personnelles des utilisateurs. Il stipule que ces applications doivent protéger les données privées des utilisateurs contre tous les risques et violations prévisibles tels que le vol, les cyberattaques, les attaques virales, la diffusion, la manipulation ou les préjudices.[359] Pour ce faire, le RPDN exige que ces applications utilisent des mesures de sécurité telles que la protection du système contre les pirates, la mise en place de pare-feu, le stockage sécurisé des données avec un accès aux personnes spécifiquement autorisées, l'utilisation de technologies de cryptage des données,

349 Article 2.13.6 (g), RPDN
350 Article 2.1. (1) (c), RPDN
351 Politique de confidentialité de l'application Carbon ; Clause de conservation des données
352 Politique de confidentialité de l'application Carbon ; Clause de conservation des données
353 Ibid
354 Politique de confidentialité de Palm Credit : Clause de conservation des données
355 Politique de confidentialité de Palm Credit : Clause de conservation des données
356 Politique de confidentialité de Palm Credit : Clause de conservation des données
357 Politique de confidentialité de Palm Credit : Clause de conservation des données
358 Politique de confidentialité d'Aella App : Clause 1.4
359 Article 2.1 (1) (d) RPDN

le développement d'une politique organisationnelle pour le traitement des données personnelles, la protection des systèmes de messagerie électronique et le renforcement des capacités du personnel.[360]

Ces mesures sont essentielles compte tenu de la quantité de données collectées par ces applications de prêt. Cependant, certaines mesures concernant la sécurité des données par ces applications suscitent beaucoup d'inquiétude. Carbon et Palm Credit, par exemple, ne garantissent pas aux utilisateurs la protection des données qu'ils transmettent à l'application, c'est-à-dire les mots de passe lors des activités de connexion.[361] Elles indiquent que cette transmission se fait aux risques et périls de l'utilisateur.[362] Cette situation est très déplorable pour un utilisateur qui a un besoin urgent des services de l'Application. Les applications conformes au RPDN sont tenues, dans de telles circonstances, d'utiliser une technologie de cryptage pour protéger les données personnelles des utilisateurs transmises à l'application lors d'activités telles que les connexions. Les seules applications qui utilisent une technologie de cryptage sont Branch et QuickCheck.[363]

Les applications ont mis en place un certain degré de sécurité ; cependant, certaines ont des mesures de sécurité plus complètes que les autres. Il s'agit de Branch et QuickCheck.

Consentement de la personne concernée

Ces applications sont tenues, en vertu du RPDN, de s'assurer de la légalité de leurs activités de traitement de données. Les applications ne doivent traiter les données à caractère personnel qu'avec le consentement de la personne concernée et dans un but précis en assurant la légalité.[364] Le RPDN oblige en outre ces applications à informer les personnes concernées de l'intention de la collecte de données afin de s'assurer que la personne concernée donne son accord dans une démarche avisée.[365]

L'auteur estime que les applications ne permettent pas aux utilisateurs de donner leur consentement librement. En effet, les services offerts par les applications dépendent du consentement de l'utilisateur, et si ce dernier s'oppose au traitement de ses données, les applications lui refusent l'accès aux services.

Deuxièmement, le RPDN précise que, pour évaluer si le consentement a été donné librement, il convient d'examiner si la fourniture d'un service est soumise au consentement du traitement de données à caractère personnel qui ne sont pas nécessaires ou (excessives) pour l'exécution du contrat.[366]

Dans ce cas, l'accès aux services de prêt à partir des applications est lié à l'accès des applications aux données inutiles et superflues qui violent la vie privée des utilisateurs. Les applications exigent l'accès à des données inutiles à des fins de prêt, telles que des informations sur les réseaux sociaux, la liste de contacts de l'utilisateur et la liste des membres de sa famille, des SMS, des photos et des vidéos de l'utilisateur, entre autres, qui portent atteinte à la vie privée de l'utilisateur.

Publicité et transparence de la politique de confidentialité

En vertu de l'article 2.5 du RPDN, tout média qui traite des données personnelles est tenu d'afficher une politique de confidentialité claire et précise que les personnes concernées

360 Article 2.6 RPDN
361 Politique de confidentialité de Carbon and Palm Credit : Clauses de sécurité
362 Ibid
363 Clauses de sécurité de Branch et QuickCheck.
364 Article 2.2 (a) RPDN
365 Article 2.3 RPDN
366 Article 2.3 (2) (d) RPDN

peuvent comprendre. La politique de confidentialité doit contenir :[367]

- Ce en quoi consiste le consentement de la personne concernée.
- La description des informations personnelles pouvant être collectées.
- Objectif de la collecte des données personnelles.
- Les méthodes techniques utilisées pour collecter et stocker les informations personnelles et les cookies.
- L'accès des tiers aux données personnelles et la finalité de cet accès.
- Une mise en évidence des principes de la protection des données.
- Les recours disponibles en cas de violation.
- Le délai de mise en œuvre des recours.
- Branch ne le fait pas. Sa politique n'est pas aussi détaillée que l'exige cette règle.

Traitement des données par des tiers

Le RPDN exige que le traitement des données par des tiers soit régi par un contrat écrit entre le tiers et le responsable du traitement des données.[368] Il stipule également que les responsables du traitement des données qui engagent des tiers pour traiter les données personnelles des personnes concernées doivent s'assurer du respect du RPDN.[369] Aucune des applications étudiées n'a conclu de contrat avec les tiers avec lesquels elles partagent les informations des utilisateurs. Certaines d'entre elles, notamment QuickCheck et Branch, n'indiquent pas les tiers avec lesquels elles partagent ces informations. Ce qui est encore plus inquiétant, c'est que ces applications ne montrent pas les mesures qu'elles prendront pour s'assurer que les tiers avec lesquels elles partagent les informations des utilisateurs respectent du RPDN.

Transfert vers un pays étranger

Le RPDN énonce les questions essentielles à prendre en considération concernant le transfert de données vers un pays étranger. Il stipule qu'un tel transfert doit avoir lieu sous réserve des dispositions du RPDN et de la supervision de l'Honorable Procureur général de la Fédération (HAGF).[370]Le point essentiel à prendre en compte est que le pays étranger doit avoir un niveau de protection des données adéquat.[371] Le l'Honorable Procureur général de la Fédération doit évaluer le système juridique du pays étranger en ce qui concerne l'État de droit et la protection des droits de l'homme, entre autres.[372]

Le RGPD prévoit également une exception à cette règle.[373] Il établit que les données à caractère personnel doivent être transférées vers un pays étranger si la personne concernée y a consenti,[374] lorsque le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement.[375] La personne concernée doit être informée des garanties appropriées en matière de protection des données dans le pays étranger.[376]

Droits de la personne concernée

Le RGPD accorde aux personnes concernées des droits au sujet du traitement de leurs données.[377] Il indique qu'avant le traitement des données personnelles d'une personne concernée, le responsable du traitement doit informer la personne concernée de l'identité et des coordonnées du responsable du traitement, des coordonnées du délégué à la

367 Article 2.5 RPDN
368 Article 2.7 RPDN
369 Ibid
370 Article 2.11 RPDN
371 Article2.11 (a) RPDN
372 Article 2.11 (b) RPDN
373 Article 2.12 RPDN
374 Article 2.12 (a) RPDN
375 Article 2.12 (b) RPDN
376 Article 3.1 (8) RPDN
377 Article 3.1. (7) RPDN

protection des données, de la finalité du traitement, de l'intérêt légitime poursuivi par le responsable du traitement, des destinataires des données personnelles, de l'intention de transférer les données vers un pays tiers, la période pendant laquelle les données à caractère personnel seront conservées et les critères de détermination de cette période, le droit de la personne concernée à demander l'accès, la rectification ou l'effacement des données à caractère personnel, le droit de la personne concernée de retirer son consentement, l'existence d'une prise de décision et d'un profilage automatisés, des informations sur la finalité d'un traitement ultérieur et des informations sur le transfert de données à caractère personnel vers un pays étranger.

Certaines des applications étudiées, comme Aella App, QuickCheck et Carbon, ne fournissent pas les coordonnées du responsable de la protection des données et n'indiquent pas si les organisations disposent de responsables de la protection des données. Branch et Palm Credit sont les seules applications à disposer de responsables de la protection des données. Comme nous l'avons vu dans la section précédente, les applications indiquent la finalité du traitement des données ;

Certaines des applications étudiées informent les destinataires qui utilisent les données des utilisateurs, d'autres non. Les applications indiquent également leur intention de transférer des données personnelles vers des pays étrangers mais n'indiquent pas les mesures de sauvegarde pour protéger les données dans les pays étrangers. The only App that gives users room the right to request access, rectification and deletion of data is Palm Credit. La seule application qui donne aux utilisateurs le droit de demander l'accès, la rectification et la suppression des données est Palm Credit. Les autres applications ont tendance à limiter ce droit. Par exemple, Branch ne donne aux utilisateurs que le droit de demander la rectification lorsque les informations sont inexactes, et Carbon n'offre aux utilisateurs que le droit de s'opposer au traitement de leurs données à des fins de marketing.

Seules deux applications permettent aux utilisateurs d'exercer leur droit à la mobilité des données, à savoir Quick Check et Palm Credit.[378]

Humiliation publique

Les applications de prêt numérique au Nigéria sont également connues pour leur réputation d'humiliation publique.[379] Ces applications contiennent des clauses dans leurs politiques de confidentialité qui leur donnent le droit de contacter les relations d'un utilisateur en cas de défaut de paiement de ce dernier.[380] Certaines applications vont jusqu'à publier les emprunteurs défaillants sur les réseaux sociaux et à les dépeindre comme des criminels.[381] Tout cela est fait pour que l'emprunteur paie sa dette. Cependant, de tels actes violent la vie privée de l'emprunteur et portent atteinte à sa réputation.

Les applications les plus connues pour cette pratique sont OKash, Soko Loan, Palm Credit, Credit9ja et Fast Money.[382] Dans leurs politiques de confidentialité, ces applications indiquent expressément qu'elles peuvent utiliser les contacts d'un utilisateur si celui-ci ne paie pas. Ces dispositions sont contraires au RPDN, qui interdit le traitement illégal des données à caractère personnel.[383] La National Information Development Agency (NITDA) devrait prendre des mesures à l'égard de ces pratiques et veiller à ce que ces applications traitent les données personnelles de manière équitable et légale. L'Agence a récemment

378 Politique de confidentialité de Quick Check : Clause des droits de l'utilisateur Politique de confidentialité de Palm Credit : Clause sur les droits de l'utilisateur

379 https://twitter.com/EthanZ/status/1429845838751207432?s=19

380 L'intrusivité des applications de prêt d'argent au Nigeria https://aanoip.org/the-intrusiveness-of-money-lending-apps-in-nigeria/

381 Violation des droits numériques au Nigeria https://www.change.org/p/central-bank-of-nigeria-violation-of-digital-rights-of-nigerians

382 Violation des droits numériques au Nigeria https://www.change.org/p/central-bank-of-nigeria-violation-of-digital-rights-of-nigerians

383 Règle 2.2, Règlement sur la protection des données du Nigeria

sanctionné Soko Loan pour atteinte à la vie privée des emprunteurs après avoir reçu des plaintes concernant la divulgation injustifiée d'informations sur les utilisateurs, l'incapacité à protéger les informations personnelles des utilisateurs et la diffamation des utilisateurs.[384]

Protection de la vie privée par défaut ou par définition

Les applications doivent être techniquement conçues de manière à limiter leur collecte aux informations nécessaires pour les prêts. La conception technique des apps ne doit pas leur permettre d'accéder aux données confidentielles des utilisateurs sur leurs appareils, telles que les photos, les vidéos, les listes de contacts, les SMS et les informations sur les réseaux sociaux. Les concepteurs de l'application doivent la concevoir de manière à respecter la vie privée des utilisateurs.

