Grands facturiers, données personnelles, bureau d'information sur le crédit et partage d'informations sur le crédit au Togo : attention aux risques !

Dessa-Nin Ewèdew Awesso

GRANDS FACTURIERS, DONNÉES PERSONNELLES, BUREAU D'INFORMATION SUR LE CRÉDIT ET PARTAGE D'INFORMATIONS SUR LE CRÉDIT AU TOGO : ATTENTION AUX RISQUES !

Dessa-nin Ewèdew Awesso
Doctorant en Cotutelle
Université Côte d'Azur/Université de Lomé

Introduction

Le 25 mai 2018 alors qu'entrait en vigueur le règlement relatif à la protection des données à caractère personnel en Europe[1], le Togo adoptait un décret autorisant le traitement automatisé des données à caractère personnel pour l'intégration des grands facturiers à la plateforme électronique de partage des informations sur le crédit[2].

Ledit décret entre dans la mise en application au Togo de la loi uniforme portant règlementation des Bureaux d'Information sur le Crédit (BIC)[3] dans les États membres de l'Union Monétaire Ouest-Africaine (UMOA). Cette loi fixe le cadre juridique de la création, de l'agrément, de l'organisation de l'activité et de supervision des BIC.

Le BIC est une personne morale agréée qui effectue à titre de profession habituelle, la collecte, la compilation, le stockage, le traitement et la diffusion d'informations sur le crédit et autres données connexes qui sont reçues à .partir de sources ou de fournisseurs de données, conformément à un accord spécifique signé par les parties, aux fins de compilation et de mise à disposition de rapports de crédit et offrant des services à valeur ajoutée aux utilisateurs[4].

Il est ici utile de rappeler que constitue notamment une opération de crédit tout acte par lequel une personne met ou promet de mettre des fonds à la disposition d'une autre personne[5]. La création des bureaux d'informations participe à l'amélioration du climat des affaires. Leur mise en place vise, entre autres, à réduire l'asymétrie d'informations[6] entre les prêteurs et les emprunteurs afin d'améliorer l'accès des populations aux services financiers à des coûts réduits, d'assainir la qualité du portefeuille des établissements assujettis via une meilleure gestion des

---

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *JO*, n° L119, 4 mai 2016, pp. 1-88.

[2] Décret n° 2018-109/PR du 25 mai 2018 portant autorisation de la mise en œuvre d'un traitement autorisé de données à caractère personnel pour l'intégration des grands facturiers à la plateforme électronique de partage des informations sur le crédit. Cependant, la loi relative à la protection des données personnelles ne sera adoptée qu'en octobre 2019 : V. en ce sens D.E. AWESSO, *Brève analyse de la loi togolaise relative à la protection des données à caractère personnel*, janvier 2020, disponible sur https://halshs.archives-ouvertes.fr/halshs-02466051.

[3] Loi uniforme n° 2016-005 du 14 mars 2016 portant règlementation des Bureaux d'Information sur le Crédit (BIC).

[4] Article 1er, alinéa 3, de la Loi uniforme n° 2016-005 portant règlementation des Bureaux d'Information sur le Crédit (BIC) dans les États membres de l'Union Monétaire Ouest-Africaine (UMOA).

[5] S. GUINCHARD et T. DEBARD, *Lexique des termes juridiques*, 28e éd., Lexiques, Paris, Dalloz, 2020, p. 313.

[6] V. en ce sens G.A. AKERLOF, « The Market for "Lemons": Quality Uncertainty and the Market Mechanism », *The Quarterly Journal of Economics*, 1970, vol. 84, n° 3, pp. 488-500.

risques et d'accroître l'efficacité de la supervision de l'activité de crédit à travers l'anticipation du surendettement des emprunteurs et la maîtrise du risque systémique[7].

Pour ce faire, le BIC exploite un ensemble de données sur les antécédents de crédit ou de paiement d'un (futur) emprunteur pour fournir des rapports de solvabilité notamment aux établissements de crédits et aux systèmes financiers décentralisés (SFD). Les données utilisées sont fournies, entre autres, par les organismes financiers, les sources publiques et ceux qu'on désigne comme étant les « grands facturiers ». Cette notion désigne, selon les dispositions du décret togolais de 2018, les opérateurs de communications électroniques, les sociétés de fourniture d'eau et d'électricité ainsi que les professionnels de la grande distribution[8]. Aux termes de l'article 2 dudit décret, les grands facturiers communiquent les données personnelles de leurs clients par le biais d'une plateforme électronique de partage d'informations en vue de leur traitement.

Il convient de rappeler que, selon de la loi n° 2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel (LPDCP) au Togo, sont considérées comme étant des données à caractère personnel *« toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique »*[9]. Par ailleurs, on qualifie de « traitement » toute opération ou ensemble d'opérations[10] effectuées ou non à l'aide de procédés automatisés telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, le cryptage, l'effacement ou la destruction des données personnelles[11].

Dans le cadre de cette analyse nous nous intéressons particulièrement aux risques de violation des droits des personnes concernées par le traitement leurs données à caractère personnel dans le cadre du système de partage d'informations. Au vu des possibilités offertes par le décret de

---

[7] BCEAO, « Promotion des Bureaux d'Information sur le Crédit dans l'UMOA », disponible en ligne sur : https://www.bceao.int/fr/content/promotion-des-bureaux-dinformation-sur-le-credit-dans-lumoa.
[8] Article 1er, alinéa 2, du décret.
[9] Article 4, alinéa 6, de la LPDCP.
[10] Prévues à l'article 2 de ladite loi.
[11] Article 4, alinéa 20, de la LPDCP.

2018, et des « tentations » qu'il peut susciter – eu égard à la disponibilité et l'accessibilité des données personnelles – peut-on affirmer que le cadre juridique existant est suffisant pour minimiser, voire éliminer, les risques liés au traitement des données à caractère personnel dans le cadre du partage d'informations sur le crédit ?

Sur le plan théorique cette analyse conduit principalement à s'intéresser à l'application des principes fondamentaux gouvernant le traitement des données à caractère personnel – notamment le respect des droits et libertés fondamentaux des personnes physiques – dans le cadre du partage d'informations sur le crédit. En pratique, cette étude permet, entre autres, de s'interroger sur le rôle des différents acteurs impliqués dans le partage d'informations et leur capacité à garantir, et/ou faire respecter, les droits des personnes concernées.

En effet, le décret de 2018 fixe les modalités de collecte, d'accès et de communication des données à caractère personnel transmises au BIC[12]. Toutefois, si le cadre juridique tel qu'il a été défini minimise, en principe, les risques d'atteinte aux droits et libertés fondamentaux en protégeant les données personnelles **(I)**, il n'en demeure pas moins que ces risques peuvent subsister dans certaines situations **(II)**.

I. Un cadre de partage des données personnelles en principe sans risques

La minimisation des risques d'atteintes aux libertés et droits fondamentaux des personnes physiques lors du traitement de leurs données personnelles repose sur l'encadrement de la fourniture des données aux BIC **(A)** et de l'exploitation qui en sera faite **(B)**.

A. L'encadrement stricte de la « fourniture » des données personnelles

Le cadre légal mis en place vise une protection efficiente des clients **(2)** dont les données personnelles sont communiquées au BIC. Par ailleurs, les grands facturiers qui sont sollicités pour alimenter la plateforme de partage d'informations sur le crédit sont aussi soumis à certaines obligations **(1)**.

[12] Article 1er, alinéa 1er, du décret.

1. Les grands facturiers : les pourvoyeurs de données obligés

Les grands facturiers ne peuvent procéder au traitement des données personnelles qu'en respectant certaines prescriptions légales **(a)**. Le législateur impose aussi des obligations envers les clients – les personnes concernées – et les utilisateurs des données **(b)**.

a. La légalité du traitement des données personnelles

Pour rappel, le décret togolais désigne comme grands facturiers les opérateurs de communications électroniques, les sociétés de fourniture d'eau et d'électricité ainsi que les professionnels de grande distribution. Les données transmises au BIC sont notamment collectées lors de la souscription aux services offerts par ces facturiers. Ainsi, les opérateurs de communications électroniques – à l'instar de Moov Togo, Togo Telecom, Togo Cellulaire – transmettent les données personnelles collectées lors de la souscription de leur service.

