DIGITAL FINANCIAL SERVICES (DFS) WORKING GROUP

CONSUMER EMPOWERMENT AND MARKET CONDUCT (CEMC) WORKING GROUP

NOTE SUR LA DIRECTIVE RELATIVE LA CONFIDENTIALITÉ DES DONNÉES POUR LES SERVICES FINANCIERS NUMÉRIQUES

Note sur la directive n° 43
Février 2021

NOTE SUR LA DIRECTIVE

SOMMAIRE

REMERCIEMENTS

Cette note sur la directive est un produit commun des membres du groupe de travail sur les services financiers numériques (DFSWG) et du groupe de travail sur l'autonomisation des consommateurs et les pratiques de marché (CEMCWG).

Auteurs et contributeurs :
Les membres du DFSWG qui ont contribué à la rédaction de la note sur la directive sont :

Alejandro Medina (SBS Pérou), Rushika Kumaraswamy (Banque centrale du Sri Lanka), Mohamed Salem Ould Mamoun (Banque centrale de Mauritanie), Rasool Roohy (Da Afghanistan Bank), Stephen Ambore (Banque centrale du Nigeria), Anil Paul (Banque de Papouasie-Nouvelle-Guinée), Khaled Barmawi (Banque centrale de Jordanie), Rania Elshama (Banque centrale d'Égypte) et Pauline Moustache (Banque centrale des Seychelles).

Au sein de l'unité de gestion de l'AIF, le projet d'élaboration de la note sur la directive a été dirigé par Ali Ghiyazuddin Mohammad (Senior Policy Manager, Digital Financial Services) avec le soutien de Eliki Boletawa (Head of Policy Programs and Regional Initiatives). Nous tenons à remercier la consultante Ros Grady pour son soutien dans la recherche et l'élaboration de la note sur la directive.

Nous tenons à remercier les institutions membres de l'AIF, les partenaires et les donateurs qui ont généreusement contribuél'élaboration de cette publication.

Concept de confidentialité des données. (Photo par metamorworks/Shutterstock)

RÉSUMÉ ANALYTIQUE

Cette note sur la directive a été élaborée par le groupe de travail de l'AIF sur les services financiers numériques (DFSWG) et le groupe de travail sur l'autonomisation des consommateurs et la conduite du marché (CEMCWG).

Le marché des services financiers numériques (SFN) est en train de se transformer à un rythme exponentiel, alimenté par les développements en matière de traitement des données rendus possibles par la FinTech. Ces changements ont donné lieu à des innovations dans la conception et la prestation des services financiers numériques, qui contribuent à leur tour à la réalisation des objectifs d'inclusion financière et de ses avantages qui sont la réduction de la pauvreté et la croissance économique.

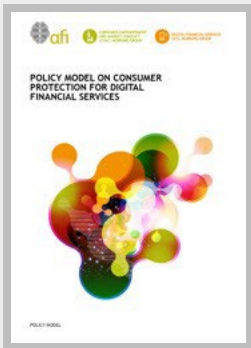
Cependant, ces innovations soulèvent des questions sérieuses en matière de confidentialité des données des personnes concernées - confidentialité des données pour les services financiers numériques (DP4DFS). La capacité financière et les défis technologiques probables des personnes concernées dans un contexte d'inclusion financière sont particulièrement préoccupants.

L'objectif de la note sur la directive est de fournir des orientations non contraignantes pour un cadre réglementaire et politique complet, fondé sur le risque et proportionnés pour le DP4DFS. L'accent est mis sur les questions de confidentialité applicables aux SFN, plutôt qu'aux services financiers traditionnels. En effet, la plupart des questions relatives à la confidentialité se posent dans le contexte des SFN. Cependant, la note sur la directive peut également être pertinente de manière plus générale.

La note sur la directive s'inspire des produits de connaissance antérieurs de l'AIF, qui couvrent les questions de confidentialité et de protection des données. Voir en particulier les principes directeurs relatifs à la confidentialité et à la protection des données dans le modèle stratégique de l'AIF sur la protection du consommateur des services financiers numériques (2020) (principe 2.1) et dans le cadre de politique de l'AIF pour un crédit numérique responsable (2020) (principe 6). D'autres produits de connaissance pertinents de l' AIF sont mentionnés ailleurs dans la note sur la directive et sont tous énumérés à l'annexe 5.

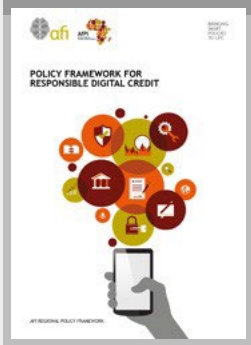
Un large éventail d'orientations politiques et réglementaires applicables au DP4DFS a été synthétisé pour les besoins de la note sur la directive. Outre les produits de connaissance de l'AIF mentionnés ci-dessus, les autres sources prises en compte comprennent un large éventail de cadres réglementaires nationaux et de normes, lignes directrices et bonnes pratiques internationales. Des recherches connexes
et commentaires recueillis auprès des organisations internationales, universitaires et des experts ont également été pris en compte.

LECTURE COMPLÉMENTAIRE



Modèle stratégique de l'AIF sur la protection des consommateurs des services financiers numériques (2020) (Principe 2. 1)

> Voir ici



Cadre stratégique de l'AIF pour un crédit numérique responsable (2020) (Principe 6)

> Voir ici

Ce travail a abouti à l'élaboration des principes directeurs suivants. Les recommandations clés pour chaque principe directeur figurent plus loin dans la présente note sur la directive.

PILIER 1 : CADRE RÉGLEMENTAIRE ET POLITIQUE RÉGLEMENTAIRE DE DP4DFS

1.1 Principe directeur : mettre en place des mécanismes de gouvernance et de consultation

1.2 Principe directeur : Évaluer le cadre juridique et réglementaire actuel des SFN et le marché

1.3 Principe directeur : établir des principes politiques et réglementaires généraux

1.4 Principe directeur : Développer le cadre juridique du DP4DFS

PILIER 2 : OBLIGATIONS DU CONTRÔLEUR ET DU PROCESSEUR DE DONNÉES

2.1 Principe directeur : Exiger des mecanismes efficaces en matière de gouvernance interne du DP4DFS

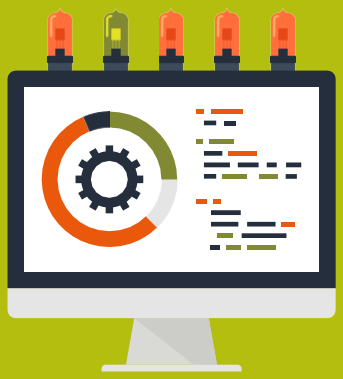
2.2 Principe directeur : élaborer des principes généraux de traitement des données