Conclusion

On peut dire que les applications étudiées ne sont pas conformes au RPDN. Les applications traitent un grand nombre de données personnelles des personnes concernées qui vont à l'encontre du prêt numérique. La collecte d'une telle quantité de données est intrusive et viole le droit à la vie privée des personnes concernées. Les applications doivent se conformer strictement au RPDN et se limiter au traitement des données personnelles nécessaires au prêt numérique. Les applications partagent également ces données avec des tiers. Certaines (comme mentionné ci-dessus) n'indiquent pas les tiers avec lesquels elles partagent ces données. Elles n'informent pas les utilisateurs de la durée pendant laquelle les tiers auront accès aux données et des mesures qu'elles mettent en place pour garantir la sécurité des données partagées avec les tiers.

384 La NITDA sanctionne Soko Loan pour atteinte à la vie privée https://nitda.gov.ng/nitda-sanctions-soko-loan-for-privacy-invasion/

Afrique du Sud

Profile du Pays

L'Afrique du Sud, également connue comme la République d'Afrique du Sud, se trouve la partie la plus au sud de l'Afrique[385]. Elle partage une frontière avec la Namibie, le Botswana, le Zimbabwe, Et le Swaziland[386] et est parmi les lieux les plus visités en Afrique. L'Afrique du Sud-Est connue pour sa belle topographie et sa diversité culturelle.[387] Le pays a 11 langues officielles c'est-à-dire l'Afrikaans, l'Anglais, le Ndebele, le Sotho du Nord, le Sotho, le Swazi, le Tswana, le Tsonga, le Venda, le Xhosa, et le Zulu, avec le Zulu, le Xhosa, et l'Afrikaans qui sont les plus parlées.[388] Elle a trois capitales, c'est-à-dire, Pretoria, qui accueille l'Exécutif; Cape Town, qui accueille la Législature; et Bloemfontein, qui accueille le Judiciaire.[389] Le pays a une population de 60 millions d'habitants[390] et couvre une superficie de 1.221.037 kilomètres carrés.

385 Afrique du Sud https://www.britannica.com/place/South-Africa
386 Ibid
387 Ibid
388 Afrique du Sud https://www.nationsonline.org/oneworld/south_africa.htm
389 Ibid
390 Population de l'Afrique du Sud 2021 https://worldpopulationreview.com/countries/south-africa-population

Protection des Données en Afrique du Sud

Le Kenya, le Nigéria, et l'Afrique du Sud sont les pays leaders en Afrique dans l'écosystème fintech, avec 450 entreprises fintech.[391] L'Afrique du Sud a 200 entreprises fintech[392] réparties en plusieurs segments, c'est-à-dire les paiements, prêts, épargne, dépôts, entre autres.[393] Notre objectif principal dans cette étude est le secteur du crédit (prêt), qui croit à un rythme rapide.[394]

Le secteur du prêt comprend plusieurs plateformes, dont Pollen Finance, qui est considérée comme l'une des plus grandes plateformes de prêt du pays,[395] suivie par Lulalend et Fundrr.[396] L'industrie relève de la compétence du National Credit Act, loi de 2005, qui prévoit la régulation du secteur du crédit et la mise en place de l'autorité Nationale

391 Afrique du Sud, Nigeria et Kenya : Les plus grands Hubs Fintech d'Afrique <https://fintechnews.africa/39379/kenya/south-africa-nigeria-and-kenya-africas-largest-fintech-hubs/ > Consulté le 4/8/2021
392 Ibid
393 Champ d'application Fintech en Afrique du Sud <http://www.treasury.gov.za/comm_media/press/2020/WB081_Fintech%20Scoping%20in%20SA_20191127_final%20(002).pdf > Consulté le 4/8/2021
394 (n1)
395 (n3) pg 8 (n1)
396 (n1)

de Régulation du Crédit, qui est premièrement responsable de la supervision et de la régulation de ce secteur.[397] La loi exige que les fournisseurs de crédit s'enregistrent et rend le fournisseur national de crédit responsable de cet enregistrement.[398] Elle fournit également la procédure détaillée d'enregistrement des fournisseurs de crédit lors de la demande d'enregistrement auprès du fournisseur national de crédit.[399]

En matière de traitement de données, les plateformes de prêt doivent respecter la loi sur les protection des renseignements personnels (POPI Act) qui énonce les principes auxquels devraient adhérer ces plateformes pour assurer la sécurité des données personnelles en leur possession.[400] Il convient de noter que l'application de la loi POPI par le Régulateur de l'Information a commencé récemment le 1er juillet 2020, et les organisations ont bénéficié d'un délai de grâce d'un an à compter de la date d'entrée en vigueur, c'est-à-dire le 1er juillet 2020, pour se conformer à la loi.[401]

Ainsi les organisations (y compris les entités propriétaires plateformes de prêt) doivent s'assurer que leurs activités de traitement des données sont conformes à la loi POPI. Dans cette optique, l'étude vise à analyser les pratiques de protection des données de ces plateformes. Cela commence par l'examen de leurs politiques afin de mettre en évidence les données collectées par elles. Il s'ensuit alors une évaluation des données collectées vis-à-vis des dispositions de la loi pour établir si ces plateformes respectent la loi sur la protection des données.

Plateformes de prêt en ligne dans cette étude

Les plateformes de prêt en ligne dans cette étude fonctionnent via des sites internet, notamment Pollen Finance, Lulalend, et Fundrr. La seule plateforme qui fonctionne via une application est Niftycredit (GetBucks) qui peut être téléchargée via Google Play.

- Pollen Finance – Une des plus grandes plateformes de prêt en ligne dans le pays
- Lulalend - Prêt
- Fundrr - Prêt
- Nifty Credit (GetBucks) - Prêt

Aperçu des Données collectées par les Applications de prêt numérique

Pollen Finance[402] (Politique de confidentialité et Termes et Conditions)	Informations collectées et traitées par l'application	
	Autorisations demandées par l'application	
	Informations collectées chez l'utilisateur	Informations générales de l'entreprise Numéros de téléphones Une adresse postale, et Une adresse email
	Informations collectées à partir de l'appareil/ navigateur de l'utilisateur	Collecte automatiquement les informations suivantes, qui sont stockées dans ses journaux de serveurs : Adresse IP Information sur les cookies Page demandée

397 Loi sur le crédit national, 2005 (Act No. 34 of 2005) https://www.gov.za/sites/default/files/gcis_document/201409/a34-050_0.pdf
398 Article 14, Loi de 2005 sur le crédit national
399 Chapitre 3, Loi de 2005 sur le crédit national
400 Loi sur la protection des informations personnelles (loi POPI) https://popia.co.za/act/
401 La date de début ou la date d'entrée en vigueur de la POPI marque le début des opérations https://www.michalsons.com/blog/popi-commencement-date-popi-effective-date/13109
402 Pollen Finance Privacy Policy https://www.pollenfinance.co.za/privacy-policy/

	Informations reçues des tiers	
	Utilisation des informations de l'utilisateur par l'application	Les informations de l'utilisateur sont utilisées aux fins suivantes : Envoi de communications et de mises à jour concernant le site Web ou les services de Pollen Finance La plateforme utilise des cookies pour suivre les sessions d'un utilisateur et les enregistrer sur ses navigateurs et ses disques durs. L'adresse IP de l'utilisateur est également utilisée pour identifier les problèmes sur le site Web et l'administrer.
	Informations utilisées par des tiers Durée d'accès des tiers	Pollen Finance partage des informations avec des tiers pour diffuser des publicités et des communications en ligne. Les tiers utilisent les données pour évaluer le type d'offres, de promotions et de publicités susceptibles d'intéresser les utilisateurs de la plateforme. Cependant, les données partagées sont agrégées et ne sont liées à aucun utilisateur de la plateforme. La plate-forme offre aux utilisateurs qui ne souhaitent pas que leurs données soient utilisées dans des publicités un espace pour exercer leur option de désinscription.
	Divulgation d'informations	Pollen Finance divulgue les informations de l'utilisateur aux fins suivantes : Statistiques de marché : divulgue des statistiques globales aux annonceurs et aux partenaires commerciaux Fournisseurs et agents tiers : le tiers est tenu d'utiliser les données uniquement pour fournir les services demandés Application de la loi : Divulgue les données quand ; requis par la loi, protéger la sécurité d'un individu et prévenir la violation de la loi. L'adresse IP peut également être divulguée si nécessaire dans le cadre d'une procédure judiciaire ou si la loi l'exige Changement de propriétaire : Fusions, acquisitions, cessions d'actifs Employés de Pollen Finance
	Technologies de suivi/Cookies de site internet	La plateforme utilise des cookies pour suivre les sessions d'un utilisateur et les enregistrer sur ses navigateurs et ses disques durs. L'adresse IP de l'utilisateur est également utilisée pour identifier les problèmes sur le site Web et l'administrer.
	Stockage/Sécurité des données	"Le site Web est hébergé dans un environnement de serveur sécurisé qui utilise un pare-feu et d'autres mesures de sécurité pour empêcher les interférences ou l'accès d'intrus extérieurs."

	Transfert transfrontalier	Pollen Finance peut transférer les données des utilisateurs en dehors de la juridiction de résidence vers d'autres pays, y compris des pays qui n'ont pas de lois proportionnelles (niveaux) sur la protection des données.