Il faut noter qu'au Togo, le décret n° 2011-120/PR portant identification systématique et obligatoire des abonnés aux services de télécommunications impose aux opérateurs de téléphonies d'identifier leurs abonnés. L'identification systématique consiste notamment à recueillir au minimum l'état civil et l'adresse complète du souscripteur. Cette obligation légale dispense ainsi les opérateurs de téléphonie fixe et mobile d'obtenir le consentement préalable du souscripteur. Il convient de rappeler que les responsables du traitement peuvent notamment déroger à l'exigence du consentement préalable lorsqu'il s'agit pour eux de se mettre en conformité avec une prescription légale à laquelle ils sont soumis[13]. C'est le cas en espèce pour les opérateurs togolais de téléphonie mobile et fixe soumis par le décret de 2011.

Quant aux sociétés de fourniture d'eau et d'électricité ainsi que les professionnels de grande distribution, la collecte de données personnelles, sans consentement préalable devient licite lorsque le traitement est, entre autres, nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande[14].

Toutefois, il convient de noter que dans les deux cas précités, la finalité de l'opération n'est pas celle de transmettre les données recueillies au BIC. De plus, la loi uniforme de 2016 fait

[13] Article 14, §1, de la LPDCP. Voir également l'article 23, point 2, a) de l'Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace CEDEAO du 16 Février 2010.
[14] Article 14, §3, de la LPDCP. Voir aussi l'article 23, point 2, c) de l'acte additionnel.

obligation aux fournisseurs de données que sont les grands facturiers d'obtenir le consentement préalable du client pour le partage des informations sur le crédit le concernant avec le BIC et la consultation desdites informations par les utilisateurs du BIC[15].

En outre, le décret de 2018 autorise le traitement des données à caractère personnel des clients des grands facturiers pour une finalité précise : la communication de certaines données personnelles au BIC. Les données dont le traitement est autorisé sont : l'état civil ; les antécédents de crédit ; l'historique de paiement, y compris sa capacité d'emprunt ou de remboursement ainsi que son comportement en matière de paiement ; l'ensemble des risques de crédit ; le volume des prêts, la maturité, les modalités et conditions ; les remboursements ; les garanties et tous autres engagements financiers permettant de déterminer la situation financière et l'exposition de la personne concernée[16]. Quelles sont alors les obligations des grands facturiers vis-à-vis de leurs clients et des utilisateurs du BIC ?

b. Les obligations vis-à-vis des « tiers » : des clients aux utilisateurs des données sur le crédit

Même si le décret de 2018[17] ne le mentionne pas expressément, il convient de rappeler et d'insister sur le fait que les grands facturiers ne peuvent fournir les données à caractère personnel de leurs clients au BIC sans consentement préalable de ces derniers. Au minimum, deux fondements justifient une telle obligation. Le premier est lié à la règlementation relative à la protection des données personnelles en vigueur au Togo. Le second est relatif à la relation contractuelle entre les grands facturiers et leurs clients.

S'agissant de la règlementation relative à la protection des données personnelles, qui date de 2019[18], elle prévoit une obligation de consentement préalable[19]. Nous évoquions plus haut, le cas des opérateurs de téléphonie mobile et fixe qui sont contraints, par un décret de 2011, de collecter des données personnelles sur ordre de l'État. Il s'agit là d'une condition dérogatoire à l'obligation d'obtention d'un consentement préalable.

---

[15] Article 42, point 1, de la loi uniforme.
[16] Article 4 du décret de 2018.
[17] Décret portant autorisation de la mise en œuvre d'un traitement automatisé de données à caractère personnel pour l'intégration des grands facturiers à la plateforme électronique de partage des informations sur le crédit
[18] Loi n° 2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel (LPDCP).
[19] Article 14, §1, de la LPDCP. Voir également l'article 23, point 2, a) de l'acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace CEDEAO du 16 Février 2010.

Dans le cas du décret de 2011 liant les opérateurs téléphoniques, la finalité du traitement est déterminée : c'est notamment celle de fournir aux autorités publiques des informations sur leurs abonnés. Ce décret ne peut donc servir de base légale pour la transmission des données au BIC. Si l'État veut imposer cette transmission aux grands facturiers, et donc les exempter de l'obligation d'obtenir un consentement préalable, encore faut-il franchir la « ligne rouge » tracée par l'UMOA. En effet, la loi uniforme 2014-02 du 30 décembre 2014, portant règlementation des Bureaux d'Information sur le Crédit (BIC) – transposée en 2016 au Togo[20] – fait du consentement préalable de la personne physique le fondement pour la collecte et la transmission des données à un BIC.

S'agissant des contrats liant les grands facturiers et leurs clients, un des fondements du traitement des données personnelles de ces derniers, ils ne peuvent autoriser la transmission des données collectées – pour des raisons contractuelles – au BIC que sous deux conditions minimales : l'information[21] et le recueil du consentement explicite du client. Lorsque ces conditions ne sont pas réunies, la transmission, voire la commercialisation, des données personnelles est illégale.

L'avis donné par l'Autorité de protection des données à caractère personnel[22] du Sénégal – la Commission de protection des données personnelles (CDP) – corrobore les précédents développements. En effet, en 2018, à la suite d'une demande d'avis relative au partage des données des clients des grands facturiers avec le BIC sans recourir au consentement des personnes concernées, l'autorité a émis un avis défavorable[23].

Cet avis était motivé par quatre éléments. Le premier est le fait que la législation nationale[24] pose le principe de l'obligation d'obtenir le consentement préalable des clients des grands facturiers avant tout partage. Ensuite, l'autorité souligne que la *« commercialisation de données à caractère personnel est strictement soumise à une autorisation préalable de la personne concernée en plus de la régularité du fichier »*. Le troisième élément est que les contrats liant les grands facturiers à leurs clients ne prévoient pas une telle communication. Enfin, le CDP

[20] Loi uniforme n° 2016-005 portant règlementation des Bureaux d'Information sur le Crédit (BIC).
[21] Voir les articles 35 à 38 de la LPDCP pour le contenu du droit à l'information.
[22] Aux termes de l'article 1er, alinéa 1, de l'Acte additionnel de la CEDEAO, il s'agit de l'autorité nationale administrative indépendante chargée de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions légales.
[23] Voir avis trimestriel n°02-2018 de la Commission de protection des données personnelles du Sénégal (CDP).
[24] Loi n° 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel.

rappelle que la loi uniforme portant règlementation des BIC fait du consentement préalable de la personne physique le fondement pour la collecte, la transmission des données à un BIC et l'émission des rapports de crédit.

Par ailleurs, au Togo, la loi uniforme de 2016 prévoit que les fournisseurs de données, ici les grands facturiers, doivent signer un contrat de prestation de services avec le BIC et adhérer au code de conduite et d'éthique qui confère le statut de fournisseur de données au BIC[25]. Outre l'obligation de garder la « confidentialité absolue » à l'égard du contenu des informations fournies aux BIC[26], les grands facturiers doivent également leur transmettre : les informations sur les antécédents de crédit de leurs clients ayant consenti au partage et à la consultation des ·informations sur le crédit les concernant[27] ; les informations sur le crédit dans les délais fixés par instruction de la Banque centrale selon les termes convenus avec le BIC en vertu du contrat de prestation de services signé[28]. En ce qui concerne les informations sur le crédit fournies au BIC, elles doivent répondre aux qualités de fiabilité et de précision. De ce fait, elles devront au besoin être mises à jour et corrigées.