2.3 Principe directeur : Créer un modèle de consentement éclairé et efficace

2.4 Principe directeur : Exiger la présence d'un responsable de la protection des données le cas échéant

SIX PILIERS DE PRINCIPES DIRECTEURS POUR UN CADRE DP4DFS

PILIER 1 :
POLITIQUE RÉGLEMENTAIRE DU DP4DFS CADRE



PILIER 2 :
CONTRÔLEUR ET PROCESSEUR DES DONNÉES OBLIGATIONS

PILIER 3 :
DROITS DES PERSONNES CONCERNÉES

PILIER 4 :
SENSIBILISATION DES CONSOMMATEURS ET RECOURS

PILIER 5 :
SUPERVISION ET APPLICATION

PILIER 6 :
DP4DFS DANS LES URGENCES INTERNATIONALES ET NATIONALES

Une page intitulée " Approche minimaliste du DP4DFS pour les régulateurs financiers " a également été insérée dans la présente note sur la directive. Cette proposition contient des suggestions relatives aux mesures minimales que les régulateurs financiers peuvent prendre dans la période intérimaire avant la mise en place d'une loi globale sur la protection des données.

En résumé, le corps principal de la présente note sur la directive est organisé comme suit :

> Champ d'application, concepts clés et définitions

> Tendances émergentes dans les cadres réglementaires et politiques de DP4DFS

> Principes directeurs pour le cadre réglementaire et politique global de DP4DFS

> Approche minimaliste de DP4DFS pour les régulateurs financiers

CHAMP D'APPLICATION, CONCEPTS CLÉS ET DÉFINITIONS

Les principes directeurs couvrent les questions de " confidentialité des données " concernant les informations personnelles, mais pas les questions spécifiques de " protection des données ".

Ces termes sont définis comme suit aux fins de la présente note sur la directive : la " confidentialité des données " est considérée comme l'utilisation et la gestion appropriées des données à caractère personnel en tenant compte du droit à la vie privée et à la " protection des données " comme la sécurisation des données contre une utilisation non autorisée. Il s'agit des définitions utilisées dans le modèle stratégique de l'AIF sur la protection du consommateur des services financiers numériques (2020). Sur cette base, des questions telles que la cyber-fraude, les systèmes de sécurité et les règles de localisation des données sont considérées comme relevant du domaine de la " protection des données ". Certaines questions relevant de la zone " grise " qui chevauche la confidentialité et la protection des données ont néanmoins été couvertes (telles que l'usurpation d'identité et l'abus de confiance).

Pour être complet, il convient également de noter que le droit à la confidentialité est généralement considéré comme " le droit d'être laissé seul ", bien que sous réserve de certaines limites. [1] Toutefois, il n'est pas du ressort de la présente Note sur la directive de discuter de la nature du droit à la " confidentialité " ou de l'existence éventuelle d'un droit ou d'une autre forme de droit à la confidentialité dans une juridiction. [2]

Les principes directeurs s'appliquent aux produits de SFN de détail et aux modèles d'affaires connexes courants dans les économies émergentes (aujourd'hui et à l'avenir). Ces produits peuvent comprendre, par exemple, les produits d'épargne, le crédit numérique, les prêts P2P, la monnaie électronique, les transferts de fonds, la micro-assurance, le financement participatif et les produits d'investissement, ainsi que les produits et services plus innovants tels que l'agrégation de comptes et d'autres services bancaires ouverts.

Les principes directeurs abordent également d'autres questions essentielles telles que :

> **L'inclusion financière :** Les principes directeurs partent du principe qu'ils doivent être pertinents pour les consommateurs dans les économies ayant des objectifs ambitieux en matière d'inclusion financière.

1 Sameul D Warren et Louis D. Brandeis. Le droit à la confidentialité. Harvard Law Review Vol. 4, No. 5 (15 décembre 1890), pp. 193-220

2 Pour une discussion de ces questions dans le contexte de l'Inde, voir l'importante décision de la Cour suprême de l'Inde dans l'affaire Justice K.S. Puttaswamy vs. Union of India (2017) 10 SCC 1 qui, en résumé, a estimé que la vie privée était un droit protégé par la Constitution de l'Inde.

- **La FinTech :** Les principes directeurs ont été élaborés en tenant compte des développements de la FinTech qui sont pertinents pour les SFN, y compris les fournisseurs, les modèles d'affaires, les systèmes de traitement et les applications nouveaux et innovants. Les principes directeurs se veulent également " neutres sur le plan technologique ", en ce sens qu'ils doivent être pertinents quelle que soit la technologie utilisée pour concevoir, commercialiser ou fournir des SFN.
- **Groupes vulnérables :** Les questions relatives à la confidentialité des données concernant les groupes vulnérables sont prises en compte dans les principes directeurs. Ces groupes comprennent, par exemple, les femmes, les jeunes, les personnes âgées, les personnes handicapées et les personnes déplacées.
- **Urgences et DP4DFS :** Il y a des avantages incontestables dans l'utilisation généralisée des SFN pour répondre aux urgences mondiales et nationales (telles que le COVID-19, la crise Ebola, la crise syrienne et les catastrophes naturelles). Cependant, il existe également des défis à relever en matière de confidentialité des données. C'est dans ce contexte qu'un pilier spécifique a été inclus dans le programme DP4DFS en cas de situations d'urgence mondiales et nationales.

Les termes clés utilisés dans la présente note sur la directive (y compris les principes directeurs) ont la signification indiquée à l'annexe 3. Ces significations ont été élaborées en tenant compte des termes les plus couramment utilisés et des définitions connexes figurant dans les cadres réglementaires, la documentation et les commentaires. Pour plus de commodité, les définitions les plus importantes sont présentées au tableau 1 ci-dessous.

Il est toutefois souligné que différentes approches peuvent être adoptées pour les termes et définitions pertinents, et que les définitions proposées n'ont pas de caractère obligatoire.

ENCADRÉ 1 : DÉFINITIONS DES " DONNÉES PERSONNELLES " OU SIMILAIRES DANS LES LOIS SUR LA CONFIDENTIALITÉ ET LA PROTECTION DES DONNÉES

Règlement général sur la protection des données de l'UE : " données à caractère personnel " signifie toute information concernant une personne physique identifiée ou identifiable (" personne concernée ") ; une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par le biais d'un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant électronique ou à l'aide d' un ou plusieurs éléments spécifiques propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne physique ; (article 4).

Pour d'autres exemples de définitions de " données à caractère personnel " ou d'un terme équivalent, voir :

- Kenya's Data Protection Act 2019 (section 2),
- Malaysia's Data Protection Act 2010 (section 4),
- Philippines Data Privacy Act 2012 (section 3).