Lulalend[403]	Informations collectées et traitées par l'application	
	Autorisations demandées par l'application	
	Informations collectées chez l'utilisateur	Nom, numéro d'enregistrement/date de naissance, adresse physique et postale, adresse e-mail, numéro de téléphone, sexe/nationalité/origine ethnique et origine sociale/âge, informations financières, opinion personnelle/opinions/préférences, correspondance confidentielle envoyée par un utilisateur, opinions / opinions d'autrui sur un utilisateur, informations de crédit et historique de l'utilisateur,
	Informations collectées sur l'appareil de l'utilisateur	Une fois qu'un utilisateur visite le site internet de Lulalend, les serveurs du site Web collectent automatiquement des informations techniques concernant la visite et l'ordinateur de l'utilisateur. Ces informations comprennent des détails sur l'ordinateur de l'utilisateur, l'adresse IP, le système d'exploitation et le type de navigateur, l'emplacement et les informations d'utilisation.
	Informations reçues des tiers	
	Utilisation des informations de l'utilisateur/Finalité de la collecte de données	Lulalend utilise les données d'un utilisateur aux fins suivantes : Prise de décision sur l'opportunité de conclure un contrat avec un utilisateur Exécution des obligations au titre du contrat Respect d'une obligation légale Protection de l'intérêt légitime de l'utilisateur Poursuite de l'intérêt légitime de Lulalend À des fins d'évaluation du crédit A des fins de marketing direct Personnalisation et affichage de contenus tels que produits, articles, publicités, etc. Envoyer du contenu sur des articles, des produits, des publicités, etc., Informer les utilisateurs des changements sur le site Web

403 Politique de confidentialité de Lulalend https://www.lulalend.co.za/PrivacyPolicy

	Informations reçues des tiers Durée d'accès du tiers	Lulalend partage des informations personnelles avec les tiers suivants : Banques ou institutions financières de l'utilisateur Fournisseurs de services de bureau de crédit Prestataires de services professionnels fournissant des services d'assistance juridique, de comptabilité ou d'audit Fournisseurs de services de livraison et de messagerie Fournisseur de passerelle de paiement Lulalend peut partager les informations agrégées de l'utilisateur et les habitudes d'utilisation du site Web à des fins publicitaires
	Stockage des informations de l'utilisateur par l'application/ Garanties de sécurité	.Lulalend s'engage à protéger les données personnelles contre la perte, la destruction et l'accès non autorisé Lulalend identifie les risques potentiels pour les informations personnelles et met en place des mesures de protection contre ces risques Lulalend garantit que ses contrats avec des tiers comportent les obligations suivantes : Les tiers ne sont pas autorisés à traiter des informations personnelles sans le consentement de Lulalend Les tiers doivent traiter les informations personnelles de manière confidentielles et ne pas les partager avec des parties non autorisées Tiers pour utiliser des mesures de sécurité de la même norme que Lulalend Tiers pour informer Lulalend lorsque des parties non autorisées ont accédé à des informations personnelles Si un tiers est situé dans un autre pays, il doit se conformer aux lois sur la protection des données de ce pays Si un tiers est légalement tenu de divulguer des informations sur l'utilisateur, il doit en informer Lulalend

	Transferts transfrontaliers des informations personnelles	Lulalend transfère les données d'un utilisateur vers un autre pays sous réserve de consentement. Les données sont transmises dans les circonstances suivantes : Lorsque le transfert est nécessaire à l'exécution du contrat entre Lulalend et l'utilisateur Lorsque le transfert est requis pour l'exécution de mesures précontractuelles Le transfert est au profit de l'utilisateur L'utilisateur a consenti au transfert Stocker électroniquement les informations de l'utilisateur dans une base de données sécurisée Les fournisseurs de services de Lulalend ont le droit de transmettre les données des utilisateurs par voie électronique dans des bases de données hébergées en dehors de l'Afrique du Sud à condition qu'ils aient le même niveau de sécurité, de politique et de procédures en matière de protection des données que Lulalend.
	Technologie de Suivi et Cookies	Lulalend utilise des cookies sur son site Internet pour : Distinguer les utilisateurs Gardez une trace des sessions des utilisateurs sur le site Web Stocker des informations sur les préférences des utilisateurs Estimer la taille de l'audience du site Web et l'utilisation du modèle Augmenter la vitesse des recherches
Fundrr[404]	Informations collectées et traitées par l'application	
	Autorisations demandées par l'application	
	Informations collectées chez l'utilisateur	Fundrr recueille les informations suivantes auprès des utilisateurs : adresse IP Informations de contact Informations sur les affaires Informations financières, et Toute information requise par Fundrr
	Informations collectées sur l'appareil de l'utilisateur	(Protocole Internet) Adresse IP Adresse du nom de domaine Identité du service Internet ou du fournisseur d'accès Type de logiciel de navigation Web Système d'exploitation informatique URL de la page visitée par un utilisateur sur le site La langue sélectionnée par un utilisateur pour un logiciel de navigation Web
	Informations reçues des tiers	

404 Politique de confidentialité de Fundrr https://fundrr.co.za/privacy-policy/

	Utilisation des informations de l'utilisateur par l'application	
	Informations partagées avec des tiers/Partage des informations personnelles Durée d'accès du tiers	Fundrr partage des informations avec des tiers dans les circonstances suivantes : Lors du traitement d'informations à des fins d'évaluation du crédit Lors de l'enregistrement des services d'organisations partenaires Lors de l'enrôlement des services de tiers fournisseurs de services tels que ; facturation et recouvrement de créances, services liés au crédit (tels que la solvabilité, la notation de crédit, la liste des défauts, etc.), entre autres
	Technologie de suivi et Cookies	Les informations recueillies par les cookies sont stockées et utilisées pour créer des profils sur les utilisateurs du site internet. Le rapport permet à Fundrr de connaître les préférences, l'utilisation et l'activité comportementale de l'utilisateur.
	Stockage des informations de l'utilisateur par l'application/ Sécurité	Informations stockées dans un serveur sécurisé pendant une période légalement requise de Fundrr
Niftycredit (GetBucks)[405]	Informations collectées et traitées par l'application	
	Autorisations demandées par l'application	

405 Politique de confidentialité de Nifty Credit https://niftycredit.co.za/za/terms-and-conditions

	Informations collectées chez l'utilisateur	Les informations collectées auprès des utilisateurs par Niftycredit incluent : Informations générales : nom, numéro d'identification, sexe, date de naissance, adresse résidentielle, coordonnées telles que l'adresse e-mail et le numéro de téléphone Informations sur l'emploi : historique des emplois, formation, qualifications, expérience, données démographiques, données géographiques et informations sur les salaires Informations sur la demande : informations fournies lors de la demande, y compris les actifs, les revenus et les dettes Informations sur le compte : informations sur le compte bancaire, prêt Informations sur les transactions : informations relatives aux transactions et à l'activité du compte, telles que les soldes des comptes, l'historique des paiements et l'utilisation du compte Informations sur le rapport du consommateur : Informations obtenues à partir des cookies Enregistrements téléphoniques Préférences marketing de l'utilisateur Identifiants tels que (protocole Internet) adresse IP Les informations sont obtenues d'un utilisateur lorsque : Affichage du site Web de Niftycredit Ouvrir un compte / demander des services Niftycredit Contacter Niftycredit par e-mail, réseaux sociaux ou téléphone Des informations sont également obtenues auprès de tiers qui : Surveiller l'utilisation du site Web Réaliser des études de marché, des sondages et des analyses commerciales et statistiques
	Informations collectées de l'appareil de l'utilisateur	
	Informations reçues de tiers	

	Utilisation des informations de l'utilisateur par l'application	Niftycredit utilise les informations des utilisateurs aux fins suivantes : Fourniture de produits et services Facilitation des transactions Entretien, maintenance ou recouvrement de comptes Applications du produit et évaluation de l'éligibilité de l'utilisateur Effectuer des recherches ou des vérifications de références de crédit Réalisation d'un scoring et d'une évaluation de crédit Réaliser la gestion des risques Assurer la sécurité des utilisateurs Vérification des comptes Confirmation et vérification de l'identité de l'utilisateur Recouvrement de créances Conformité aux exigences légales et réglementaires, entre autres
	Informations partagées avec des tiers/Partage des information personnelles	Niftycredit partage l'actualité avec les membres de son groupe et des conseillers professionnels pour obtenir des conseils professionnels et défendre des actions en justice, entre autres. Il partage également des informations avec les tiers suivants : Fournisseurs de systèmes de paiement, agences de recouvrement de créances, agents de recherche et fournisseurs surveillant l'utilisation des médias sociaux Fournisseurs informatiques, auditeurs, agences marketing, fiscalistes, etc., Les organismes d'application de la loi Cabinets d'avocats ou organisations fournissant des conseils juridiques ou une représentation juridique Fournisseurs d'enquêtes Régulateurs et autorités gouvernementales, médiateurs ou autorités fiscales
	Technologie de suivi et cookies	Utilise des cookies aux fins suivantes : Authentification des utilisateurs Statut d'utilisation du site par l'utilisateur (c'est-à-dire si un utilisateur est connecté au site) Personnalisation du site pour les utilisateurs Protection du compte de l'utilisateur et prévention des connexions frauduleuses Publicité Analyse des performances du site
	Stockage des informations de l'utilisateur par l'application/ Transfert international de données	Demande le consentement de l'utilisateur dans les cas où les données sont traitées en dehors du pays. Lorsque les serveurs, fournisseurs ou prestataires de services sont basés en dehors du pays, ou lorsque les serveurs sont basés en dehors de l'Afrique du Sud, Niftycredit demandera à la partie à laquelle les données de l'utilisateur sont transférées d'accepter ses principes et pratiques de confidentialité.

Analyse des pratiques de protection de données sur les Plateforme numérique de prêts

Responsabilité

La loi sur la protection des informations personnelles (loi POPI) [406] oblige les plateformes de prêt en ligne, entre autres organismes, à traiter les données personnelles pour garantir la responsabilité lors du traitement des données. Elle leur impose notamment de respecter les conditions fixées par la loi pour un traitement licite. Ces conditions doivent être appliquées lors de la détermination de la finalité et les moyens du traitement des données personnelles[407].

Les conditions comprennent la responsabilité, la limitation du traitement, la spécification de la finalité, la limitation du traitement ultérieur, la qualité des informations, l'ouverture, les garanties de sécurité et la participation des personnes concernées, comme indiqué dans les sections suivantes[408].

Limitation des traitements

Cette condition comporte plusieurs principes. [409] Premièrement, elle exige que les données à caractère personnel soient traitées de manière licite et raisonnable, sans porter atteinte au droit à la vie privée de la personne concernée[410]. Deuxièmement, elle exige que les données personnelles soient collectées directement auprès de la personne concernée, sauf dans des circonstances exceptionnelles prévues par la loi[411]. Troisièmement, elle exige que les données à caractère personnel soient traitées aux fins pour lesquelles elles ont été collectées et que ces données soient adéquates, pertinentes et non excessives. Enfin, cette condition requiert que cette collecte de données soit soumise au consentement de l'utilisateur, avec une justification raisonnable du traitement. L'utilisateur a le droit de s'opposer à un tel traitement. [412]

Un examen des plateformes de prêt en ligne dans cette étude indique que les sociétés de crédit obtiennent automatiquement des données personnelles une fois qu'un utilisateur se connecte à leur site internet, soumet des détails lors de l'inscription ou utilise les produits. Les utilisateurs qui ne consentent pas/qui s'opposent au traitement de leurs données sont invités à cesser d'accéder aux sites internet et sont automatiquement privés des produits proposés par les sites internet. Dans ce cas, on peut dire que le consentement n'est pas donné par le libre arbitre de l'utilisateur mais par le besoin de celui-ci d'accéder au produit. Certaines des plateformes étudiées collectent des informations non pertinentes et non conformes à ces traitements. Niftycredit, par exemple, collecte des informations telles que l'historique des emplois, l'expérience, les coordonnées bancaires et les lectures téléphoniques d'un utilisateur qui ne sont pas pertinentes aux fins de crédit[413]. Lulalend, quant à elle, recueille des informations telles que l'origine ethnique de l'utilisateur, l'opinion personnelle/point de vue et les opinions personnelles/les points de vue d'autres personnes sur l'utilisateur, qui ne sont pas pertinents[414].