Il convient de rappeler également que certains grands facturiers, principalement les opérateurs de téléphonie mobile, peuvent être soumis à l'extraterritorialité du RGPD. En effet, en vertu de de l'article 3, paragraphe 2, du RGPD, ce règlement s'applique au traitement des données personnelles relatives à des personnes qui se trouvent sur le territoire de l'Union européenne (UE) par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union. Par conséquent, le RGPD s'applique alors aux abonnés des compagnies de téléphonie mobile, en *roaming*, au sein de l'UE puisque les activités de traitement sont liées à l'offre, à titre gratuit ou non, de biens et de services. Il peut également s'agir du suivi du comportement de ces abonnés dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'UE. La durée du transit dans un territoire membre de l'UE importe peu. Même s'il ne dure que quelques minutes, il est fait obligation au responsable de traitement de respecter la législation européenne pendant ce laps de temps.

Les opérateurs de téléphonie mobile devront donc, en plus des démarches à effectuer auprès de l'Autorité nationale de protection des données à caractère personnel – l'Instance de protection

[25] Article 42, point 4, de la loi uniforme.
[26] Article 42, point 3, de la loi uniforme.
[27] Article 42, point 5, de la loi uniforme.
[28] Article 42, point 6, de la loi uniforme.

des données à caractère personnel (IPDCP) au Togo – obéir aux règles fixées par le RGPD afin de pouvoir rendre compte aux autorités européennes de contrôle. Il peut être notamment question de tenir un registre des activités de traitement[29]. Ledit registre comprend entre autres : une description générale des mesures de sécurité techniques et organisationnelles[30] ; les finalités du traitement[31] ; le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué[32] à la protection des données[33]. L'intérêt prononcé pour la protection des données à caractère personnel nous conduit donc à analyser la situation des clients qui font l'objet d'une sollicitude particulière de la part du législateur.

2. Les clients : les concernés protégés

Le législateur a pris soin de garantir la protection des droits des clients des grands facturiers, qu'il s'agisse du droit à l'information ou du droit d'accès **(a)**. Les clients peuvent également exercer des recours en cas d'atteintes injustifiées à leurs droits **(b)**.

a. La préservation des droits : du droit à l'information au droit d'accès

Pour prendre une décision éclairée, les clients, dont les données innervent la plateforme d'échange d'informations gérée par un BIC, doivent être informés. Ce devoir d'information incombe, comme vu précédemment, en premier lieu aux fournisseurs d'informations dont font partie les grands facturiers. Cette obligation pèse aussi sur le BIC et sur les utilisateurs de données sur le crédit.

Nous nous consacrerons ici à l'analyse des obligations générales d'information pesant sur l'ensemble des responsables de traitement des données : les grands facturiers, la plateforme de partage d'informations et les utilisateurs de données sur le crédit. Les obligations spécifiques à ces deux dernières catégories d'acteurs seront analysées plus loin. Aux termes de l'article 35 de la LPDCP, le responsable du traitement doit communiquer à la personne concernée, au plus tard, lors de la collecte et quels que soient les moyens et supports employés, les informations

[29] Article 30 du RGPD.
[30] Article 30, g) du RGPD.
[31] Article 30, b) du RGPD.
[32] Dénommé « Correspondant à la protection des données à caractère personnel » en droit togolais. Voir article 75 de la LPDCP.
[33] Article 30, a) du RGPD.

suivantes : l'identité du responsable du traitement et, le cas échéant, de son représentant ; la ou les finalités déterminées du traitement auquel les données sont destinées ; les catégories de données concernées ; le ou les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées[34] ; le caractère obligatoire ou non de répondre aux questions et les conséquences éventuelles d'un défaut de réponse ; la possibilité de demander à ne plus figurer sur le fichier ; l'existence d'un droit d'accès aux données la concernant et de rectification de ces données ; la durée de conservation des données ; le cas échéant, des transferts de données à caractère personnel envisagés à destination de l'étranger.

Lorsque les informations ne sont pas collectées directement auprès de la personne concernée, les informations susmentionnées doivent lui être transmises au moment de l'enregistrement des données ou, si leur communication est prévue, au plus tard lors de la première communication[35]. Qu'arrive-t-il alors lorsque la finalité du traitement des données collectées change ? En l'absence de réponse expresse dans la LPDCP, il convient de retenir qu'il revient au responsable du traitement – lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données ont été obtenues – de fournir au préalable à la personne concernée des informations au sujet de cette autre finalité[36].

Toutefois, le droit à l'information connaît des limites. L'article 38 de la LPDCP en énumère trois. D'abord, lorsque les données sont recueillies et utilisées lors d'un traitement mis en œuvre pour le compte de l'État et intéressant la sûreté de l'État, la défense, la sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté, dans la mesure où une telle limitation est nécessaire au respect des fins poursuivies par le traitement. Ensuite, lorsque le traitement est nécessaire à la prévention, la recherche, la constatation et la poursuite de toute infraction. Enfin, lorsque le traitement est essentiel à la prise en compte d'un intérêt économique ou financier important de l'État, y compris dans les domaines monétaire, budgétaire, douanier et fiscal.

En sus du droit à l'information ; une fois le consentement donné, et les informations collectées, la personne concernée par le traitement a le droit d'accéder à ses données. Le droit d'accès permet à la personne concernée de demander au responsable du traitement de lui transmettre

[34] On peut y ajouter, le cas échéant, les coordonnées du correspondant à la protection des données à caractère personnel.
[35] Article 37 de la LPDCP. Voire également article 13 du RGPD.
[36] V. les dispositions de l'article 14, paragraphe 4, du RGPD.

entre autres : les informations permettant de connaître et de contester le traitement ; la confirmation que ses données font ou ne font pas l'objet de ce traitement ; la communication des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées[37].

La personne concernée peut aussi demander la transmission d'une copie des données personnelles en possession du responsable du traitement[38]. Afin de rendre le droit d'accès effectif, il est prévu que toute personne, qui a des raisons sérieuses de penser que les données qui lui ont été communiquées ne sont pas conformes aux données traitées, puisse informer l'Instance de protection des données à caractère personnel (IPDCP)[39] qui procèdera aux vérifications nécessaires[40]. La personne concernée peut aussi, dans certaines conditions, user de voies de recours pour assurer le respect de ses droits.

b. La subsistance de « voies de recours » : de l'opposition à la mise en jeu de responsabilités

Dans sa relation avec les grands facturiers, fournisseurs des données au BIC, le client dispose de plusieurs « voies de recours » dont font partie : le droit d'opposition et le droit de rectification et de suppression. En vertu du droit d'opposition, toute personne physique a le droit de s'opposer – pour des motifs légitimes – à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement. Elle a aussi le droit d'être informé avant que ses données ne soient transmises pour la première fois à des tiers et de se voir expressément offrir le droit de s'y opposer de manière gratuite. Toutefois, il faut rappeler que le droit d'opposition n'est pas applicable lorsque le traitement répond à une obligation légale[41].

---

[37] Article 39 de la LPDCP.
[38] Article 40 de la LPDCP.
[39] Le projet de décret portant organisation et fonctionnement de l'IPDCP a été adopté le 09 décembre 2020 en Conseil des Ministres. Togopresse, «Le Conseil des ministres adopte le projet de décret portant organisation et fonctionnement de l'IPDCP », 9 décembre 2020, disponible sur : https://togopresse.tg/le-conseil-des-ministres-adopte-le-projet-de-decret-portant-organisation-et-fonctionnement-de-lipdcp/. V. aussi Ministère de l'économie numérique, « Le Gouvernement adopte le décret portant organisation et fonctionnement de l'Instance de protection des données à caractère personnel (IPDCP) », 11 décembre 2020, disponible sur :https://numerique.gouv.tg/le-gouvernement-adopte-le-decret-portant-organisation-et-fonctionnement-de-linstance-de-protection-des-donnees-a-caractere-personnel-ipdcp/.
[40] Article 41 de la LPDCP.
[41] Article 45 de la LPDCP.

Le client a aussi intérêt à pouvoir corriger les informations la concernant. Ainsi la personne concernée peut exiger du responsable de traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou supprimées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite[42]. Si les données avaient été transmises à des tiers, à l'instar du BIC, il incombe alors au responsable de traitement, ici le grand facturier, d'accomplir les diligences utiles pour notifier les modifications effectuées[43].