Voir également le projet de loi de l'Inde sur la protection des données personnelles 2019 (section 3 (28)), qui inclut spécifiquement toute information tirée de données personnelles à des fins de profilage.

TABLEAU 1 : CONCEPTS CLÉS ET

CONCEPT	DÉFINITIONS
PERSONNE CONCERNÉE	Une personne dont les données personnelles sont ou peuvent être traitées.
DONNÉES PERSONNELLES	Les informations ou opinions relatives à une personne identifiée ou identifiable, qu'elles soient vraies ou non, conservées sous une forme matérielle ou non, et automatisées ou non.
CONTRÔLEUR	Une personne physique ou morale ou une autorité publique qui, seule ou conjointement avec d'autres, détermine la finalité ou la méthode de traitement des données à caractère personnel.
PROCESSEUR	Une personne physique ou morale ou une autorité publique qui traite des données à caractère personnel pour le compte du contrôleur.
TRAITEMENT	Les opérations effectuées en relation avec des données à caractère personnel, manuellement ou par des procédés automatisés, y compris la collecte, l'utilisation, la divulgation, le stockage, l'enregistrement, l'effacement ou autre, ainsi que les termes " traite ", " traité " et autres termes similaires ayant un sens analogue, mais excluant tout traitement : - exigé pour des activités déterminées (telles qu'une fonction judiciaire, l'application d'une réclamation, la sécurité nationale ou une préoccupation purement domestique ou ménagère) ; ou - entrepris dans un but requis ou autorisé par la loi

HISTORIQUE ET CONTEXTE

NOUVELLES FORMES DE TRAITEMENT DES DONNÉES, FINTECHS ET DP4DFS

Le phénomène du " Big Data " et les technologies connexes alimentent les innovations et les opportunités des SFN, y compris dans les pays en développement.

Aux fins de la présente note sur la directive, les " Big Data " peuvent être considérées comme des ensembles de données massives et complexes qui se caractérisent par d'énormes volumes de données personnelles traditionnelles et alternatives, structurées ou non, d'une grande variété, qui peuvent être traitées à grande vitesse pour les besoins des SFN.

Les catégories de données qui peuvent être traitées comprennent : les formes traditionnelles de données relatives aux clients, aux comptes et aux transactions, ainsi que les formes alternatives de données telles que les données des médias sociaux, les données dérivées de téléphones mobiles et les données accessibles au public. La connectivité accrue à l'internet et l'adoption des téléphones intelligents peuvent également constituer une riche source de données à traiter et accroître la disponibilité des SFN. [3] Les technologies pertinentes comprennent les algorithmes, qui facilitent l'apprentissage automatique, l'informatique en nuage, la technologie blockchain, les outils d'identification biométrique et les systèmes d'identification numérique. [4] Enfin, ces nouvelles formes de traitement des données peuvent être utilisées :

- Pour ré-identifier une personne en comparant des données anonymes (données dépersonnalisées) avec des données accessibles au public, des informations déjà connues ou d'autres données ; et
- Déduire des données sensibles à partir de données non sensibles (par exemple, utiliser le nom d'une personne pour déduire sa race, sa religion ou son genre). [5]

Les entités de la FinTech qui s'appuient sur ces développements sont différentes des fournisseurs financiers traditionnels. Il n'est plus question que les données soient traitées à des fins de SFN par des entités hautement réglementées, telles que les banques traditionnelles, les assureurs ou les entités de valeurs mobilières, qui sont soumises à des règles de conduite sur le marché ainsi qu'à des règles prudentielles. Un éventail toujours plus large d'entités et de modèles d'affaires de la FinTech nouveaux, innovants, agiles et souvent sans frontières, traitent désormais les données, soit en tant que fournisseur financiers proprement dit, soit en tant que fournisseur de services tiers (par exemple à des fins d'analyse de données).

AVANTAGES DES NOUVELLES FORMES DE TRAITEMENT DES DONNÉES

Les développements en matière de traitement des données décrits ci-dessus peuvent apporter des avantages significatifs aux personnes concernées par les SFN. En voici quelques exemples :

- **Choix des produits :** Les consommateurs doivent avoir un meilleur accès à une large gamme de services financiers, y compris les produits de nano crédit pour ceux qui n'ont pas d'historique de crédit formel, les produits de prêt de pair à pair, les produits de paiement tels que la monnaie électronique, les produits de micro-assurance, les comptes d'épargne à faible coût et le financement participatif.
  En outre, les systèmes bancaires ouverts tels que l'agrégation de comptes peuvent permettre aux personnes concernées de mieux contrôler leurs données et de bénéficier d'avantages connexes dans le choix et la tarification des produits, ainsi que dans la gestion de leurs affaires financières.
- **Produits personnalisés :** Les grandes quantités de données personnelles dont disposent les prestataires de SFN peuvent être utilisées pour concevoir et proposer des produits adaptés aux besoins et au profil de risque des personnes concernées et dont le prix peut être fixé en conséquence.
- **Identification plus facile :** Les systèmes d'identification numérique développés à partir de nouvelles sources de données, telles que les données biométriques et les technologies de traitement améliorées, peuvent faciliter l'accès sécurisé aux SFN.
- **Aide d'urgence :** L'identification des bénéficiaires ayant droit à une aide d'urgence (comme les transferts d'argent de gouvernement à personne (G2P) et les crédits subventionnés) peut être facilitée.

Les fournisseurs des SFN sont susceptibles d'être avantagés par ces progrès en matière de traitement des données. Ils peuvent améliorer leur capacité à concevoir, commercialiser et tarifer des produits et services financiers ciblés et à gérer les risques commerciaux liés aux données (tels que les risques de crédit, l'évaluation des risques liés l'assurance, les plaintes et les réclamations). Certains fournisseurs peuvent également chercher à vendre des droits d'accès à des tiers. La concrétisation de ces avantages potentiels serait, bien entendu, soumise aux lois applicables.

Les progrès en matière de traitement des données présentent également une série d'avantages potentiels au niveau national. En résumé, dans le contexte des SFN, cela pourrait inclure l'aide à la réalisation des objectifs d'inclusion financière, pour le développement et la gestion des systèmes d'identification nationaux, pour la promotion de la concurrence et de l'innovation dans le secteur financier ; et pour la gestion des risques dans ce secteur.

---

3 GSMA : Rapport sur l'état de la connectivité internet mobile (2020)

4 Banque mondiale : Protection des consommateurs des services financiers et nouvelles formes de traitement des données au-delà des rapports de crédit (2018)

5 UIT : Initiative mondiale pour l'inclusion financière (FIGI) Groupe de travail sur l'infrastructure de sécurité et la confiance, Big data, machine learning, consumer protection and privacy (2018).