Lulalend se conforme à l'exigence de collecter des informations de l'utilisateur directement auprès de ce dernier et fournit des circonstances exceptionnelles conformément à la loi

406 Loi sur la protection des informations personnelles (loi POPI), loi 4 de 2013 https://popia.co.za/
407 Article4 (1) (a) de la loi POPI
408 Article 4, Loi POPI
409 Article 4 (1) (b), Loi POPI
410 Article 4 (1) (9), Loi POPI
411 Article 12 de la loi POPI
412 Article 11 de la loi POPI
413 Politique de confidentialité de Nifty Credit https://niftycredit.co.za/za/terms-and-conditions
414 Politique de confidentialité de Lulalend https://www.lulalend.co.za/PrivacyPolicy

POPI où la conformité peut ne pas être respectée[415].

Conservation des données

Les plateformes de prêt en ligne sont tenues en vertu de la loi POPI de ne pas conserver les informations personnelles plus longtemps que nécessaire pour atteindre l'objectif de la collecte. [416] Elle stipule que l'entreprise ne disposera de données personnelles durant de longues périodes uniquement si la loi l'exige. La plateforme de prêt l'exige dans un but licite, une conservation de données implique un contrat entre les parties, ou un consentement de la personne concernée[417].

Les plateformes examinées dans cette étude ont mentionné ce principe dans leurs politiques de confidentialité, indiquant expressément que l'entreprise supprimera les données des utilisateurs une fois que l'objectif de cette collecte aura été atteint[418]. Cependant, d'autres plateformes telles que Fundrr et Nifty Credit exigent que les utilisateurs demandent la suppression de leurs informations. En revanche, Pollen Finance ne fait aucune mention de ce principe dans sa Politique de Confidentialité, et il n'est pas clair s'il respecte ce principe.

Garanties de Sécurité

La loi POPI impose à ces plateformes de prêt en ligne de sécuriser l'intégrité et la confidentialité des informations personnelles en leur possession en prenant des mesures appropriées, raisonnables, techniques et organisationnelles pour prévenir; la perte, l'endommagement ou la destruction non autorisée de données personnelles et l'accès illégal à des informations confidentielles[419]. Dans cette optique, elle ajoute que ces plateformes devraient prendre des mesures raisonnables pour: identifier tous les risques prévisibles pour les informations personnelles, maintenir des garanties appropriées contre les risques identifiés, vérifier que les sécurités sont mises en œuvre et s'assurer que les garanties sont continuellement mises à jour en réponse à de nouvelles menaces[420].

En cas d'atteinte à la sécurité, ces plateformes sont invitées à en informer le Régulateur et la personne concernée[421]. Concernant les tiers traitant des informations personnelles pour le compte de ces plateformes, la loi leur impose de; traiter ces données avec l'autorisation de ces plateformes et traiter ces données de manière confidentielle[422]. Lulalend et Nifty credit semblent avoir intégré ces mesures dans leurs politiques de confidentialité parmi les plateformes de cette étude. Les politiques de confidentialité de Fundrr et Pollen Finance, en revanche, ne s'engagent qu'à assurer la sécurité des données personnelles mais n'indiquent pas aux utilisateurs les mesures de sécurité que les plateformes prendront pour assurer la confidentialité de leurs informations personnelles

Droits de l'Utilisateur et Participation

Les personnes concernées disposent de droits concernant leurs données. En particulier, elles ont le droit d'accéder à leurs informations personnelles[423] et le droit d'en demander la rectification[424]. La loi prévoit en outre l'accès à l'information dans le cadre des dispositions de la loi sur la promotion de l'accès à l'information (PAIA). [425]

415 Politique de confidentialité de Lulalend https://www.lulalend.co.za/PrivacyPolicy
416 Article 14 de la loi POPI
417 Article 14 (1), Loi POPI
418 Politique de confidentialité de Lulalend https://www.lulalend.co.za/PrivacyPolicy
419 Article 19 de la loi POPI
420 Article 19 (2), Loi POPI
421 Article 22 (1), Loi POPI
422 Article 21 (1), POPI
423 Article 23 de la loi POPI
424 Article 24 de la loi POPI
425 Article 25 de la loi POPI

Les plateformes permettent aux utilisateurs d'accéder, de corriger et de mettre à jour leurs informations personnelles. Elles fournissent également des pistes (c'est-à-dire des coordonnées) sur la façon dont cela peut être fait. Les plateformes permettent en outre aux utilisateurs de faire part de leurs préoccupations et de déposer des plaintes.

Option de désinscription

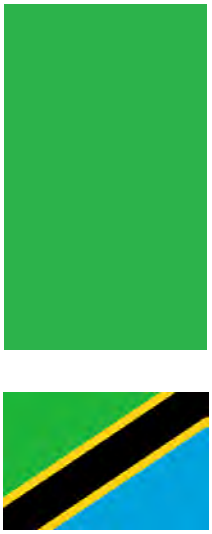
L'exigence de consentement en ligne dans le cadre du POPIA concernant le marketing par voie électronique signifie que[426] Toutes les plateformes étudiées offrent aux utilisateurs la possibilité de se désinscrire des messages publicitaires/marketing.

Conclusion

En conclusion, les politiques de confidentialité de certaines des plateformes de cette étude peuvent être conformes à POPIA. Cependant, cette conformité ne se situe qu'au niveau de la politique. Nous sommes impatients de voir si les plateformes seront conformes au POPIA dans la pratique, étant donné qu'elle est entrée en vigueur le 1er juin.

426 Article 69 de la loi POPI

Tanzanie



Profil du Pays

Située en Afrique de l'Est, la République-Unie de Tanzanie est limitée à l'est par l'océan indien. Elle a des frontières terrestres avec huit pays : (dans le sens inverse des aiguilles d'une montre à partir du nord) le Kenya, l'Ouganda, le Rwanda, le Burundi, la République démocratique du Congo (de l'autre côté du lac Tanganyika), la Zambie, le Malawi et le Mozambique. Le pays comprend Zanzibar (l'île principale d'Unguja, plus Pemba et d'autres îles plus petites). [427] La population du pays est estimée à 59 734 210 habitants en 2020. [428]

‘

427 https://www.eac.int/eac-partner-states/tanzania
428 https://data.worldbank.org/indicator/SP.POP.TOTL?locations=TZ

Protection de données en Tanzanie

En 2014, Vodacom Tanzania est devenu un précurseur dans l'écosystème fintech en Tanzanie. Ce changement a résulté de son partenariat avec Commercial Bank of Africa - CBA (aujourd'hui NCBA), pour lancer MPawa, un produit bancaire révolutionnaire permettant aux abonnés de Vodacom d'économiser de l'argent via leur téléphone, d'obtenir des intérêts sur leurs économies et éventuellement d'obtenir des microcrédits. [429]

Depuis lors, l'écosystème fintech en Tanzanie a suivi une trajectoire rapide et ascendante, culminant avec la montée et la popularité des applications financières pour les consommateurs.

Plus de 54 % de la population tanzanienne utilise les services de paiement mobile et de transactions monétaires[430].

Les institutions bancaires traditionnelles, les institutions non bancaires et les opérateurs de téléphonie mobile - les ORM (avec leurs portemonnaies électroniques) ont lancé leurs propres applications mobiles de prêt au fil des ans. Ceux-ci incluent mais ne sont pas limités à; TigoPesa Nivushe[431], Branch[432], Halotel Haloyako, [433] etc.

La Tanzanie n'ayant pas de législation sur la protection des données et la confidentialité, [434] la

429 https://www.vodacom.co.tz/mpawa
430 https://www.statista.com/statistics/1082056/tanzania-mobile-money-transaction-value/
431 https://www.tigo.co.tz/tigo-pesa-nivushe
432 https://branch.co.tz
433 https://halotel.co.tz/package-mobile/1552657603579
434 https://www.mwananchi.co.tz/mw/habari/kitaifa/usalama-taarifa-binafsi-shakani-3006726

nature prédatrice de certaines de ces applications est susceptible de mettre en danger la vie privée et les données personnelles des utilisateurs.

Aperçu des Données collectées par les Applications de prêt numérique

Vodacom MPawa[435]	Données collectées et traitées par l'application	
	Autorisations demandées par l'application	Cette application a accès à : Coordonnées téléphoniques Localisation (GPS et réseau) SMS de l'utilisateur Statut et identité du téléphone Contenu du stockage de l'appareil Appareil photo ID de l'appareil et informations sur les appels Connexions internet (réseau)
	Données Utilisateur collectées	Le cas échéant : Nom, adresse, numéro de téléphone et de portable, date de naissance, sexe et adresse e-mail ; Informations de carte de crédit ou de débit, informations sur le compte bancaire et autres informations bancaires
	Informations collectées chez l'utilisateur	Référence de l'appareil Données de trafic. Données de localisation ; Données du système de positionnement global (GPS)/points d'accès Wi-Fi/adresse IP ou informations telles qu'un code postal ou le nom d'une ville ou d'une cité ;
	Informations reçues des tiers	Référence de crédit
	Utilisation des données Utilisateur par l'application	Traiter les commandes et fournir à un utilisateur des produits et services Améliorer et innover les produits et services Service de marketing et de personnalisation à un utilisateur Profilage (à des fins de crédit, de fraude et de sécurité)

435 https://www.vodacom.co.tz/mpawa

	Données partagées avec des tiers	Le cas échéant, Vodacom partage des informations avec : Entreprises du groupe Vodacom Partenaires ou mandataires intervenant dans la livraison des produits et services commandés ou utilisés ; Les sociétés engagées pour fournir des services pour ou au nom de Vodacom Tanzania Public Limited Company, du groupe Vodacom ou du groupe Vodafone ; Agences de référence de crédit, de prévention de la fraude ou de notation commerciale, ou autres agences de notation de crédit ; Les agences de recouvrement de créances ou autres organismes de recouvrement de créances ; Les organismes chargés de l'application de la loi, les organismes gouvernementaux, les organismes de réglementation, les tribunaux ou d'autres autorités publiques si nous y sommes obligés ou autorisés par la loi ; Un tiers ou un organisme où une telle divulgation est requise pour satisfaire à toute loi applicable ou à d'autres exigences légales ou réglementaires ; Services d'urgence (si vous faites un appel d'urgence), y compris votre emplacement approximatif ; Des tiers pour des promotions conjointes avec ce tiers ;
	Technologies de suivi/Cookies de site internet	GPS/ Cookies du site internet
	Stockage des données utilisateur par l'application	Les données personnelles sont stockées en Tanzanie

TigoPesa Nivushe[436]	Données collectées et traitées par l'application	
	Autorisations demandées par l'application	Cette application a accès à : Coordonnées téléphoniques Localisation (GPS et réseau) SMS de l'utilisateur Statut et identité du téléphone Contenu du stockage de l'appareil Appareil photo ID de l'appareil et informations sur les appels Connexions internet (réseau)
	Données Utilisateur collectées	Informations d'enregistrement/inscription: nom complet, âge, numéro de téléphone, adresse e-mail, adresse postale, informations de paiement, adresse de facturation ou nom d'utilisateur et mot de passe de l'utilisateur.