Au cas où les données transmises au BIC s'avèrent inexacte par la faute du grand facturier qui n'a pas tenu à jour les informations du client – en vertu du principe de l'exactitude – le client qui s'est vu refuser l'octroi d'un crédit peut engager sa responsabilité. Aux termes de l'article 17 de la LPDCP, le principe de l'exactitude implique que les données collectées doivent être exactes et, si nécessaire, mises à jour. Toutes les mesures raisonnables doivent être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement, soient effacées ou rectifiées. Pour que l'action en responsabilité aboutisse, il faudra tout de même prouver que c'est cette inexactitude qui est à la base d'un rapport de crédit défavorable à l'octroi de crédit. D'ailleurs, l'article 57 de la loi uniforme dispose que le fournisseur de données engage sa responsabilité civile et pénale non seulement pour toute collecte de renseignements en l'absence de consentement, mais aussi sa responsabilité en cas de transmission de données erronées au BIC.

Le cadre légal ne se limite pas seulement le processus de collecte et de transmissions des données dans le cadre du partage d'informations sur le crédit. Le législateur fixe également les conditions d'exploitation des données traitées permettant de réduire, un peu plus, les risques d'atteintes aux libertés et droits fondamentaux des personnes concernées.

B. L'organisation rigoureuse de l'exploitation des données personnelles

Le cadre juridique de partage d'informations sur le crédit impose des obligations, relatives aux conditions de traitement des données personnelles, non seulement à la charge BIC **(1)**, mais aussi à la charge des utilisateurs des données traitées par ce dernier **(2)**.

---

[42] Article 46, alinéa 1er, de la LPDCP.
[43] Article 46, alinéa 4, de la LPDCP.

1. Le bureau d'information sur le crédit : le destinataire obligé

Le BIC ne peut exercer son activité qu'après l'obtention préalable d'un agrément **(a)**. Aussi, l'exercice de la fonction de BIC implique le respect d'un certain nombre de prescriptions légales **(b)**.

a. La nécessité d'un agrément préalable

Le décret de 2018 désigne comme destinataires des données personnelles collectées par les grands facturiers, le BIC et les officiers de police judiciaire compétents[44]. Rappelons qu'un BIC est une institution qui : collecte auprès des organismes financiers, des sources publiques et des grands facturiers (sociétés d'électricité, d'eau et de téléphonie mobile), des données disponibles sur les antécédents de crédit ou de paiement d'un emprunteur ; traite les informations collectées à l'aide de techniques (statistiques, informatiques, etc.) appropriées ; commercialise les produits dérivés de ces informations traitées (notamment des rapports de solvabilité et des *scoring*) auprès, entre autres, d'établissements de crédit[45].

La loi uniforme de 2016 soumet l'exercice de la fonction de BIC[46] à l'obtention préalable d'un agréement et l'inscription sur la liste des BIC[47]. Ne peuvent prétendre à l'obtention de cet agrément que les personnes morales présélectionnées à l'issue d'un appel à concurrence. Dans l'espace UMOA, ce dernier est organisé par la Banque centrale[48]. C'est ainsi qu'à la suite d'une procédure conforme aux dispositions prévues par les articles 5 à 7 de la loi uniforme la Société CREDITINFO-VOLO a obtenu un agrément unique lui permettant d'exercer l'activité de BIC dans l'UMOA[49] et donc au Togo. Le BIC est autorisé à effectuer comme activités entre autres : la collecte et le stockage des informations sur le crédit ; le traitement des informations sur le crédit ; la fusion de différentes sources d'informations et la mise à disposition des utilisateurs

---

[44] Article 5 du décret de 2018.
[45] BCEAO, « Qu'est-ce qu'un Bureau d'Information sur le Crédit (BIC) ? », Disponible en ligne sur : https://www.bceao.int/fr/documents/1-quest-ce-quun-bureau-dinformation-sur-le-credit-bic.
[46] Le cadre légal de l'activité du BIC dans l'UMOA est constitué, d'une part, de la loi uniforme portant réglementation des BIC dans l'UMOA, adoptée par le Conseil des Ministres de l'UMOA au cours de sa session du 28 juin 2013 pour être insérée dans l'ordonnancement juridique interne des États membres et, d'autre part, des textes d'application de ladite loi.
[47] Article 4 de la loi uniforme.
[48] Article 5 de la loi uniforme.
[49] À ce jour, la Société CREDITINFO-VOLO, dont le siège social se trouve en République de Côte d'Ivoire, s'est déployée sur l'ensemble de l'espace Communautaire, à la faveur de l'entrée en vigueur de la loi uniforme portant réglementation des BIC et des autorisations d'installation de bureaux de représentation dans tous les États membres de l'Union.

des rapports de crédit à titre onéreux ; la diffusion des informations de crédit et des rapports pour les utilisateurs[50]. Le BIC est aussi autorisé à identifier les clients par « tout moyen approprié[51], notamment la biométrie »[52].

L'agrément peut être retiré par un arrêté du ministre chargé des finances de l'État du siège social du BIC, après avis conforme de la Banque centrale dans quatre cas limitativement énumérés[53]. Tout d'abord, le BIC peut se voir retirer son agrément s'il ne démarre pas « effectivement » ses activités dans les deux ans suivant la notification de l'arrêté portant agrément dudit BIC[54]. Ensuite, l'agrément peut être retiré en cas de commission d'infractions « graves ou répétées » à la réglementation des BIC ou à toute autre règlementation applicable aux BIC[55]. Il en est de même lorsque le BIC n'exerce plus d'activités depuis au moins un an[56]. Enfin, le BIC peut perdre son agrément lorsqu'il transfère son siège social hors de l'UMOA, y compris lorsqu'il intervient à la suite d'opération de fusion par absorption, scission ou création d'une société nouvelle[57].

Le retrait d'agrément du BIC par l'État du siège d'origine dudit BIC s'étend aux représentation et succursale dans les autres États membres de l'UMOA[58]. Toutefois, en cas de retrait d'agrément d'une société-mère, il revient au ministre des finances de l'État d'implantation d'une filiale de décider du sort de cette dernière[59]. En ce qui concerne le sort de la base de données constituée par le BIC et toute copie électronique de secours, l'article 8, alinéa 4, de la loi uniforme prévoit qu'elles soient transférées à la Banque centrale. Quelles sont alors les obligations pesant sur le BIC agréé dans le cadre de ses activités ?

b. Les obligations de l'agréé

Les données recueillies et diffusées par le BIC, dans un État membre de l'UMOA, ne peuvent être délocalisées, conservées et maintenues que dans l'espace UMOA. Cette obligation

---

[50] Article 33 de la loi uniforme.
[51] Il faudrait sans doute en déduire la nécessaire légalité des moyens utilisés en vertu de la règlementation en vigueur, notamment, en matière de protection des données à caractère personnel.
[52] Article 34 de la loi uniforme.
[53] Article 8 de la loi uniforme.
[54] Article 8, point 1, de la loi uniforme.
[55] Article 8, point 2, de la loi uniforme.
[56] Article 8,point 3, de la loi uniforme.
[57] Article 8, point 4, de la loi uniforme.
[58] Article 11, alinéa 1er, de la loi uniforme.
[59] Article 11, alinéa 2, de la loi uniforme.

concerne l'ensemble des bases de données et les sites de sauvegarde[60]. En outre, pour diffuser les informations, le BIC ne doit utiliser que les moyens qui répondent aux dispositions de sécurité, de confidentialité, de protection des données, y compris les données personnelles, et d'intégrité[61].

Afin d'assurer l'intégrité des données personnelles, le BIC doit s'assurer de la mise en place d'un dispositif adéquat ayant les capacités de sécuriser la base de données et d'éviter l'accès, la modification et la divulgation non autorisée des informations[62]. Il doit informer la Banque centrale des insuffisances constatées dans le dispositif de sécurité à chaque fois que le système enregistre « une menace »[63].