LES RISQUES LIÉS AUX NOUVELLES FORMES DE TRAITEMENT DES DONNÉES

ENCADRÉ 2 : MODÈLE STRATEGIQUE DE L'AIF SUR LA PROTECTION DU CONSOMMATEUR DES SERVICES FINANCIERS NUMÉRIQUES (2020)

" À l'ère de la finance numérique, les données sont au cœur des SFN.

…

Dans ce contexte, l'utilisation, la gestion et le stockage inappropriés des données des clients, associés à une divulgation et une transparence insuffisantes, risquent d'exclure les segments vulnérables des services financiers, de susciter un manque de confiance dans les SFN et de compromettre les progrès de l'inclusion financière " (Principe directeur 2.1 : Sauvegarde de la confidentialité et protection des données à caractère personnel)

Ces progrès présentent un large éventail de risques pour les personnes concernées par les SFN, en particulier lorsqu'il n'existe pas de cadre réglementaire en matière de confidentialité.
À un niveau élevé, ces risques peuvent avoir des conséquences néfastes telles que le refus d'un SFN ou d'une prestation publique, une perte financière, une atteinte à la réputation sociale ou professionnelle, ou un traitement injuste tel que la discrimination.
Plus précisément, ils comportent les risques importants suivants :

- **Les personnes concernées peuvent n'avoir aucun contrôle ou un contrôle limité sur leurs données à caractère personnel** : Aucune information ou des informations limitées peuvent être fournies ou disponibles sur les types de données traitées, par qui, comment et où. Même lorsque l'information est disponible, le consentement peut ne pas être donné librement ou en connaissance de cause.
- **Les données sensibles peuvent être compromises par une collecte, une utilisation ou une divulgation non autorisée :** la confidentialité des données qui peuvent être considérées comme particulièrement sensibles suscite de vives inquiétudes. Par exemple, des informations sur les données biométriques d'une personne, son identifiant officiel, ses croyances ou son affiliation religieuse ou politique, sa race, son appartenance ethnique, sa caste, sa santé ou son identité sexuelle. En outre, comme indiqué ci-dessus, des données non sensibles peuvent être utilisées pour détecter des données sensibles. [6]
- **Des données à caractère personnel incorrectes, trompeuses, incomplètes ou obsolètes peuvent être traitées :** Cela peut entraîner un traitement injuste, tel que le refus injustifié de facilité de crédit, le harcèlement du débiteur, le refus injuste d'une demande d'assurance ou le refus de prestations gouvernementales, ainsi que des pertes financières et une atteinte à la réputation.
- **La prise de décision automatisée, y compris le profilage, peut entraîner des décisions injustes :** Décisions concernant un intéressé, qui sont effectuées sur la base d'un traitement automatisé et d'un profilage sans intervention humaine, peuvent donner lieu à des discriminations et à des préjugés injustes. [7] En outre, les personnes concernées ne sont pas susceptibles de comprendre les algorithmes complexes et en constante évolution ainsi que les autres technologies utilisées dans de tels processus. Ces technologies sont d'autant plus complexes qu'elles peuvent être considérées comme confidentielles sur le plan commercial et sont susceptibles d'être protégées par des droits de propriété intellectuelle et des obligations.
- **L' identification de la fraude et l'utilisation abusive des identifiants numériques peut se produire :** Ces événements peuvent entraîner des pertes financières et porter atteinte à la réputation des personnes concernées. Il faut également tenir compte de la complexité supplémentaire qui fait que les données d'identité biométriques ne peuvent pas être corrigées, contrairement à d'autres identifiants de sécurité compromis (comme un mot de passe ou un numéro d'identification personnel). Voir plus loin la section intitulée " Identités numériques et risques liés à la fraude d'identité, à l'utilisation abusive et l'accès inapproprié ".
- **Les droits de recours peuvent être limités :** En l'absence d'un cadre réglementaire relatif à la confidentialité, la personne concernée est susceptible de ne pas disposer de recours en cas d'utilisation abusive de leurs données. Il peut s'agir, par exemple, d'un recours qui exige du contrôleur des données qu'il cesse ou modifie son traitement des données à caractère personnel, qu'il corrige ou supprime les enregistrements qu'il possède ou qu'il verse une indemnisation.
- **Les systèmes et procédures utilisés par les contrôleurs des données ne garantissent pas la confidentialité :** Il peut également y avoir un risque que les contrôleurs des données n'aient pas mis en place des systèmes et des procédures globaux qui reflètent de manière proactive les considérations relatives à la confidentialité dans la conception et la commercialisation des SFN.
  En d'autres termes, les questions de confidentialité ne sont pas au centre des préoccupations. Cela pourrait être plus probable avec les nouvelles entités de la FinTech innovantes, comparées aux fournisseurs des SFN plus traditionnels.
- **Les risques d'atteinte à la vie privée liés aux intermédiaires tels que les courtiers en données qui font le commerce des Big Data et des analyses connexes font l'objet d'un examen de plus en plus minutieux : Par exemple,** l'Information Commissioner's Office du Royaume-Uni a récemment enquêté sur trois agences de référence en matière de crédit qui opéraient également en tant que courtiers en données. [8]

Les prestataires de SFN peuvent également être confrontés à de nouveaux défis en matière de traitement des données, même s'ils n'ont pas l'obligation de se conformer à un cadre réglementaire relatif à la confidentialité des données.

6 Projet de loi de l'Inde sur la protection des données (2019) (section 3 (36))

7 G20 : Principes de haut niveau pour l'inclusion financière numérique (2016) Le principe 5 fait référence à une action clé pour soutenir les services financiers numériques : " Exiger que les données ne soient pas utilisées de manière injustement discriminatoire pour les services financiers numériques (par exemple, pour discriminer les femmes par rapport à l'accès au crédit ou à l'assurance) ".

8 https://ico.org.uk/about-the-ico/news-and-events/news-and- blogs/2020/10/ico-takes-enforcement-action-against-experian-after- data-broking-investigation/

Il s'agit notamment des complexités et des coûts liés à la mise à jour de ces innovations et de l'adaptation des systèmes et processus existants ; les conséquences commerciales du traitement de données inexactes ou non pertinentes ; la nécessité de recourir à des méthodes plus complexes de collecte et de vérification des données ; les risques et les coûts liés à une dépendance accrue à l'égard de fournisseurs externes de données et d'analyses de données, et la nécessité de sensibiliser les clients à la nécessité de protéger leurs données personnelles, leurs documents d'identité officiels et leurs justificatifs de sécurité.