436 https://www.tigo.co.tz/tigo-pesa-nivushe

	Informations collectées sur l'appareil de l'utilisateur	Informations sur l'emplacement de l'utilisateur Les informations sur les applications mobiles sont basées sur les sites internet visités et les applications téléchargées à partir du réseau Tigo. Informations sur l'utilisation du portail : l'adresse réseau et le système d'exploitation d'un ordinateur, le type de navigateur utilisé, le site Web à partir duquel l'utilisateur s'est connecté au site, l'activité de l'utilisateur sur le portail, ainsi que l'historique de visualisation de l'utilisateur, l'heure et la date auxquelles ils ont effectué la visite et acheté les produits et services via le Portail.
	Informations reçues des tiers	Référence de Crédit
	Utilisation des informations Utilisateur par l'application	Détermination des consommations, maintenance et amélioration des services, Service client, personnalisation des contenus, services et offres, business plans, satisfaction client, création de bases de données, analyse des informations et des données, conception d'indicateurs clés de performance (KPI) d'applications, facturation, sécurité , le contrôle qualité et, en général, toutes les informations nécessaires pour se conformer aux contrats de produits ou de services de Tigo, ainsi qu'aux lois et réglementations applicables Pour étendre les offres, promotions, produits, publicités, opportunités, tirages au sort, campagnes, programmes de fidélité, fidélisation de la clientèle
	Partage de données avec des tiers	Tigo partage des données personnelles avec : Les tiers qui fournissent des services à Tigo tels que des services de stockage, l'exécution des commandes, la collecte et l'expédition, les enquêtes, le service client ou la publicité Application de la loi Les autres entités de Tigo, ou en cas de fusion, acquisition, vente d'actifs de l'entreprise ou transfert de service à un autre fournisseur Les autres juridictions qui ont des lois sur la protection des données autres que celles établies en Tanzanie, par ordre écrit d'une autorité judiciaire compétente ou lorsque cela est autorisé conformément à la loi
	Technologies de suivi/Cookies de site internet	GPS / Cookies de site internet
	Stockage des informations de l'utilisateur par l'application	Les données personnelles sont principalement stockées en Tanzanie mais peuvent être transférées vers d'autres juridictions avec des lois sur la protection des données autres que celles établies en Tanzanie par ordre écrit d'une autorité judiciaire compétente ou lorsque cela est autorisé conformément à la loi.

Branch Tanzania[437]	Données collectées et traitées par l'application	
	Autorisations demandées par l'application	Cette application a accès à : Coordonnées téléphoniques Localisation (GPS et réseau) SMS de l'utilisateur Statut et identité du téléphone Contenu du stockage de l'appareil Appareil photo ID de l'appareil et informations sur les appels Les connexions internet (réseau)
	Données Utilisateur Collectées	Nom, adresse, adresse e-mail et numéro de téléphone, numéro de téléphone de l'appareil, détails de la carte SIM, âge, nom d'utilisateur, mot de passe et autres informations d'enregistrement/inscription, informations financières et de crédit (y compris les détails du compte mobile money, les détails du compte bancaire et le numéro de vérification bancaire, le cas échéant), description personnelle et photographie.
	Informations collectées sur l'appareil de l'utilisateur	Les informations techniques, y compris le type d'appareil mobile, les identifiants uniques de l'appareil (par exemple, l'IMEI ou le numéro de série de l'appareil de l'utilisateur), des informations sur la carte SIM utilisée par l'appareil, des informations sur le réseau mobile, le système d'exploitation de votre appareil, le type de navigateur ou l'emplacement de l'appareil et le réglage du fuseau horaire (informations sur l'appareil) ; Les informations stockées sur l'appareil de l'utilisateur, y compris les listes de contacts, les journaux d'appels, les journaux de SMS, les amis Facebook, les listes de contacts d'autres comptes de réseaux sociaux, les photos, les vidéos ou tout autre contenu numérique (Informations sur le contenu) ; Données provenant de l'utilisation de toute autre application tierce sur l'appareil ou les sites de service
	Informations reçues des tiers	Agences d'évaluation du crédit et fournisseurs de réseaux mobiles
	Utilisation des informations Utilisateur par l'application	Les informations recueillies sont utilisées pour déterminer l'éligibilité du client, le montant d'un tel prêt et les termes et conditions applicables à un tel prêt. Le cas échéant : Conformément à une ordonnance de la Cour, d'un comité arbitral, d'un tribunal, d'une directive ou d'une ordonnance réglementaire ou de toute autre obligation légale ou réglementaire
	Données partagées avec des tiers	Branch partage des données personnelles avec : Bureaux de référence de crédit Tout membre du groupe de succursales, c'est-à-dire les filiales, les sociétés affiliées, la société holding et ses filiales Toute autorité légale ou réglementaire à la demande

437 https://branch.co.tz

	Technologies de suivi/Cookies de site internet	GPS / Cookies de site internet
	Stockage de données Utilisateur par l'application	Les données peuvent être transférées et stockées dans une destination en dehors de la Tanzanie (le cas échéant). Elles peuvent également être traitées par du personnel opérant en dehors de la Tanzanie (le cas échéant)

Halotel Haloyako[438]	Données collectées et traitées par l'application	
	Autorisations demandées par l'application	Cette application a accès à : Coordonnées téléphoniques Localisation (GPS et réseau) SMS de l'utilisateur Statut et identité du téléphone Contenu du stockage de l'appareil Appareil photo ID de l'appareil et informations sur les appels Les connexions internet (réseau)
	Données Utilisateur collectées	Nom, date de naissance, adresse, type et numéro de pièce d'identité, lieu de naissance et nationalité, état civil, informations de compte, e-mail, etc.
	Informations collectées sur l'appareil de l'utilisateur	Informations sur l'emplacement de l'utilisateur
	Informations reçues des tiers	Référence du crédit
	Utilisation des données Utilisateur par l'application	Traiter les biens et services achetés auprès d'Halotel Fournir le service ou le produit pertinent à un utilisateur Facturer l'utilisateur pour l'utilisation de nos produits ou services. Faire connaître à l'utilisateur les produits et services d'autres entreprises susceptibles de l'intéresser Effectuer des recherches et des analyses statistiques, notamment en surveillant la manière dont les clients utilisent les produits et services de manière anonyme ou personnelle. Prévenir et détecter les fraudes ou autres délits, recouvrir des dettes ou retrouver ceux qui doivent de l'argent à Halotel. Fournir des rapports agrégés à des tiers

438 https://finca.co.tz/haloyako/

	Données partagées avec des tiers	Partenaires ou agents impliqués dans la livraison des produits et services que vous avez commandés ou utilisés Partenaires ou agents qui mènent des enquêtes de satisfaction client et toute autre enquête liée aux produits ou services fournis à un utilisateur Les entreprises qui sont engagées pour fournir des services pour, au nom de HaloPesa ou Halotel Tanzania. Le cas échéant, référence de crédit, prévention de la fraude, agences d'évaluation des entreprises ou autres agences d'évaluation du crédit. Agences de recouvrement de créances ou autres organismes de recouvrement de créances. Les organismes chargés de l'application de la loi, les organismes de réglementation, les tribunaux ou d'autres autorités publiques si nous y sommes obligés ou autorisés par la loi. Services d'urgence (en cas d'appel d'urgence)
	Technologies de suivi/Cookies de site internet	GPS / cookies de site internet
	Stockage des information Utilisateur par l'application	Les données personnelles des utilisateurs sont prises en main par Halotel en Tanzanie mais peuvent être traitées par d'autres organisations ayant des obligations contractuelles avec HaloPesa ou Halotel Tanzanie conformément à la loi.

Analyse des applications des paiements quotidiens en ce qui concerne l'écosystème réglementaire

Bien que la Tanzanie n'ait pas mis en place de législation sur la protection des données, la Constitution de la République-Unie de Tanzanie de 1977 ("la Constitution") garantit le droit à la vie privée et à la sécurité personnelle[439]. Les articles 98 et 99 de la loi de 2010 sur les communications électroniques et postales ("l'EPOCA") imposent respectivement la responsabilité de la confidentialité des informations aux titulaires de licence de services réseaux et interdisent la divulgation de ces informations sans autorisation[440]. Le Règlement de 2018 sur les communications électroniques et postales (protection des consommateurs), quant à lui, exige qu'un titulaire de licence protège les informations des consommateurs contre toute divulgation inappropriée ou accidentelle[441].

La loi de 2015 sur les systèmes de paiement nationaux (NPS) et la loi de 2006 sur la Banque de Tanzanie habilitent la Banque de Tanzanie (BoT) à réglementer et à superviser les services et produits des systèmes de paiement proposés par les institutions bancaires et non bancaires en Tanzanie[442].

Droit à la vie privée

Chaque application de prêt en ligne évaluée demande l'autorisation d'accéder aux contacts téléphoniques, à l'emplacement, aux SMS de l'utilisateur et à d'autres autorisations. Cette autorisation expose les utilisateurs de ces applications au risque de voir leur vie privée

439 Article 16, Constitution de la République Unie de Tanzanie (1977) https://rsf.org/sites/default/files/constitution.pdf
440 La loi de 2010 sur les communications électroniques et postales (« EPOCA ») https://www.tcra.go.tz/uploads/documents/sw-1619082940-The%20Electronic%20and%20Postal%20Communications%20Act,%202010%20(Act%20No.%203%20out%20of%2010).pdf
441 Règlement 6 (1) & (2) https://www.tanzania.go.tz/egov_uploads/documents/EPC%20consumer%20Protection%20Regulations%202011.pdf
442 https://www.bot.go.tz/PaymentSystem

compromise si elles atterrissent entre les mains de contrôleurs de données malhonnêtes.

Transparence

Il est évident que les politiques de confidentialité des applications sont transparentes, car elles indiquent toutes deux le type d'informations qu'elles collectent auprès des utilisateurs, la raison de la collecte, avec qui elles partagent les données collectées et pourquoi, et si le partage de données est dans et ou hors du pays de domicile.