Le BIC a également pour obligation de fournir aux utilisateurs des données des rapports de crédit[64] mis à jour[65] en s'assurant que les informations qu'elles diffusent ne datent pas de plus de cinq ans[66]. Il doit donc prendre les mesures nécessaires à même d'assurer l'exactitude des données au même titre que les fournisseurs de données[67]. Les clients ont également le droit de contester et de rectifier les données les concernant en possession du BIC[68]. En ce sens le BIC met à disposition des clients les informations concernant la procédure de saisine lui permettant d'accéder aux informations sur le crédit les concernant, de les faire corriger voire supprimer[69].

En outre, il est formellement interdit de procéder au traitement ou de faire figurer dans un rapport de crédit des données sensibles[70]. Il convient tout de même de souligner que la définition des données sensibles diverge entre la loi uniforme de 2016 et la loi sur la protection des données à caractère personnel de 2019. Cette dernière inclut les données relatives *« aux poursuites, aux sanctions pénales ou administratives »*[71]. S'il ne s'agit pas seulement d'une

---

[60] Article 35 de la loi uniforme.
[61] Article 37 de la loi uniforme. Voir aussi l'article 10, alinéa 1er, du décret de 2018.
[62] Article 41, point 11, de la loi uniforme.
[63] Article 41, point 10, de la loi uniforme.
[64] Ils comportent selon l'article 1er, alinéa 10, de la loi uniforme : *« les antécédents de crédit, l'historique de paiement ou la compilation d'informations fournies par un BIC sur support écrit ou électronique, liés à des obligations financières d'une personne physique ou morale notamment les antécédents de paiement de ses engagements, ou des informations accessibles au public et toutes autres données pertinentes recueillies par le BIC et autorisées (…) ».*
[65] Article 41, point 2, de la loi uniforme.
[66] Article 41, point 3, de la loi uniforme.
[67] Article 41, point 13, de la loi uniforme.
[68] Article 41, point 6, de la loi uniforme.
[69] Articles 45 et 48 de la loi uniforme.
[70] Article 62, alinéa 1er, de la loi uniforme.
[71] Article 4, alinéa 8, de la LPDCP.

différence liée au moment de la rédaction des deux textes, l'exclusion des sanctions, par la loi uniforme, permet ainsi de mentionner – dans le rapport de crédit – si une personne a déjà fait l'objet d'interdiction d'exercer une activité pour laquelle elle vient demander un prêt bancaire.

Si cette hypothèse ne pose pas véritablement de difficultés lorsqu'il s'agira d'une personne morale, il en est autrement lorsqu'il s'agira d'un client personne physique. Faudra-t-il appliquer la LPDCP ou la loi uniforme ? On serait tenté d'opter pour la loi sur la protection des données à caractère personnel excluant de ce fait la possibilité pour le BIC de mentionner les sanctions infligées à une personne physique ou les poursuites dont elle fait l'objet. Cependant, en application de la maxime selon laquelle *speciala generalibus derogant* ; en la matière c'est la loi uniforme qui devrait prévaloir. D'ailleurs en matière bancaire l'obligation d'identification des clients (*Know Your Customer, KYC*) doit s'appliquer. Cela implique notamment pour l'établissement de crédit de savoir si son client a déjà fait l'objet de condamnations pouvant l'empêcher d'avoir accès au crédit. Néanmoins, au regard de la proportionnalité du traitement des informations effectuées, il faudra que le BIC ne mentionne que les poursuites ou sanctions pouvant influencer l'octroi d'un crédit bancaire par exemple. On peut donc exclure, par exemple, les contraventions liées au non-respect du Code de la route.

Par ailleurs, le BIC doit permettre aux clients d'accéder à leurs rapports de crédit lorsque les antécédents de crédit de ces derniers sont en sa possession[72]. Il doit également mettre en place un dispositif de traitement des réclamations des clients tout en s'assurant de la qualité des données en sa possession[73]. Ainsi, le BIC doit tenir un registre sur les manquements relatifs à la qualité des données transmises[74]. Il lui est également fait obligation de garder un registre de toutes les demandes de renseignements et autres demandes reçues des utilisateurs indiquant la finalité de ces dernières[75].

En respectant le principe de finalité, de pertinence et de conservation[76] en matière de traitement des données personnelles, la loi uniforme de l'UMOA fixe la durée de l'archivage des informations recueillies à cinq ans. Ces dernières peuvent être utilisées en cas de contentieux

[72] Article 41, point 5, de la loi uniforme.
[73] Article 41, point 7 et 8, de la loi uniforme.
[74] Article 41, point 14, de la loi uniforme.
[75] Article 41, point 9, de la loi uniforme.
[76] Article 16 du décret de 2018. V. aussi article 25 de l'acte additionnel relatif à la protection des données à caractère personnel de la CEDEAO.

judiciaire ou sur requête de la BCEAO[77]. En outre, le décret de 2018 fixe une durée de 10 ans maximum pour la conservation des données collectées. Cette durée englobe celle de validité de données diffusables par le BIC, soit cinq ans, et la durée de l'archivage également de cinq ans fixées par la loi uniforme de l'UMOA. Au-delà de ce délai, la conservation de ces données n'est donc plus autorisée.

Pour finir, il faut rappeler que le BIC a l'obligation de communiquer certaines informations[78] aux personnes dont les données personnelles. Il s'agit notamment de : l'identité du responsable du traitement et le cas échéant de son représentant légal ; les objectifs du traitement ; les catégories de données concernées ; les destinataires auxquelles les données sont susceptibles d'être communiquées ; l'existence des droits d'accès, de rectification et d'opposition pour les personnes concernées, et les coordonnées du service auprès duquel elles doivent faire valoir lesdits droits ; la durée de conservation des données traitées ; l'éventualité du transfert des données traitées à destination de pays tiers. Ces informations sont transmises par le biais : d'affiches dans les lieux où s'effectue le traitement autorisé ; de mentions légales sur les formulaires et sur son site internet ; de la presse[79]. Il convient de rappeler que l'article 35, alinéa 2, de loi uniforme interdit le transfert des données en dehors de l'espace UMOA.

S'agissant de l'information du transfert des données vers un pays tiers de l'UMOA, le client togolais, par exemple, doit savoir si ces données seront transférées vers le Sénégal ou la Côte d'Ivoire. Si le cadre juridique de protection de ses données dans ces pays n'offrait pas un niveau de protection équivalent à celui du Togo il pourrait, le cas échéant, s'y opposer[80]. Même s'il occupe la place centrale dans le système de partage d'informations sur le crédit, le BIC n'est pas la seule personne soumise à des obligations, il en est de même pour les utilisateurs de ses services.

---

[77] Article 41, point 4, de la loi uniforme.
[78] Article 8 du décret de 2018.
[79] Article 9 du décret de 2018.
[80] Voir en ce sens les motifs de l'annulation du bouclier de protection des données – *Privacy Shield* – entre l'UE et les États-Unis dans l'affaire *Schrems II*. CJUE 16 juillet 2020, Aff. C 311/18, *Data Protection Commissioner c./ Facebook Ireland Ltd, Maximillian Schrems.* L. COSTES, « Le « bouclier de protection des données » (accord « Privacy Shield ») annulé par la CJUE », *RLDI*, août 2020, n° 173, pp. 23-25. *Adde* C. CRICHTON, « Transfert de données vers les USA : l'arrêt Schrems II », *Dalloz actualité*, juillet 2020.

2. Les utilisateurs des données : les bénéficiaires coobligés

Les personnes utilisatrices des données traitées dans le cadre du partage d'informations sur le crédit sont formellement identifiées par le législateur **(a)** qui les soumet à des obligations vis-à-vis, notamment, de leurs clients **(b)**.

a. L'identification des utilisateurs autorisés

Aux termes de l'article 60 de la loi uniforme de 2016, sont concernés par le partage d'informations, les établissements de crédits et les systèmes financiers décentralisés (SFD) soumis au contrôle de la BCEAO et de la commission bancaire de l'UMOA. Afin d'évaluer le risque de crédit de leurs clients, ils doivent adresser une requête au BIC pour obtenir un rapport de crédit. Cependant, le client concerné doit donner préalablement son consentement libre et écrit[81]. La demande d'un rapport de crédit, sans autorisation de l'emprunteur, n'est donc pas possible pour les utilisateurs de la plateforme. Ils ne peuvent pas non plus la lui imposer.