Les régulateurs financiers et les décideurs politiques sont également confrontés à des défis dans le contexte du PD4DFS. D'une manière générale, il s'agit du risque que les consommateurs ne fassent pas confiance à l'utilisation des SFN à cause des leurs préoccupations concernant la confidentialité des données, avec des implications sur l'inclusion financière. Des défis plus spécifiques peuvent être la nécessité pour les régulateurs et les décideurs politiques :

- De comprendre les modèles d'affaires, les partenariats, les activités et les techniques de traitement des données des nouveaux agiles, et innovants fournisseurs de la FinTech ;
- D'acquérir les capacités et les ressources organisationnelles et technologiques appropriées ;
- D'identifier les lacunes et les chevauchements dans les règles sectorielles du DP4DFS (par exemple, dans le secteur bancaire, les paiements, la monnaie électronique ou les lois générales sur le droit de la consommation) ; et
- De mettre en place des mécanismes de consultation et de coordination avec d'autres agences gouvernementales, le secteur privé (y compris les fournisseurs traditionnels et les SFN de la FinTech) et les parties prenantes de la société civile (telles que les groupes de consommateurs).

DP4DFS ET GROUPES VULNÉRABLES

La vulnérabilité doit être prise en compte dans l'élaboration d'un cadre de politique réglementaire pour le DP4DFS. Comme indiqué ci-dessus, le terme " vulnérabilité " couvre les personnes concernées susceptibles d'avoir des besoins particuliers, notamment les femmes, la jeunesse, les personnes âgées, les personnes handicapées et les personnes déplacées. Les questions particulièrement préoccupantes concernent :

- **Les femmes :** Les normes culturelles de certaines sociétés peuvent porter à croire que les femmes sont particulièrement préoccupées par la confidentialité de leurs données de SFN, y compris en ce qui concerne d'autres membres du ménage (tels que leurs partenaires) et de leurs communautés.
- **La jeunesse :** La jeunesse est susceptibles d'avoir grandi en étant familiarisée avec les technologies de la FinTech et les SFN, même s'il n'est pas certain qu'elle comprenne tous les risques liés à la confidentialité.
- **Les personnes âgées :** Ce groupe est particulièrement susceptible d' être limité en matière de capacités financières et technologiques, ce qui peut à son tour affecter de manière disproportionnée leur capacité à comprendre et à exercer leurs droits en matière de données privées.
- **Les personnes handicapées :** Il existe un large éventail de handicaps qui peuvent constituer des obstacles pour la lecture ou la compréhension des divulgations des données confidentielles et des formulaires de consentement. Il s'agit notamment de handicaps visuels et intellectuels, ainsi que de troubles du langage. Ce dernier point est particulièrement probable dans les pays qui ont plusieurs langues officielles et dialectes locaux.
- **Personnes déplacées :** Les questions relatives à la confidentialité des données pour ce groupe particulièrement vulnérable peuvent inclure des préoccupations concernant l'accès à leurs données personnelles, y compris les dossiers biométriques créés par les organisations humanitaires telles que le UNHCR (par exemple, pour faciliter la fourniture d'une assistance en espèces par le biais des SFN). Cette question est largement débattue, y compris par le UNHCR, qui dispose de sa propre politique de protection des données.

Les facteurs susmentionnés montrent qu'il est nécessaire de tenir compte de la diversité des utilisateurs des SFN lors de l'élaboration d'un cadre réglementaire de politique de DP4DFS, et de développer des programmes d'alphabétisation ciblés.

ENCADRÉ 3 : DISCOURS DU DIRECTEUR EXÉCUTIF DE L' AIF, DR. ALFRED HANNIG (18 NOVEMBRE 2020)

La littératie numérique joue un rôle important dans l'apprentissage des utilisateurs à naviguer dans ces services. Ceci implique que les régulateurs doivent se concentrer sur et proportionner les méthodes l'éducation financière des clients, en particulier ceux qui ne sont pas familiarisés avec les risques. Par exemple, les personnes âgées ne sont pas habituées aux SFN et aux services bancaires en ligne et, en raison de leur manque de connaissances, elles risquent d'être exclues du système. Les régulateurs doivent donc tenir compte de la diversité des groupes et des risques auxquels ils sont confrontés ".

Les clients des services financiers à faibles revenus ont montré qu'ils se soucient de la confidentialité des données. Il existe plusieurs enquêtes et études pour étayer ce point de vue, bien que certaines indiquent que les consommateurs peuvent être prêts à partager leurs données avec les sociétés financières en échange d'avantages supplémentaires. [9] Plus précisément, des études récentes menées par le CGAP au Kenya et en Inde ont révélé (en résumé) que la plupart des clients pauvres participant à ces expériences :

- Ils accordent de l'importance à la confidentialité des données et sont prêts à payer pour cela des frais ou un taux d'évaluation plus élevés ;
- Sont prêts à consacrer du temps à l'obtention d'un prêt offrant une protection de la vie privée ; et/ou
- Ne sont pas disposés à partager des données personnelles avec des tiers. [10]

DP4DFS ET INCLUSION FINANCIÈRE

Existe-t-il un compromis entre l'inclusion financière et les règles relatives à la confidentialité des données ? On peut, par exemple, considérer que les règles en matière de confidentialité des données entravent les innovations des SFN, telles que le crédit numérique et les produits de micro-assurance, ou imposent des restrictions aux services bancaires ouverts ou à l'utilisation de certaines technologies, telles que les services d'informatique en nuage [11]. Inversement on peut penser que la confidentialité des données et l'inclusion financière sont des objectifs compatibles, étant donné que les droits en matière de confidentialité des données sont susceptibles d' instaurer la confiance dans l'utilisation des SFN. En outre, un régime proportionné de confidentialité de données peut servir de base à des innovations telles que les systèmes bancaires ouverts et la numérisation de l'économie en général.[12] Les pratiques non réglementées en matière de données peuvent également aller à l'encontre des objectifs fondamentaux de l'inclusion financière (voir encadré 4).

ENCADRÉ 4 : DR KATHERINE KEMP, MAÎTRE DE CONFÉRENCES, UNIVERSITÉ DE NEW SOUTH WALES : "BIG DATA, FINANCIAL INCLUSION AND PRIVACY FOR THE POOR" FORUM DE LA FINANCE RESPONSABLE (2017)

" La protection des données des consommateurs doit-elle être reléguée au second plan face au besoins financiers plus pressants d'inclusion financière ?

…

À cet égard, il est important de rappeler notre point de départ : l'inclusion financière n'est pas une fin en soi, mais un moyen d'atteindre d'autres objectifs, notamment de permettre aux pauvres et aux personnes vivant dans des zones reculées de subvenir aux besoins de leur famille, prospérer, maîtriser leur destin financier et éprouver un sentiment de fierté et d'appartenance à leur communauté. Les préjudices causés par les données non réglementées vont à l'encontre de chacun de ces objectifs ".