Droit d'accès et de suppression des données personnelles

Alors que les utilisateurs de ces applications peuvent faire modifier leurs données par les opérateurs de données, la question du droit à la suppression de leurs données est vague dans certaines des applications. [443] Vodacom reste la seule entreprise qui tente d'aborder la question du droit d'accès dans son programme de stockage/conservation. Selon Vodacom, les informations des utilisateurs sont conservées pendant la durée du contrat d'un utilisateur ou tel que requis par la loi. Vodacom supprimera ensuite les informations de l'utilisateur. [444]

443 Article 93(4) de la loi sur les communications électroniques et postales https://www.tcra.go.tz/uploads/documents/sw-1619082940 The%20Electronic%20and%20Postal%20Communications%20Act,%202010%20(Act%20No.%203%20out%20of%2010).pdf

444 https://www.vodacom.co.tz/public/assets/files/Vodacom%20Tz-%20%20Customer%20Privacy%20Statement-retention-schedule.pdf

Ouganda

Profile du Pays

Situé en Afrique de l'Est, l'Ouganda est un pays enclavé à cheval sur l'équateur. Ses pays limitrophes (dans le sens des aiguilles d'une montre à partir du nord) sont le Soudan, le Kenya, la République-Unie de Tanzanie, le Rwanda et la République démocratique du Congo. [445] Le pays a une population estimée à 39,0 millions[446]

445 EAC https://www.eac.int/eac-partner-states/uganda
446 https://www.eac.int/component/documentmananger/?task=download.document&file=bWFpbl9kb2N1bWVudHNfcGRmX0V2cFVzSHl3RUF6dUhnS2hXc3RkVkRNRUFDIEZhY3RzIEZpZ3VyZXMgMjAxOQ==&counter=575

Protection de Données en Ouganda

L'Ouganda se vante d'avoir un secteur des TIC dynamique et à croissance rapide, avec plus de la moitié de sa population ayant accès aux téléphones mobiles. L'Ouganda dispose d'un organisme statutaire autonome connu sous le nom de National Information Technology Authority-Uganda (NITA-U), créé en vertu de la loi NITA-U de 2009. Son rôle est de coordonner et de réglementer les services de technologies de l'information en Ouganda. Les données du NITA-U montrent que les smartphones et les téléphones multifonctions avec accès direct à Internet restent le moteur des nouveaux abonnements à Internet mobile. Les abonnements sont passés de 21,5 millions de smartphones et de téléphones polyvalents au cours de l'exercice 2018/19 à environ 24,1 millions au cours de l'exercice 2019/20[447].
Le prêt numérique, un concept qui prend rapidement racine en Afrique de l'Est, a permis aux abonnés mobiles d'accéder rapidement et facilement aux facilités de prêt. MTN, la plus grande société de téléphonie mobile du pays, en partenariat avec la Commercial Bank of Africa (CBA) - désormais NCBA - a lancé MoKash, un service de prêt numérique mobile, en 2016[448].

Basé sur le besoin des clients pour plus d'options d'épargne et de crédit, MoKash a tiré les leçons des lancements et des succès similaires de M-shwari au Kenya en 2012 et de M-Pawa en République-Unie de Tanzanie en 2014[449].

Suite au lancement de MoKash, 83 000 clients se sont inscrits dans les 48 premières

447 NITA https://www.nita.go.ug/publication/nita-u-statistical-abstract-2020
448 https://techweez.com/2016/08/10/cba-partners-mtn-launching-mokash-m-shwari-equivalent-uganda/ accessed 18 July 2021
449 https://www.uncdf.org/article/2844/disrupting-savings-lending-market-uganda-mokash consulté le 20 juillet 2021

heures, 650 000 après un mois et plus de 1 000 000 en trois mois[450], battant les précédents records établis par ses homologues M-Shwari au Kenya (645 000 clients dans les 21 jours après le lancement) et M- Pawa en République Unie de Tanzanie (250 000 clients le premier mois) [451].

L'écosystème dynamique de la technologie pour la finance (Fintech) en Ouganda a stimulé la prolifération des applications de paie. Outre MoKash de MTN, d'autres applications familières incluent Wewole d'Airtel, Money Mate Uganda et, enfin et surtout, Numida Business Loans.

Aperçu des Données collectées par les Applications de prêt numérique

MTN MoKash[452]	Données collectées et traitées par l'application	
	Autorisations demandées par l'application	Cette application a accès à : Coordonnées téléphoniques Localisation (GPS et réseau) SMS de l'utilisateur Statut et identité du téléphone Contenu du stockage de l'appareil Appareil photo ID de l'appareil et informations sur les appels Les connexions internet (réseau)
	Données Utilisateur collectées	Nom, numéro d'identification, adresse physique, date de naissance, nationalité, adresse e-mail, numéros de téléphone
	Informations collectées sur l'appareil de l'utilisateur	Numéro d'identification de la station mobile Système mondial de télécommunications mobiles ("GSM")
	Informations reçues des tiers	Référence du Crédit
	Utilisation des informations de l'utilisateur par l'application	Traiter les commandes et fournir à un utilisateur des produits et services Service de marketing et de personnalisation à un utilisateur
	Données partagées avec des tiers	Partenaires ou agents impliqués dans la livraison de produits et services ; Agences de référence de crédit, de prévention de la fraude ou de notation des entreprises ; Les organismes chargés de l'application de la loi, les organismes gouvernementaux, les organismes de réglementation, les tribunaux ou d'autres autorités publiques si nécessaire ou si la loi l'autorise ;
	Technologies de suivi/ Cookies de site internet	GPS / Cookies de sites internet

450 https://www.uncdf.org/article/1675/three-months-down-the-road-the-story-of-mokash-in-uganda-migration consulté le 20 juillet 2021
451 Ibid.
452 https://www.mtn.co.ug/mtn-momo/

	Stockage des informations de l'utilisateur par l'application	Les données personnelles sont stockées en Ouganda

AirtelMoney Wewole[453]	Données collectées et traitées par l'application	
	Autorisations demandées par l'application	Cette application a accès à : Coordonnées téléphoniques Localisation (GPS et réseau) SMS de l'utilisateur Statut et identité du téléphone Contenu du stockage de l'appareil Appareil photo ID de l'appareil et informations sur les appels Les connexions internet (réseau)
	Données Utilisateur collectées	Nom, numéro d'identification, adresse physique, date de naissance, nationalité, numéro de téléphone
	Informations collectées sur l'appareil de l'utilisateur	Numéro d'abonnés mobiles aux services d'intégration, et numéro d'identification correspondant et PUK pour accéder au réseau Airtel
	Informations reçues des tiers	Référence de crédit
	Utilisation des informations de l'utilisateur par l'application	Traiter les commandes et fournir à un utilisateur des produits et services
	Données partagées avec des tiers	Partenaires et/ou agents impliqués dans la fourniture de produits et services ; Application de la loi / organismes de réglementation
	Technologies de suivi/Cookies de site internet	GPS / Cookies de site internet
	Stockage des informations de l'utilisateur par l'application	Bien que domicilié en Ouganda, l'endroit où les données sont stockées n'est pas défini

453 https://www.airtel.co.ug/media/press_release/extends_credit_services

MoneyMate Uganda[454]	Données collectées et traitées par l'application	
	Autorisations demandées par l'application	Cette application a accès à : Statut et identité du téléphone Les connexions de réseau
	Données Utilisateur collectées	Nom d'utilisateur, numéro d'utilisateur du téléphone, numéro d'identification, numéro de téléphone mobile, téléphone fixe, adresses de correspondance, société ou société enregistrée (pour les entités commerciales)
	Informations collectées sur l'appareil de l'utilisateur	Identifiant de l'appareil
	Informations reçues des tiers	Fournisseurs de services non définis
	Utilisation des données utilisateurs par l'application	Traitement des demandes / transactions
	Données partagées avec des tiers	Fournisseurs de services non définis
	Technologies de suivi/Cookies de site internet	GPS / Cookies de site internet
	Stockage des informations de l'utilisateurs par l'application	Ouganda

Numida - Business Loans[455]	Données collectées et traitées par l'application	
	Autorisations demandées par l'application	Cette application a accès à : Localisation (GPS et réseau) Contenu du stockage de l'appareil Appareil photo ID de l'appareil et informations sur les appels Les connexions internet (réseau)
	Données Utilisateur collectées	Nom, Identifiant, Numéro de téléphone/Information sur l'entreprise (pour les entreprises)
	Informations collectées sur l'appareil de l'utilisateur	ID de l'appareil / Système d'exploitation (OS)
	Informations reçues des tiers	Bureaux de référence de crédit

454 https://play.google.com/store/apps/details?id=com.moneymateuganda.mmg
455 https://play.google.com/store/apps/details?id=com.numidatech.numida&hl=en_US&gl=US

	Utilisation des informations de l'utilisateur par l'application	Fournir et améliorer nos services. Publicité ciblée Communication avec l'utilisateur
	Données partagées avec des tiers	Agence de référence de crédit Personnel et fournisseurs
	Technologies de suivi/Cookies de site internet	GPS / Cookies de site internet
	Stockage des informations de l'utilisateur par l'application	Les données personnelles sont stockées en Ouganda mais peuvent être partagées et traitées par le personnel opérant à l'intérieur ou à l'extérieur de l'Ouganda

Analyse des Applications de paie au regard de l'écosystème réglementaire

Dans la période précédant l'ère de la croissance rapide de l'écosystème Fintech en Ouganda, les régulateurs ont promulgué de nombreuses législations.

Il s'agit notamment de la loi sur les transactions électroniques (2011) [456], une loi prévoyant l'utilisation, la sécurité, la facilitation et la réglementation des communications et des transactions électroniques, encourageant l'utilisation des services d'administration en ligne et prévoyant les questions connexes ;

Loi sur l'utilisation abusive des ordinateurs (2011) [457], une loi prévoyant la sûreté et la sécurité des transactions électroniques et des systèmes d'information pour empêcher l'accès illégal, l'abus ou l'utilisation abusive ; la loi sur les contrats (2010) [458]; la loi sur les signatures électroniques (2011) [459]; et Directives sur la monnaie électronique de la Banque d'Ouganda (BoU) (2013) [460]

Malgré l'incapacité de ces différentes législations à répondre aux contraintes ou à soutenir le fonctionnement ou le développement futur des systèmes de paiement numériques, en théorie, elles semblaient accorder une certaine « protection » aux parties prenantes. Afin de se tenir au courant des dernières avancées technologiques dans le secteur numérique, une législation supplémentaire visant à réglementer l'écosystème fintech florissant a récemment été adoptée. La loi sur le système national de paiement (2020) [461] vise à assurer la sécurité et l'efficacité des systèmes de paiement, à assurer les fonctions de la Banque centrale concernant les systèmes de paiement. Le Règlement sur les agents des systèmes de paiement nationaux (2021) [462] vise à rationaliser l'octroi de licences aux agents d'argent mobile. Le règlement sur les systèmes de paiement nationaux (bac à sable) (2021) [463], d'autre part, fournit un cadre de bac à sable « sous-réglementaire » pour les produits et services financiers innovants, les modèles commerciaux ou les mécanismes de livraison dans l'écosystème des systèmes de paiement.