S'ils obtiennent le rapport de crédit, bien entendu avec l'accord de leur client, ledit rapport doit figurer dans le dossier de l'emprunteur[82]. En vue d'alimenter la plateforme, les différents utilisateurs doivent aussi participer à la collecte des informations sur le crédit en partageant les données sur tous les prêts dans leur portefeuille[83]. Peuvent aussi participer au système d'échanges d'informations sur le crédit dans les mêmes conditions que celles fixées par l'article 60 de la loi uniforme : les SFD soumis au contrôle du ministère chargé des finances, les institutions communes de financement, les institutions financières exerçant une activité de garantie de crédit, les sociétés commerciales, les concessionnaires de services publiques et tout autre entité ou intermédiaire dont les activités comprennent l'octroi de crédits ou qui offrent des options de paiement en différé[84].

Il faut reconnaître que l'ouverture de la plateforme à d'autres entités telles que les sociétés commerciales est une opportunité pour ces dernières pour mieux choisir leurs partenaires. Encore faut-il que ces derniers consentent à jouer le « jeu de la confiance » en partageant leurs antécédents de crédits. Cela permet également de prendre en compte des informations

[81] Article 60, point 1, de la loi uniforme.
[82] Article 60, point 2, de la loi uniforme.
[83] Article 60, point 3, de la loi uniforme.
[84] Article 61 de la loi uniforme.

susceptibles d'échapper à un système clos entre établissement de crédits et SFD soumis au contrôle de la BCEAO et de l'UMOA. Si c'était le cas, la base de données disponible serait assez incomplète puisqu'elle ne donnerait pas une vue d'ensemble de la situation réelle du client.

Au regard de la sensibilité des informations auxquelles les utilisateurs des services du BIC auront accès, ils sont également contraints de respecter certaines prescriptions destinées à assurer la sauvegarde des droits des personnes concernées.

b. Les obligations des utilisateurs autorisés

Au-delà de l'obligation de l'utilisateur de données sur le crédit d'assurer la confidentialité des données qui lui sont transmises par le BIC, l'utilisateur doit, entre autres, fournir au client une copie du rapport de crédit qui a servi de base à la prise d'une décision défavorable à son égard[85]. Cette copie doit aussi lui être fournie même si la suite défavorable n'est fondée qu'en partie sur les informations contenues dans le rapport de crédit provenant d'un BIC[86].

En outre, la finalité du rapport de crédit doit être respectée. Ainsi, il est interdit à l'utilisateur des données de communiquer les informations issues des rapports de crédit ou de les utiliser à des fins commerciales, de marketing, d'études de marché, de publicité et/ou de vente directe de produits ou de services, et de ciblages des clients d'autres utilisateurs[87].

L'utilisateur de données sur le crédit engage sa responsabilité civile et pénale pour toute demande de rapports de crédits non autorisée par la personne physique ou morale concernée. Il en est de même pour toute utilisation illicite ou abusive des informations sur le crédit qui lui sont fournies notamment à des fins commerciales[88].

Malgré l'existence de mesures techniques et législatives censées minimiser voire, dans la mesure du possible, exclure les risques liés au traitement des données personnelles, force est de constater que le mécanisme de partage d'informations sur le crédit laisse subsister quelques failles sources de risques.

---

[85] Article 43, point 4, de la loi uniforme.
[86] Article 47 de la loi uniforme.
[87] Article 43, point 4 et 5, de la loi uniforme.
[88] Article 58 de la loi uniforme.

II. Un cadre de partage des données personnelles en réalité à risques

Les risques liés au partage des données à caractère personnel des clients peuvent être essentiellement décelés à deux niveaux. Le premier est celui du mode de fonctionnement de la plateforme de partage d'informations sur le crédit **(A)**. Le second est relatif à l'accessibilité et l'utilisation des données collectées par d'autres personnes, en dehors notamment des établissements de crédits et des SFD, à l'instar de l'administration judiciaire **(B)**.

A. La sensibilité du mécanisme de traitement des données collectées par la plateforme

Le partage des informations sur le crédit des clients est censé favoriser une meilleure évaluation de la solvabilité des clients au profit des utilisateurs des données sur le crédit. Cependant cette opération n'est pas sans difficultés **(2)**. Il convient aussi d'analyser l'impact d'une modification de la loi uniforme de 2016 touchant au consentement préalable du client avant tout traitement de ses données **(1)**.

1. La mise en veilleuse « temporelle » du consentement préalable : la modification de l'article 53 « originel »

Dans sa version initiale, l'article 53 de la loi uniforme n° 2016-005 portant règlementation des Bureaux d'Information sur le Crédit (BIC) ne contenait que quatre alinéas. Une modification substantielle y ajoutera un cinquième alinéa qui prévoit que l'obligation d'obtenir le consentement préalable des clients ne s'applique pas au client ayant bénéficié de crédits avant l'entrée en vigueur de la loi uniforme sur les BIC au Togo, plus précisément le 16 mars 2016[89].

Avant la modification de l'article 53, outre les autorisations légales limitativement énumérées, il n'y avait pas de dérogation au principe posé par l'alinéa 1er dudit article qui dispose que : *« toute collecte d'informations, toute utilisation, tout partage et diffusion de renseignements personnels, y compris les informations sur le crédit, sont subordonnés au consentement préalable du client, personne physique ou morale, concerné ».*

En décidant, de ne plus donner force obligatoire au consentement préalable du client quant aux traitement de ses données personnelles, comme prévu à l'article 1er de l'article 53 originel, il

[89] Nouvel article 53, alinéa 5, de la loi uniforme introduit par la loi n° 2018-009 du 27 juin 2018 modifiant l'article 53 de loi uniforme du 14 mars 2016 portant règlementation des Bureaux d'Information sur le Crédit (BIC) dans les États membres de l'Union Monétaire Ouest-Africaine (UMOA).

s'agit là d'une véritable entorse au principe du consentement et de légitimité du traitement qui impose le consentement préalable de la personne concernée[90]. En principe, le responsable du traitement ne peut y déroger que si le traitement est notamment nécessaire pour assurer le respect d'une obligation légale ou encore l'exécution d'une mission d'intérêt public. C'est ce que permet la modification de l'article 53 de la loi uniforme.

Doit-on considérer qu'il s'agit là de l'imposition d'une obligation de traitement – au sens stricte du terme – ou d'une « simple » exemption d'obtenir le consentement de la personne concernée ? En effet, le nouvel alinéa 5 de l'article 53 dispose : *« L'obligation d'obtenir le consentement préalable du client (…) ne s'applique pas au client ayant bénéficié de prêts avant le 16 mars 2016 »*. Au vu de la formulation utilisée par le législateur, nous optons pour la seconde option. En outre, si les responsables de traitements – ici les grands facturiers, le BIC et les utilisateurs de données – sont ainsi exemptés de l'obligation d'obtenir le consentement préalable des personnes ayant bénéficiées de crédits avant le 16 mars 2016, qu'est-ce qui pourrait justifier ce choix du législateur ?

À première vue, il s'agit là d'un choix éminemment politique pour arriver à mettre en route la plateforme de partage d'informations sur le crédit dont le démarrage était ralenti par la nécessité d'obtenir le consentement préalable des clients. L'exposé des motifs de la loi n° 2018-11 modifiant la loi uniforme n° 2014-02 du 06 janvier 2014 portant règlementation des Bureaux d'information sur le crédit (BIC) dans les pays membres de l'Union Monétaire Ouest Africaine, au Sénégal, faisait ainsi état des difficultés de fonctionnement du BIC. En effet, le législateur y exprime ses inquiétudes sur l'atteinte des avantages attendus du partage d'informations sur le crédit en raison de la faiblesse des données collectées notamment sur l'historique de crédit qui ne permettent pas d'alimenter la base de données du BIC et de produire des rapports de qualité.