DP4DFS, COVID-19 ET AUTRES URGENCES

Le COVID-19 et d'autres urgences mondiales et nationales ont mis en évidence la nécessité de prendre en compte les questions relatives aux DP4DFS. L'importance fondamentale des services financiers numériques pour préserver le fonctionnement du système financier, renforcer la sécurité et pour la réduction de la pauvreté en cas de situation d'urgence mondiale telle que le COVID-19 a été bien reconnue, notamment dans le cadre politique de l'AIF pour tirer parti des services financiers numériques dans la réponse aux situations d'urgence mondiale - cas du COVID-19 (2020). Les raisons comprennent notamment la capacité des SFN pour faciliter les transferts de fonds G2P à faible coût, les crédits d'urgence et les envois de fonds locaux et internationaux. Les SFN permettent également de gérer des comptes et d'effectuer des paiements pour des biens et des services à distance et sans contact.

Toutefois, la multiplication de l'utilisation des SFN lors de crises telles que le COVID-19 pose des problèmes de confidentialité des données. L'ampleur des préoccupations existantes en matière de confidentialité des données risque d'être exacerbée en cas d'urgence. En effet, les contrôles habituels sur les informations d'identification ou la confidentialité des données relatives aux paiements peuvent être levés ou ignorés en cas d'urgence au profit du secteur privé et/ou des agences publiques.[13] Cela peut se produire à cause de la nécessité urgente d'identifier les personnes ayant droit à une aide d'urgence. Un autre élément à prendre en compte est la demande extrême en retrait de fonds, qui peut rendre encore plus improbable que les personnes concernées puissent lire des informations relatives à la confidentialité ou qu'elles puissent donner un consentement effectif.
Ces préoccupations s'ajoutent à d'autres questions relatives à la confidentialité et à la protection des données (par exemple, le risque accru de cyber-fraude, la nécessité de garantir la confidentialité des informations sur la santé et des données personnelles chargées sur les applications de localisation liées au COVID-19).

9 OCDE : L'utilisation des données personnelles dans les services financiers et le rôle de l'éducation financière : Une analyse centrée sur le consommateur (2020) (section 1. 6)

10 CGAP : Focus Note - Is Data Privacy Good for Business ? (2019) et CGAP : Blog - Data Privacy Concerns Influence Financial Behaviours in India, Kenya

11 Centre de Toronto : Informatique en nuage : Questions pour les superviseurs (2020)

12 Comité de Bâle BRI sur le contrôle bancaire : Rapport sur les systèmes bancaires ouverts et les interfaces de programmation d'applications (2019) (résumé et section 6)

13 FMI : Série spéciale sur COVID-19 - Les services financiers numériques et la pandémie : Opportunités et risques pour les économies émergentes et en développement (2020)

TENDANCES ÉMERGENTES EN MATIÈRE DE POLITIQUE RÉGLEMENTAIRE DE DP4DFS

LOIS GÉNÉRALES SUR LA CONFIDENTIALITÉ DES DONNÉES

La tendance est de plus en plus à la création de cadres réglementaires en matière de confidentialité des données, qui reflètent l'importance des développements susmentionnés en matière de traitement des données.

La base de données de la CNUCED sur la législation en matière de protection des données et de confidentialité dans le monde indique que 66 % des pays disposent d'une telle législation et que 10 % disposent d'un projet de loi y relatif. Le document DLA Piper Data Protection Laws of the World donne également un aperçu des lois relatives à la confidentialité et à la protection des données dans 116 juridictions.

L'exemple le plus connu d'un cadre réglementaire de protection des données à vocation générale est probablement le règlement général de l'UE sur la protection des données (RGPD), [14] **mais il existe d'autres exemples de premier plan.** De nombreux pays émergents, ainsi que des pays développés, ont adopté ces dernières années des lois de grande portée sur la confidentialité et la protection des données. Le Ghana, la Malaisie, le Kenya, le Mexique, le Pérou, les Philippines et l'Afrique du Sud sont des exemples de membres de l'AIF disposant de telles lois. L'Inde a également un projet de loi avancé de ce type et le cabinet du Rwanda a récemment approuvé un projet de loi relatif à la protection des données et de la confidentialité. [15] Voir l'annexe 2 pour plus de détails. Ces lois sont d'application générale en ce sens qu'elles s'appliquent à toutes les formes de traitement de données, à toute autre fin, c'est-à-dire pas seulement aux services financiers. Toutefois, elles reflètent un certain nombre de tendances émergentes pertinentes pour les SFN, dont les plus significatives sont examinées ci-dessous.

UNE APPROCHE PROPORTIONNÉE FONDÉE SUR LES RISQUES

Il est généralement admis qu'une approche basée sur le risque et proportionnée doit être un élément clé dans la régulation des développements innovants du marché, y compris ceux qui sont pertinents pour le DP4DFS. C'est l'approche reflétée dans les principes directeurs proposés. Comme l'indique le Rapport Spécial de l'AIF sur la création d'écosystèmes favorables : Le rôle des régulateurs (2020) : " pour
réguler les mécanismes innovants du marché, de nombreux pays membres de l'AIF, tels que le Kenya, la Tanzanie et les Philippines, mettent en œuvre des approches réglementaires proportionnées ."[16] Le concept de " proportionnalité " est défini dans le Modèle stratégique de l'AIF sur la protection du consommateur des services financiers numériques (2020) comme " garantissant que
les réponses réglementaires reflètent le modèle d'affaires, la taille, l'importance systémique, ainsi que la complexité et l'activité transfrontalière des entités réglementées " . [17]

Une approche proportionnée fondée sur les risques est particulièrement importante dans le contexte de la FinTech et de l'inclusion financière, compte tenu de la volonté de ne pas freiner l'innovation ou la concurrence des SFN Cela peut se produire avec des exigences réglementaires trop lourdes, en particulier pour les petites entités de la FinTech dont les incitations et les ressources pour la gestion les risques liés à la protection de la confidentialité sont limitées. Une autre considération importante est que les régulateurs des pays en développement peuvent ne pas disposer des ressources ou de capacités techniques nécessaires pour superviser des normes complexes de DP4DFS. Le défi
est d'assurer un équilibre entre ces considérations et les risques liés au DP4DFS, ainsi que la nécessité de promouvoir l'inclusion financière et la confiance des personnes concernées.

Les régulateurs auront besoin d'une méthode d'évaluation des risques liés à la confidentialité des données pour une approche fondée sur les risques du DP4DFS.
Une telle méthodologie doit tenir compte des facteurs de risque communs dans le traitement des données par les modèles d'affaires des SFN, y compris ceux qui découlent des sources d'information, de la sensibilité de l'information, des cas d'utilisation et de l'inter-connectivité des systèmes. L'AIF envisage de publier un document sur cette question.