456 https://ict.go.ug/2019/12/03/the-electronics-transactions-act-2011/
457 https://ict.go.ug/2019/12/03/the-computer-misuse-act-2011/
458 https://commons.laws.africa/akn/ug/act/2010/7/eng@2010-05-28.pdf
459 https://www.nita.go.ug/publication/electronic-signatures-act-2011-act-no-7-2011
460 https://www.bou.or.ug/bou/bouwebsite/FinancialInclusion/innovations.html
461 https://www.bou.or.ug/bou/bouwebsite/bouwebsitecontent/acts/supervision_acts_regulations/Payment-Systems-Act/The-National-Payments-Systems-Act-2020.pdf
462 https://www.bou.or.ug/bou/bouwebsite/bouwebsitecontent/acts/supervision_acts_regulations/Payment-Systems-Regulations/The-National-Payment-Systems-Agents-Regulations-2021.pdf
463 https://www.bou.or.ug/bou/bouwebsite/bouwebsitecontent/acts/supervision_acts_regulations/Payment-Systems-Regulations/The-National-Payment-Systems-Sandbox-Regulations-2021.pdf

La loi sur la protection des données et la vie privée[464] a été votée le 25 février 2019 mais est entrée en vigueur le 3 mai 2019. La loi réglemente la collecte et le traitement des informations personnelles. Elle s'applique à toute personne, institution ou organisme public qui collecte, traite, stocke ou utilise des données personnelles en Ouganda ou en dehors de l'Ouganda.

Pour les entités domiciliées en dehors de l'Ouganda, la loi est limitée aux données personnelles relatives aux citoyens ougandais.

Droit à la vie privée

Avec les diverses réglementations en place, parmi lesquelles la législation ougandaise sur la protection des données et la confidentialité, les sociétés d'applications de prêt semblent avoir intégrées les considérations relatives aux questions de confidentialité dès le début du développement de leurs produits et services dans le but de maintenir la confidentialité de tous les renseignements personnels recueillis.

Transparence

Les sociétés d'application de prêt sont ouvertes en ce qui concerne les pratiques de collecte de données personnelles ; collecte, stockage, partage avec des tiers et mesures administratives pour garantir la sécurité des données personnelles collectées, une démarche conforme à l'analyse d'impact sur la protection des données.

Droit d'accès et de suppression de données personnelles

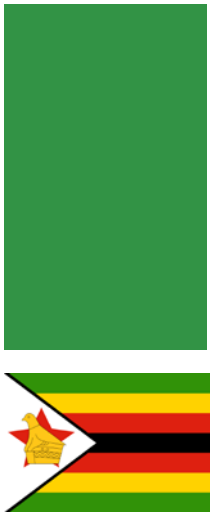
L'article 35 de la loi sur la protection des données et la vie privée énonce le droit d'accéder aux informations personnelles détenues par un responsable du traitement des données. Une personne concernée a le droit de demander que celles-ci soient modifiées en conséquence. Elle (personne concernée) doit cependant satisfaire à l'exigence de preuve d'identité, lorsqu'elle fournit l'un des éléments suivants - (a) une carte d'identité nationale ou une carte d'identité pour les étrangers ; (b) un passeport ou tout document de voyage ; ou (c) un permis de conduire. D'autre part, un responsable du traitement est tenu d'informer la personne concernée de sa décision dans les sept jours suivant la réception de la demande.

Dans ses conditions d'utilisation, MTN déclare que "toute personne soumettant des informations à MTN via le système de monnaie électronique peut se voir accorder des droits d'accès à ces informations". La déclaration ajoute que "MTN a développé des systèmes qui permettent l'accès et la correction des informations qui lui sont soumises"[465]. Les autres, Airtel Money, Money Mate et Numida, ne donnent aucune informations sur les actions concernant cette disposition.

464 Loi ougandaise pour la protection des données et la confidentialité https://ict.go.ug/wp-content/uploads/2019/03/Data-Protection-and-Privacy-Act-2019.pdf <https://www.nita.go.ug/sites/default/files/publications/Data%20Protection%20and%20Privacy%20Act%20No.%209%20of%202019.pdf> consulté le 23 juillet 2021.

465 https://www.mtn.co.ug/wp-content/uploads/2019/10/MTN-MOBILE-MONEY-Consumer-Terms-and-Conditions-0519.pdf

Zimbabwe



Profil du Pays

Le Zimbabwe, également connu sous le nom de République du Zimbabwe, est situé en Afrique australe. Il partage une frontière avec l'Afrique du Sud, le Botswana, la Zambie et le Mozambique. Il couvre une superficie de 390 757 km et compte 15 millions d'habitants[466]. Sa capitale est Harare et l'anglais, le shona et le ndebele sont ses langues les plus parlées. [467]

466 Zimbabwe https://www.nationsonline.org/oneworld/zimbabwe.htm
467 Zimbabwe https://www.nationsonline.org/oneworld/zimbabwe.htm

Protection des données au Zimbabwe

L'émergence de la technologie a entraîné un développement significatif du secteur financier au Zimbabwe. Elle a donné naissance à la fintech, qui a révolutionné l'industrie et provoqué l'inclusion financière où la population non bancarisée peut accéder aux services financiers. Le secteur des prêts numériques est une caractéristique essentielle de l'écosystème fintech, facilitant un accès rapide et facile à l'argent en ligne sans aucune sécurité.

Le prêt numérique au Zimbabwe, cependant, reste non réglementé. Le cadre réglementaire des systèmes financiers ne couvre que les institutions financières telles que les banques, les sociétés de construction et les compagnies d'assurance[468]. La loi bancaire limite les pouvoirs d'octroi de licences, de supervision et de réglementation de la Banque de réserve du Zimbabwe aux institutions de dépôt et d'émission de prêts[469]. Cela laisse un immense gap en matière de régulation des pratiques des plateformes de prêt.

Il n'existe pas non plus de cadre réglementaire couvrant les pratiques de protection des données des plateformes de prêt numériques. Le Zimbabwe a actuellement un projet de loi sur la protection des données qui n'a pas encore été promulgué. Le Sénat a récemment adopté le projet de loi, mais il a ensuite été renvoyé au Parlement pour amendements[470]. Le droit à la vie privée est inscrit dans la constitution et dans certaines lois sectorielles, comme la loi sur la liberté d'information, qui régit la protection des données par les organismes

468 Article 2 (a)(iii), Loi de 2015 portant modification de la loi sur les banques. https://www.rbz.co.zw/documents/acts/Banking%20Amendment%20Act,%202015.pdf
469 Fsd Afrique, Etude de l'écosystème Fintech du Zimbabwe (mars 2020) pg 27 https://www.fsdafrica.org/wp-content/uploads/2020/03/Zim-Fintech-Report-25.03.20_FINAL.pdf
470 Le Zimbabwe sur le point de finaliser sa loi sur la protection des données https://iapp.org/news/a/zimbabwe-on-the-cusp-of-finalizing-data-protection-law/# Renvoi du projet de loi controversé sur la cybersécurité et la protection de la vie privée au Zimbabwe https://www.grcworldforums.com/global/zimbabwes-controversial-cyber-security-and-privacy-bill-sent-back/2325.article

publics[471].

L'absence de loi sur la protection des données au Zimbabwe laisse les pratiques de protection des données des applications de prêt non réglementées et pose un risque important pour les utilisateurs des applications. Cette étude examine les données recueillies par trois applications remarquables au Zimbabwe, à savoir GetBucks, MyBucks et eShagi. Il fournit ensuite des conseils sur les pratiques de protection des données que les applications doivent adopter sur la base des meilleures pratiques internationales.

Aperçu des Données Collectées par les Application de Prêt en ligne

GetBucks[472]	Informations Collectées et traitées par l'Application	
	Autorisations demandées	
	Informations collectées chez l'utilisateur	Numéro d'identification, numéro de contact, numéro de rue, adresse e-mail et adresse IP La plate-forme reçoit et enregistre les informations utilisateur traitées à partir du navigateur d'un utilisateur sur ses serveurs lors de l'utilisation du site Web. Ces informations comprennent : Adresse IP Informations sur les cookies La page demandée par un Utilisateur « GetBucks peut également intercepter, surveiller, bloquer, filtrer, lire, supprimer et divulguer toute communication via son système d'information. Cela inclut, mais sans s'y limiter, le suivi des adresses de protocole Internet (adresses IP) des utilisateurs, et les utilisateurs acceptent que GetBucks puisse demander leurs informations personnelles à leur fournisseur de services Internet pour quelque raison que le site juge appropriée pour assurer une relation sûre et de confiance avec le utilisateur".
	Informations collectées à partir de l'appareil de l'utilisateur/ Utilisation du site internet	La plate-forme reçoit et enregistre les informations utilisateur traitées à partir du navigateur d'un utilisateur sur ses serveurs lors de l'utilisation du site internet. Ces informations comprennent : Adresse IP Informations sur les cookies La page demandée par un utilisateur
	Comment les informations de l'utilisateur sont collectées	Les informations de l'utilisateur sont collectées lors de l'utilisation du site internet
	Informations reçues d'un tiers	

471 Zimbabwe : Aperçu de la protection des données https://www.dataguidance.com/notes/zimbabwe-data-protection-overview
472 Politique de confidentialité de GetBucks https://zw.getbucks.com/site-policy

	Utilisation des informations de l'utilisateur par l'application	
	Informations partagées avec des tiers/ Divulgation d'informations Durée d'accès du tiers	GetBucks partage les informations personnelles des utilisateurs avec les tiers suivants : Marketers - divulguer les informations des utilisateurs à des fins de marketing Fournisseurs ou agents - divulguer des informations sur les utilisateurs aux fournisseurs pour la fourniture de services Organismes chargés de l'application de la loi - divulguer les informations de l'utilisateur lorsque cela est requis par une ordonnance du tribunal ou la loi Peut divulguer l'adresse IP d'un utilisateur lorsque la loi l'exige Affiliés Partenaires commerciaux en cas de ; changement de propriétaire, fusion, acquisition ou vente d'actifs Employés - dans l'exercice de leurs fonctions Tiers lors de la résolution ou de l'examen des plaintes[473]
	Technologies de suivi/Cookies de site internet	
	Transfert international de données	Cette plate-forme peut transmettre ou transférer des données personnelles des utilisateurs vers des pays en dehors du Zimbabwe. Les pays peuvent avoir des lois sur la protection des données moins strictes.
	Stockage des informations/ Sécurité des données	"Utilise des mesures de sécurité avancées pour protéger les données personnelles en sa possession."