D'ailleurs, à la suite de la modification de la loi uniforme sur les BIC dans l'espace UMOA, le nombre de clients enregistré dans la base du BIC est passé de 30.694 en fin février 2016, période de démarrage des activités de CREDITINFO-VOLO, à 5.820.029 au 31 mars 2019, dont 93.577 personnes morales et 5.726.452 personnes physiques. Cette évolution traduit principalement l'effet combiné d'une part de l'adoption par certains États de textes dispensant, les établissements assujettis, de l'obligation de recueil de consentement pour le partage des données

[90] Aux termes de l'article 14 de la LPDCP, le traitement est considéré comme légitime si la personne concernée donne son consentement.

des clients ayant bénéficié de prêts avant la date d'entrée en vigueur de la loi uniforme (Côte d'Ivoire, Niger, Sénégal et Togo), et d'autre part, de textes complémentaires autorisant la mise en œuvre d'un traitement automatisé de données personnelles pour l'intégration des grands facturiers à la plateforme électronique de partage d'informations sur le crédit (Côte d'Ivoire, Niger et Togo).

Cependant, même si l'on considérait que la loi uniforme de 2016 ne valait que pour l'avenir, est-ce à dire qu'aucun texte, même d'ordre général, ne justifiait le besoin d'obtenir le consentement préalable de la personne concernée avant tout traitement de ses données à caractère personnel. Était notamment en vigueur avant le 16 mars 2016, l'Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace CEDEAO du 16 février 2010 et la Convention de l'Union africaine (UA) sur la cybersécurité et la protection des données à caractère personnel adoptée le 27 juin 2014[91]. En principe, le législateur ne devrait pouvoir déroger au principe du consentement préalable notamment qu'en présence d'un motif d'intérêt général. Si l'on peut comprendre l'opportunité d'une telle décision lourde d'implications juridiques pour les clients – qui ne peuvent donc en principe user du droit d'opposition pour les informations consenties avant l'entrée en vigueur de la loi sur le BIC – on peut se demander si elle est justifiée par un motif d'intérêt général ? La réponse ne va pas de soi.

Néanmoins, à certains égards, le motif d'intérêt général peut être assimilé aux objectifs de l'opérationnalisation de la plateforme de partage d'informations sur le crédit dont l'existence bénéficie aux clients, aux utilisateurs des données – notamment les établissements de crédit, les SFD et autres institutions financières concernées – et l'économie nationale. Sur ce dernier aspect, le partage d'information contribue : à l'amélioration du financement des agents économiques à moindre coût ; au renforcement de la supervision de l'activité de crédit – à l'instar de la prévention du surendettement – et la maîtrise du risque systémique. Par ailleurs, le BIC contribuerait à améliorer la réputation d'un pays sur le plan international et donnerait une appréciation de la solidité de son système financier[92]. Qu'en est-il de la possibilité pour les

[91] À la date du 18 juin 2000, ladite Convention n'est toujours pas entrée en vigueur. Seuls huit instruments de ratification ont été déposés sur les quinze nécessaires à l'entrée en vigueur. Pour sa part le gouvernement togolais a adopté en octobre 2019 un projet de loi autorisant la ratification de la Convention de Malabo.

[92] Voir, au Sénégal, l'exposé des motifs de la loi n° 2018-11 modifiant la loi uniforme n° 2014-02 du 06 janvier 2014 portant règlementation des Bureaux d'information sur le crédit (BIC) dans les pays membres de l'Union Monétaire Ouest-Africaine, pp. 1-2.

utilisateurs des services du BIC de mieux évaluer la solvabilité de l'emprunteur ? Ne présente-t-elle aucun risque pour les droits et libertés fondamentaux des personnes concernées ?

2. La complexité de l'évaluation de la solvabilité du client : le *scoring*

Le *scoring* est la méthodologie statistique développée à partir des données recueillies par le BIC, qui permet d'évaluer la solvabilité ou le profil de risque d'un demandeur de crédit[93]. Cette méthodologie pose quelques interrogations. Le client dont le profil de risque est établi peut-il, au-delà de la contestation de l'exactitude des données utilisées pour réaliser l'évaluation, demander que lui soit communiqué la méthodologie employée, voire le code source de l'algorithme utilisé lorsqu'il s'agira d'un traitement automatisé, pour vérifier la loyauté de l'algorithme ou l'exactitude des résultats obtenus ?

Il convient de rappeler que lorsque les traitements effectués sont susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, le responsable de traitement doit procéder à une analyse d'impact relative à la protection des données à caractère personnel (AIPDCP). L'AIPDCP doit être réalisée avant la mise en œuvre du traitement et mise à jour tout au long de son cycle de vie. Cependant, en l'absence de précisions suffisantes dans la LPDCP – et en l'absence de prévision dans le cadre de l'Acte additionnel de la CEDEAO – il faudra donc attendre que le cadre de mise en œuvre de l'AIPDCP soit défini par l'Instance de protection des données à caractère personnel (IPDCP) au Togo.

En France, à titre comparatif, une analyse d'impact doit être notamment menée lorsque le traitement remplit au moins deux des neuf critères issus des lignes directrices du G29 : évaluation/*scoring* – y compris le profilage – ; décision automatique avec effet légal ou similaire ; collecte de données sensibles ou données à caractère hautement personnel ; croisement de données. On peut donc en déduire que le traitement opéré par le BIC – qui permet entre autres l'évaluation du profil de risque du client et le croisement des données de ce dernier – doit faire l'objet d'une AIPDCP.

Quoiqu'il en soit, l'utilisateur des données sur le crédit ne peut en principe prendre sa décision uniquement sur le fondement d'un traitement automatisé. En effet, il ressort de l'article 27, alinéa 2, de la LPDCP qu'aucune décision produisant des effets juridiques à l'égard d'une

[93] Article 1er, alinéa 11, de la loi uniforme.

personne ne peut être prise sur le seul fondement d'un traitement automatisé des données à caractère personnel destiné à définir le profil de l'intéressé. Peut-être pourrait on inclure dans la notion de « profil de l'intéressé » son profil de risque et de solvabilité.

Cependant, quelques soucis pourraient se poser s'agissant des données utilisées pour la réalisation du *scoring*. En effet, il s'agit de la prise en compte d'informations sur le crédit concernant l'emprunteur qui en fait dépendent d'autres personnes. Pour mieux exprimer cette situation prenons l'exemple suivant : un bailleur d'immeuble dont les factures – eau, électricité, téléphonique – sont en son nom, alors qu'il ne gère pas le paiement de ces dernières qui incombe à son preneur à bail. En principe du fait de l'automaticité de la transmission des informations par les grands facturiers, les informations, faisant par exemple état d'impayés, seront prises en compte dans l'évaluation de sa solvabilité. Il peut en être de même dans le cas de la vente d'un immeuble dont les factures portent toujours le nom de l'ancien propriétaire.

En l'absence de faute de mise à jour des informations du fait du grand facturier, à qui la personne concernée n'a pas dûment signifié le transfert, le client ne peut alors lui imputer le *scoring* défavorable dont il peut faire l'objet. Il reviendra donc au client de faire les démarches nécessaires lorsqu'ils se retrouvent dans de telles situations. Il doit aussi, et surtout, en avertir l'utilisateur de données – à l'instar de l'établissement de crédit – pour qu'il en tienne compte dans la décision d'octroi de crédit. En dehors des opérations de crédits, le législateur rend accessible les données collectées par le BIC dans le cadre notamment de procédures judiciaires. Toutefois, ce cadre reste encore perfectible.

B. L'inachèvement du cadre de traitement des données par l'administration judiciaire

Le législateur rend accessible, sous certaines conditions, les données traitées dans le cadre du système d'échange d'informations sur le crédit à certaines personnes intervenant dans les procédures judiciaires voire administratives **(1)**. Cependant, cette ouverture circonstanciée contraste avec une insuffisance d'encadrement **(2)**.