Afin d'assurer la proportionnalité, on peut envisager de fixer des exigences en fonction de l'importance des activités de traitement des données. Les facteurs pertinents peuvent comprendre, par exemple :

- La nature des produits des SFN ou du modèle d'affaires ;
- Le volume et la sensibilité des données traitées ;
- Le nombre de personnes concernées ;
- Rotation du fiduciaire des données ;
- Le risque de préjudice lié au traitement ; et
- Les nouvelles technologies utilisées.

14 https://gdpr.eu/

15 https://www.primature.gov.rw/index.php?id=131&tx_news_pi1%5Bnews%5D=933&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&cHash=7a012c144e6b2eb6d384a0bf1f153c26

16 https://www.afi-global.org/publications/3181/Creating-Enabling-FinTechFinTechFinTech-Ecosystèmes FinTech-Rôle des régulateurs

17 https://www.afi-global.org/publications/3465/Policy-Model-on-Protection des consommateurs pour les services financiers numériques. Cette définition figure également dans les orientations politiques du G20 et de l'OCDE : Approches en matière de protection des consommateurs des services financiers : Protection financière du consommateur à l'ère numérique (2018)

Les obligations précises imposées au " contrôleur des données important " dépendront probablement du contexte national. Par exemple, il peut arriver que seuls les contrôleurs des données « importants » soient tenus de s'enregistrer, de préparer une analyse d'impact sur la confidentialité des donnée pour des activités de traitement spécifiques, de désigner un délégué à la protection des données ou de préparer des rapports annuels de conformité ou de les faire auditer. La loi kényane sur la protection des données de 2019 et le projet de loi indien sur la protection des données personnelles de 2019 en sont des exemples.

Les obligations peuvent également être formulées en termes de mesures " raisonnables " ou d'autres normes modératrices. La loi philippine sur la protection des données (2019), par exemple, fait référence à des droits d'accès " raisonnables ", à des demandes " raisonnables " de correction des données de la part de la personne concernée et à des exigences " raisonnables et appropriées " en matière de sécurité. [18] D'autres indications sur la signification
de " raisonnable " sont utiles dans le cadre de la présente approche, comme par exemple les règlements et des directives publiés par l'autorité chargée de la protection des données.

Une autre approche de la proportionnalité consiste à exempter des " petites entreprises " qui sont clairement reconnues comme telles, de toute obligation de se conformer à un cadre réglementaire relatif à la protection de la confidentialité des données. L'Australie offre actuellement un rare exemple de cette approche, avec son exemption pour la plupart des " petites entreprises " (celles qui ont une rotation annuel de
de 3 millions de dollars australiens ou moins). [19] Toutefois, l'exemption est en cours d'examen.[20] La difficulté de cette approche est qu'elle ne prend pas en compte l'impact des activités des petites entreprises sur la vie privée des personnes concernées. Une " petite " entité de la FinTech, par exemple, peut avoir très peu d'employés mais utiliser des outils et des techniques de traitement des données avancés et opaques pour traiter d'énormes volumes de données à caractère personnel, y compris des données sensibles. En outre, une telle approche ne crée pas de conditions de concurrence équitables et augmente le risque d'arbitrage réglementaire. [21]

Par exemple, lorsque le droit à la confidentialité des données est reconnu par la législation nationale, toute limitation de ces droits doit être proportionnelle aux risques encourus par la personne concernée. Par exemple, le traitement des données à caractère personnel ne doit être autorisé que pour de raisons pour lesquelles elles ont été collectées et en tenant compte des consentements fournis.
En outre, toute limitation sur des droits de confidentialité des données doit être justifiée de manière réfléchie et des garanties proportionnées doivent être exigées. [22]

ENCADRÉ 5 : EXIGENCES DE PROPORTIONNALITÉ EN INDE

La Cour suprême de l'Inde a relevé les 4 exigences de " proportionnalité " suivantes lors de l'examen de la loi Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act (2016) et des limitations du droit constitutionnel de l'Inde relatives à la confidentialité :

(a) Une mesure restreignant un droit doit avoir un but légitime (étape du but légitime).

(b) Il doit s'agir d'un moyen approprié d'atteindre cet objectif (étape d'adéquation ou d'enjeu).

(c) Il ne doit pas y avoir d'alternative moins restrictive mais tout aussi efficace (étape de nécessité).

(d) La mesure ne doit pas avoir un impact disproportionné sur le titulaire du droit (étape d'équilibrage)

Source : Justice K.S. Puttaswamy vs. Union of India (arrêt du 26 septembre 2018)

MESURES D'ATTÉNUATION DES RISQUES DU DP4DFS

Les lois sur la confidentialité des données examinées aux fins de la présente note sur la directive contiennent des mesures d'atténuation des risques liés aux données personnelles. Le tableau 2 ci-dessous récapitule les plus courantes
de ces mesures d'atténuation en se référant aux risques liés à la confidentialité décrits ci-dessus. Les mesures d'atténuation sont susceptibles de varier d'un pays à l'autre, d'être plus détaillées dans la pratique et de faire l'objet de réserves et d'exceptions.

Le tableau est suivi d'une explication plus détaillée des facteurs d'atténuation les plus importants et des concepts connexes, ainsi que d'une analyse des questions spécifiques de proportionnalité.

La procédure d'exercice des droits des personnes concernées est également clarifiée. Il s'agit d'une question importante compte tenu de la complexité de l'environnement de la FinTech et de la nécessité pour les personnes concernées de savoir comment exercer leurs droits. Par exemple, les règlements instaurés en application de la loi mexicaine sur la protection des données privées détenues par des parties privées (2012) contiennent des dispositions étendues concernant les procédures d'exercice des droits
d'accès, de rectification, d'annulation et d'opposition (ACRO) (chapitre VII).

18 Philippines : Loi sur la protection des données (2019) (sections 16 et 20)

19 Bureau du commissaire australien à l'information : Small Business (consulté le 14 décembre 2020) et définitions connexes en Australie : Privacy Act 1988 (Division 1 of Part 1)

20 Australie : Attorney - General's Department : Privacy Act Review Issues Paper (2020)

21 Voir les principes de haut niveau du G20 pour l'inclusion financière numérique (2016) (principe 3)

22 Contrôleur européen de la protection des données : Le guide rapide du CEPD sur la nécessité et la proportionnalité (2020).