MyBucks[474]	Informations Collectées et traitées par l'Application	
	Autorisations demandées par l'application	

473 Politique de confidentialité de GetBucks : Clause de divulgation https://zw.getbucks.com/site-policy
474 Politique de confidentialité de MyBucks https://corporate.mybucks.com/privacy

	Informations collectées chez l'utilisateur	Traiter les informations/données utilisateur suivantes : Données d'utilisation : adresse IP, emplacement géographique, type de navigateur et version, système d'exploitation, source de référence, durée de la visite, pages consultées et chemins de navigation du site Web, moment de l'utilisation, fréquence des utilisateurs et mode d'utilisation du service. [475] Données du compte utilisateur : nom et adresse e-mail de l'utilisateur Données de profil de l'utilisateur : nom, adresse, numéro de téléphone, adresse e-mail, photo de profil, sexe, date de naissance, statut relationnel, intérêts et passe-temps, détails sur l'éducation et les détails de l'emploi Données sur l'emploi de l'utilisateur : nom, adresse, numéro de téléphone, adresse e-mail, photo de profil, sexe, date de naissance, statut relationnel, intérêts et passe-temps, historique de l'emploi, éducation, qualifications, expérience, informations démographiques, emplacement géographique et informations sur le salaire Données de service de l'utilisateur : données relatives à l'utilisation par l'utilisateur des services de MyBuck Données de publication : données basées sur les informations publiées par l'utilisateur sur le site MyBucks. Données de demande : données basées sur la demande d'un utilisateur concernant les produits, services ou emplois MyBucks Données sur la relation client : Inclut celles d'un utilisateur ; le nom, l'employeur, la fonction, les coordonnées, les informations contenues dans la correspondance entre MyBucks et l'utilisateur ou l'employeur de l'utilisateur. Données de transaction : informations relatives aux transactions de l'utilisateur avec MyBucks via le site Web Données de notification : comprend des informations relatives à l'abonnement d'un utilisateur aux notifications par e-mail MyBucks. Données de correspondance : informations relatives à la communication d'un utilisateur avec MyBucks Informations traitées via les cookies
	Informations collectées de l'appareil de l'utilisateur	
	Comment les informations de l'utilisateur sont collectées	
	Informations reçues d'un tiers	

475 Politique de confidentialité de MyBucks : Article 3.2

	Utilisation des informations de l'utilisateur par l'application	MyBucks utilise les informations utilisateur aux fins suivantes : Exécution de MyBucks et de ses opérations internes Respect des obligations légales et réglementaires Évaluer la capacité de l'utilisateur à rembourser le prêt Fournir aux utilisateurs des services durables Offrir aux utilisateurs des services appropriés de qualité Fournir à MyBucks une compréhension de son activité et améliorer ses services S'assurer que les systèmes MyBucks fonctionnent efficacement S'assurer que les informations traitées sur les utilisateurs sont correctes Prévention des crimes tels que la fraude Administrer les remboursements Recouvrement de dettes Tenue des dossiers commerciaux Commercialisation des produits et services MyBucks Améliorer la qualité des services offerts par MyBucks S'assurer que les systèmes MyBucks fonctionnent efficacement Protéger la sécurité des systèmes MyBucks Résoudre les plaintes Défense des réclamations légales Respect d'une obligation légale
	Informations partagées avec un tiers Durée d'accès des informations aux tiers	Divulgue les informations de l'utilisateur aux parties suivantes : Membres du groupe MyBucks Assureurs et conseillers professionnels Les prestataires de services, c'est-à-dire les fournisseurs de systèmes de paiement, les agences de recouvrement de créances, etc., Fournisseurs informatiques, auditeurs, agences de marketing, conseillers fiscaux, fournisseurs surveillant l'utilisation du site MyBucks L'agent d'un utilisateur Banques ou institutions financières Organismes chargés de l'application de la loi dans le cadre d'une enquête et de la prévention de la criminalité Cabinets d'avocats/organisations fournissant des conseils juridiques à MyBucks ou les représentants dans des procédures judiciaires Experts désignés pour réaliser des études de marché Partenaires commerciaux lors de la vente, du transfert ou de la cession de l'entreprise de MyBuck Régulateurs et autorités gouvernementales
	Technologies de suivi/Cookies de site internet	

	Transfert international de données/Transfert de données transfrontalier	MyBucks transfère les données de l'utilisateur vers des pays en dehors de la juridiction de l'utilisateur.
	Stockage des informations de l'utilisateur par l'application	

eShagi[476] -eShagi n'a aucune politique de confidentialité -Il ne dispose pas non plus de Termes & Conditions	Informations Collectées et traitées par l'Application	
	Autorisations demandées par l'application	
	Informations collectées chez l'utilisateur	
	Informations collectées de l'appareil de l'utilisateur	
	Comment l'agence collecte les informations	
	Informations reçues d'un tiers	
	Utilisation des informations de l'utilisateur	
	Informations partagées avec des tiers Durée d'accès des informations aux tiers	
	Technologies de suivi/ Cookies de site internet	
	Transferts internationaux de données	
	Stockage des données de l'utilisateur par l'application	

Analyses des pratiques de Protection de données des applications
Contrôle de l'utilisateur

Les plateformes de prêt numériques doivent permettre aux utilisateurs d'exercer une autonomie sur leurs données. Elles doivent leur permettre de connaître la nature des données personnelles traitées, la manière dont les informations sont utilisées, les parties avec lesquelles les données seront partagées et la manière dont elles seront traitées. Elles devraient également créer des moyens permettant aux utilisateurs d'accéder à leurs données, de les corriger ou de les mettre à jour, voire de les supprimer. Ceci est important car les utilisateurs ont des droits sur leurs données et toute action entreprise

476 eShagi website https://www.eshagi.com/

sur les données doit être soumise à leur consentement. L'application de prêt GetBucks ne semble pas garantir la pleine jouissance de ce droit. La politique de cette entreprise permet uniquement aux utilisateurs de corriger ou de mettre à jour leurs données[477]. Les utilisateurs n'ont aucun moyen d'accéder à leurs données ou même de les supprimer lorsqu'ils n'ont plus besoin des services. Les utilisateurs ne peuvent pas non plus chercher à transférer leurs données. D'autre part, MyBucks garantit aux utilisateurs ces droits. Dans le cadre de leur politique, les utilisateurs disposent d'un droit d'accès, de rectification, de suppression et de portabilité de leurs données[478].

Le Consentement

Le consentement des utilisateurs aux politiques de confidentialité est sur une base "à prendre ou à laisser". Ces applications collectent des données excessives et ne laissent aux utilisateurs d'autre choix que d'accepter les conditions en raison de leur « besoin » pour les services. Prenons, par exemple, la politique de confidentialité de GetBucks « Clause d'interception et de surveillance ». Cette clause stipule que la plate-forme « peut intercepter, surveiller, bloquer, filtrer, lire, supprimer et divulguer toute communication sur son système. Cela inclut, mais sans s'y limiter, le suivi des adresses de protocole Internet (adresses IP) des utilisateurs et la demande d'informations personnelles de l'utilisateur auprès de son fournisseur d'accès Internet pour les raisons que le site juge appropriées....

Limites de l'objectif

Les applications de prêt en ligne doivent indiquer aux utilisateurs l'objectif de la collecte de données et l'utilisation proposée[479]. Elles devraient également veiller à se limiter au traitement des données nécessaires à la fourniture de leurs services[480]. Ce faisant, elles doivent s'assurer qu'ils traitent des données personnelles adéquates, pertinentes et non excessives.

Les applications étudiées semblent collecter plus de données que nécessaire pour le prêt numérique. MyBucks traite les informations des utilisateurs telles que les centre d'intérêts et les passe-temps des utilisateurs, le statut amoureux, l'historique des emplois, l'expérience professionnelle, entre autres, qui ne sont pas pertinentes aux fins du prêt numérique[481].

Transfert international de données

Les applications de prêt étudiées transfèrent les données des utilisateurs vers des juridictions en dehors du Zimbabwe. Des applications telles que GetBucks, par exemple, transfèrent les données personnelles des utilisateurs vers des juridictions dont les lois sur la protection des données sont moins strictes[482]. Ce transfert présente un risque important pour la sécurité des données des utilisateurs.

Les applications devraient garantir la protection des données personnelles transférées à l'extérieur du pays. Ce faisant, ells devraient mettre en place des garanties appropriées pour protéger les données et veiller à ce que les données soient transférées vers des juridictions dotées de lois adéquates sur la protection des données.

Partage des données des utilisateurs avec des tiers

Les applications de prêt numérique doivent indiquer aux utilisateurs les tiers avec lesquels elles ont l'intention de partager leurs données. Elles devraient préciser dans leurs politiques les données qu'ils entendent partager avec les tiers, la durée d'accès aux données par les

477 Politique de confidentialité de GetBucks https://zw.getbucks.com/site-policy
478 Politique de confidentialité de MyBucks : Clause 10 https://corporate.mybucks.com/privacy
479 Privacy International - pg 39
480 Rapport de minimisation des données - pg.4
481 Politique de confidentialité de MyBucks : Clause 3 'Utilisation des données personnelles' https://corporate.mybucks.com/privacy
482 Politique de confidentialité GetBucks: Transfert transfrontalier https://zw.getbucks.com/site-policy

tiers et les mesures de sécurité mises en place pour protéger les données partagées avec les tiers.

Les applications étudiées ne les indiquent pas dans leurs politiques de confidentialité. Getbucks n'affiche que les tiers avec lesquels elle partage des informations et aucune information sur les données partagées avec les tiers, la durée d'accès ou les mesures de sécurité[483]. MyBucks, en revanche, n'indique pas clairement les tiers avec lesquels ils partagent des informations[484]. eShagi n'a pas de politique de confidentialité, laissant les utilisateurs sans aucune information sur les tiers qui accèdent à leurs données.

Conservation des données des utilisateurs

Les applications de cette étude n'indiquent pas les paramètres qu'elles utilisent pour déterminer la durée de stockage des données d'un utilisateur. Elles n'indiquent pas non plus aux utilisateurs la période précise pendant laquelle ils conserveront leurs données. Ces informations sont essentielles pour les utilisateurs des applications pour les aider à savoir combien de temps les applications auront accès à leurs données et quels moyens ils peuvent utiliser pour supprimer leurs données des applications.

483 Politique de confidentialité GetBucks: Clause de divulgation https://zw.getbucks.com/site-policy
484 Politique de confidentialité MyBucks https://corporate.mybucks.com/privacy

Conclusion

Ce n'est un secret pour personne que les applications financières numériques se sont améliorées et ont accru la pénétration des services bancaires, en particulier dans les régions rurales des pays africains. Cependant, dans le cas des applications de prêt en ligne, ce support semble être un cadeau grec car les applications collectent de grandes quantités de données personnelles sans réelle précision ni clarté sur leur traitement, et les régulateurs semblent être dépassés ou désemparés sur la façon de normaliser la collecte et l'utilisation.

Dans les pays pionniers en matière de réglementation comme le Cap-Vert, le secteur financier est contrôlé sur le traitement réserve aux données des consommateurs. Cependant, cela n'a pas empêché l'utilisation abusive de ces données car il y a un flou sur le degré de surveillance réglementaire de l'Agence de protection des données sur les applications numériques. Il est maintenant devenu essentiel que les lois des pays africains expriment de la clarté et des détails à propos de :

Si les applications financières numériques sont soumises aux mêmes normes de traitement des données que les banques traditionnelles ;

Le cadre réglementaire nécessaire pour soutenir et sécuriser les données des utilisateurs du secteur des technologies financières en constante croissance et innovant.

Paradigm Initiative continue de travailler avec diverses parties prenantes pour promouvoir la confidentialité et la protection des données, et pour contribuer aux mesures de comblement des lacunes dans les pays mis en évidence, des copies de ce rapport seront mises à la disposition des agences de protection des données concernées pour action, et à d'autres partenaires pour le travail requis sur la sensibilisation.