1. L'élargissement du champ d'accessibilité des données

L'article 6 du décret de 2018 prévoit que les officiers de police judiciaire (OPJ) compétents munis d'une autorisation du président du tribunal, d'une réquisition du procureur de la République ou d'une ordonnance du juge d'instruction peuvent accéder aux données dont le

traitement est autorisé. Il en est de même pour les autorités publiques habilitées dans l'exercice de leurs missions, et les prestataires techniques et agents chargés du fonctionnement, de la maintenance et de l'entretien du dispositif désignés pour une durée limitée.

Rappelons que les OPJ sont des fonctionnaires placés sous l'autorité du parquet et le contrôle de la chambre de l'instruction ayant pour mission d'accomplir les opérations à l'enquête de police (préliminaire), ou à la flagrance (flagrant délit) et d'effectuer les délégations des magistrats instructeurs (commission rogatoire, mandat). Les OPJ ont plénitude de pouvoirs et peuvent, dans certains cas, agir sans autorisation du parquet.

L'article 5 du décret de 2018 prévoit que les OPJ sont aussi destinataires des données à caractère personnel au même titre que les agents habilités de la société gestionnaire de la plateforme dont le traitement est autorisé. Même si les dispositions de l'article 5 ne mentionnent pas expressément d'autres autorités publiques habilitées – en dehors des OPJ – comme potentiels destinataires, il n'en demeure pas moins que la liste n'est pas fermée. C'est ce qui ressort de l'article 4 de la LPDCP qui définit le destinataire d'un traitement des données à caractère personnel comme étant *« toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données. Toutefois, les autorités publiques légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, peuvent demander au responsable du traitement de leur communiquer des données à caractère personnel »*[94].

En outre, les informations collectées peuvent aussi être utiles dans le cadre d'un contentieux civil ou commerciale. Le juge civil peut ainsi demander la communication de tout renseignement lui permettant d'apprécier la situation d'un débiteur en surendettement. Le président du tribunal de commerce peut aussi obtenir des renseignements de nature à lui donner des informations sur la situation économique et financière d'un débiteur. Dans le cadre d'une procédure de règlement préventif, de redressement ou de liquidation, il peut s'agir également d'une demande de l'administrateur et/ou du mandataire judiciaire[95].

[94] Article 4, paragraphe 5, de la LPDCP.
[95] Voir l'Acte Uniforme portant organisation des Procédures Collectives d'Apurement du Passif (AUPCAP) révisé en 2015.

Au-delà des interrogations qui peuvent émerger relativement au droit d'accès des OPJ aux données personnelles des clients des grands facturiers – personnes physique et morale – notamment en ce qui concerne le contrôle du respect de la vie privée et du droit processuel, que nous n'abordons pas dans le cadre de cette analyse, il faut surtout s'interroger sur l'encadrement de l'usage qui peut être fait de ces données.

2. L'encadrement insuffisant du traitement des données

En pratique, la finalité du traitement – pour lequel l'OPJ est désigné comme destinataire ou se voit octroyé un droit d'accès – doit être précisée dans l'habilitation donnée par l'autorisation du président du tribunal, la réquisition du procureur de la République ou l'ordonnance du juge d'instruction. L'OPJ ne peut donc aller au-delà du cadre fixé par l'acte l'habilitant à accéder aux données communiquées au BIC par les grands facturiers.

Si l'acte d'habilitation peut définir le but et le cadre de l'autorisation donnée – en d'autres termes la finalité du traitement autorisé – à l'OPJ, peut-il à lui seul définir tous les contours d'une entreprise aussi sensible qui relèverait en principe du pouvoir du législateur. Il faudrait donc une intervention de ce dernier pour définir de manière plus précise le cadre de traitement des données pour éviter des atteintes disproportionnées aux droits et libertés fondamentaux des personnes concernées.

Il convient dès lors que ces domaines soient régis par des règles spécifiques relatives à la protection des personnes physiques à l'égard du traitement des données personnelles par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces[96]. *A contrario,* la LPDCP s'appliquerait alors aux finalités de traitement ne relevant de cette réglementation spécifique.

Les autorités compétentes en question peuvent comprendre non seulement les autorités publiques telles que les autorités judiciaires, la police ou d'autres autorités répressives mais

[96] V. en ce sens les dispositions de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

aussi tout autre organisme ou entité à qui est confié l'exercice de l'autorité publique et des prérogatives de puissance publique. Sont aussi mis à contribution certaines entités telles que les établissements financiers qui doivent conserver, à des fins de détection ou de poursuites d'infractions pénales ou d'enquêtes en la matière, certaines données à caractère personnel qu'ils traitent et qu'ils ne transmettent aux autorités compétentes que dans des cas spécifiques.

Si le traitement autorisé est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, notamment parce qu'il porte sur des données sensibles, le responsable de traitement doit effectuer une analyse d'impact relative à la protection des données à caractère personnel (AIPDCP). Dans le cas où les données collectées auprès du BIC doivent faire l'objet d'un traitement par un sous-traitant, cette opération doit être régi par un contrat ou un autre acte juridique, qui lie le sous-traitant à l'égard du responsable de traitement, définissant entre autres l'objet et la durée du traitement, la nature et la finalité du traitement, les mesures techniques et organisationnelles destinées à garantir la sécurité du traitement, et prévoyant que le sous-traitant ne peut agir que sur instruction du responsable de traitement.

Rappelons qu'au titre de l'article 27 de la LPDCP, aucune décision de justice impliquant l'appréciation du comportement d'une personne ne peut avoir pour seul fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de la personnalité de cette personne. De même, aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à prévoir ou à évaluer certains aspects personnels relatifs à la personne concernée.

Quoiqu'il en soit, toute personne physique a le droit de s'opposer – pour des motifs légitimes – à ce que des données personnelles la concernant fassent l'objet d'un traitement. Toutefois, le droit d'opposition ne peut être exercé lorsque le traitement répond à une obligation légale ou lorsque son application est expressément écartée par l'acte autorisant ledit traitement.

Conclusion

La mise en place d'un système d'échange d'informations sur le crédit : la cause est noble, l'objectif est ambitieux. La participation des grands facturiers à cette « aventure » l'est encore plus d'autant qu'ils détiennent et agrègent d'importantes quantités de données exploitables dans le cadre de procédure d'octroi de crédit. Quoi de mieux que d'analyser le risque de solvabilité

d’un client en tenant compte de ses antécédents de crédits et de paiement, pour ne pas dire de son « comportement ».

Si le client peut bénéficier d’une meilleure accessibilité au crédit avec une tarification basée sur l’individualisation des risques pouvant induire une baisse du coût du crédit et des garanties ; il n’en ressort que grandit. Gare alors aux mauvais payeurs ! Quant aux utilisateurs des données sur le crédit, ils peuvent alors mieux évaluer et gérer les risques de solvabilités et de surendettement de leurs emprunteurs. De surcroît ils bénéficient d’une réduction sensible de l’asymétrie d’information permettant ainsi d’améliorer leur portefeuille. Et tout cela rejaillit sur l’économie.

Cependant, il ne faut pas non plus trop vite se réjouir. Certes le législateur a pris soin – à travers la loi uniforme sur les BIC, la loi autorisant l’intégration des grands facturiers à la plateforme de partage d’informations et enfin la LPDCP – de circonscrire les risques d’atteintes aux droits et libertés fondamentaux qui peuvent découler du traitement des données à caractère personnel. Toutefois, le « diable se cache dans les détails ». Il faut donc suivre de près les conditions de collectes et d’exploitation des données personnelles par le BIC, sans oublier l’usage qu’en feront les tiers autorisés – à l’instar des OPJ et autres autorités publiques habilitées – pour ne pas verser dans la dérive. C’est la mission à laquelle est notamment conviée l’IPDCP afin d’éviter, au maximum, les abus dans le traitement des données à caractère personnel des clients des grands facturiers./.