TABLEAU 2 : RISQUES ET MESURES D'ATTÉNUATION DU DP4DFS

AUCUN CONTRÔLE SUR LE TRAITEMENT DES DONNÉES PERSONNELLES	**Traitement licite :** Le traitement doit être " licite ", ce qui signifie généralement que la personne concernée a donné son consentement ou que le traitement est nécessaire aux fins d'un contrat, d'une obligation légale ou pour protéger les intérêts vitaux de la personne concernée ou ceux du contrôleur des données. **Transparence de l' information :** Des informations doivent être fournies à la personne concernée lors de la collecte de données à caractère personnel sur des questions telles que : les objectifs et les sources de la collecte ; les types d'informations à collecter, à qui elles peuvent être communiquées, les coordonnées du contrôleur des données, et les droits de la personne concernée. En outre, toutes les informations doivent être exprimées de manière claire et simple et dans une langue que la personne concernée est susceptible de comprendre. **Demandes de consentement :** Les demandes de consentement doivent être présentées séparément, être spécifiques et transmises librement et en connaissance de cause. **Exigence de loyauté :** Les processeurs des données sont tenus de traiter les personnes concernées de manière " équitable ". Ce concept n'est pas normalement défini et peut nécessiter des orientations réglementaires. **Limitation de la finalité :** Les données à caractère personnel ne peuvent être traitées que pour la finalité première/spécifique de leur collecte, à moins qu'une exception ne s'applique (comme le consentement). Cette mesure d'atténuation peut être une variante de la mesure d'atténuation de la " légalité ". **Minimisation des données :** Les données traitées doivent être adéquates et pertinentes et limitées au minimum nécessaire aux fins du traitement.	**Droit à l'information :** La personne concernée a le droit d'obtenir des informations claires et simples sur les activités de traitement et les entités concernées. **Droit à l'effacement/à l'oubli :** La personne concernée a le droit de demander l'effacement de ses données à caractère personnel lorsqu'elles ne sont plus nécessaires aux fins pour lesquelles elles ont été traitées. **Droit à la limitation du traitement :** La personne concernée peut demander la limitation du traitement des données dans certaines cas, par exemple lorsque l'exactitude de ces données est contestée ou que leur traitement est illégal. **Droit à la portabilité :** La personne concernée peut demander que les données à caractère personnel qui ont fait l'objet d'un traitement automatisé lui soient fournies sous une forme structurée, couramment utilisée et lisible par machine. **Droit de retirer son consentement :** La personne concernée peut retirer son consentement à tout moment.
LES DONNÉES SENSIBLES PEUVENT ÊTRE COMPROMISES	**Consentement explicite** : Exiger un consentement préalable, exprès le consentement doit être obtenu pour le traitement des informations " sensibles ". Voir l'annexe 3 pour une proposition de définition de ce concept.	
DES DONNÉES À CARACTÈRE PERSONNEL INCORRECTES, TROMPEUSES, INCOMPLÈTES OU PÉRIMÉES PEUVENT ÊTRE TRAITÉES	**Qualité des données :** Le contrôleur des données est tenu de prendre au moins des mesures raisonnables pour s'assurer que les données traitées sont exactes et à jour. **Délai de conservation :** Les données à caractère personnel ne peuvent être conservées que pendant la période nécessaire à la réalisation de la finalité du traitement.	**Droit de rectification :** La personne concernée a le droit de demander que ses informations soient corrigées. **Droit d'accès :** Une personne concernée a le droit d'accéder à ses informations sur demande et d'obtenir des détails sur toutes les activités y afférentes et sur les personnes qui les réalisent.
PRISE DE DÉCISION AUTOMATISÉE Y COMPRIS LE PROFILAGE PEUT CONDUIRE À DES DÉCISIONS INJUSTES	**Informations sur le traitement automatisé :** Exiger que la personne concernée reçoive des informations nécessaires sur toute prise de décision automatisée (y compris le profilage) et ses possibles conséquences, au moment où les données à caractère sont collectées.	**Droit d'opposition :** La personne concernée a le le droit légitime de s'opposer à la prise de décision uniquement sur la base d'un traitement automatisé de leurs données personnelles.

TABLEAU 2 : *SUITE*

RISQUES LIÉS A LA CONFIDENTIALITÉ DES DONNÉES	MESURES D'ATTÉNUATION - OBLIGATIONS DU CONTRÔLEUR DES DONNÉES	MESURES D'ATTÉNUATION - DROITS DES PERSONNES CONCERNÉES
IDENTIFIER LA FRAUDE ET L'UTILISATION ABUSIVE DES IDENTIFICATIONS OFFICIELLES QUI PEUVENT SE PRODUIRE	**Traiter les informations relatives à l'identité comme une catégorie d' " informations sensibles " :** Ces informations doivent faire l'objet d'un consentement explicite avant d'être traitées. D'autres mesures d'atténuation sont probables dans les lois qui mettent en place les systèmes d'identification nationaux et, plus généralement, dans les exigences de sécurité applicables aux systèmes de traitement des données à caractère personnel et dans les lois pénales.	**Sensibilisation des consommateurs :** Exiger que les personnes concernées soient informées de la meilleure méthode de sécuriser les informations relatives à leur identité, y compris leurs identifiants de sécurité.
LES DROITS DE RECOURS PEUVENT ÊTRE LIMITÉS.	**Obligation de rendre des comptes :** Rendre le contrôleur des données responsable de ses propres actions et de celles de tout sous-traitant qui agit en son nom. **Systèmes de réclamation :** Exiger des responsables du traitement des données qu'ils disposent d'un système transparent, efficace et gratuit pour traiter les réclamations concernant l'utilisation abusive de données à caractère personnel. **Appels :** veiller à la mise en place d'un système de Règlement Externe des Litiges (REL) pour assurer la médiation sur les litiges entre une personne concernée et un contrôleur des données et prendre les mesures appropriées (par exemple, en ce qui concerne l'indemnisation ou la correction des données). Le système de REL est généralement fourni par l'autorité compétente en matière de protection des données. **Limitations sur les transferts transfrontaliers de données :** Exiger que les transferts transfrontaliers de données ne soient effectués que vers des juridictions qui disposent de systèmes de protection de la confidentialité équivalents à celles de la juridiction destinataire, et/ou que des garanties contractuelles appropriées soient mises en place. Des règles de localisation des données peuvent également être en place. **Enregistrement des contrôleur des données :** Il peut également être exigé que les contrôleurs soient enregistrés auprès de l'autorité de protection des données compétente. Cette obligation peut ne s'appliquer qu'aux contrôleurs des données les plus importants.	**Sensibilisation aux systèmes de traitement des réclamations et au système de REL :** Les personnes concernées doivent être informées de leurs droits et des voies de réclamation et de recours pertinentes par le contrôleur des données lors de la transmission des données et de l'introduction d'une réclamation.
SYSTÈMES DE CONTRÔLE DES DONNÉES ET LES PROCÉDURES N'ASSURENT PAS LA CONFIDENTIALITÉ DES DONNÉES.	**Mécanismes de gouvernance :** Exiger que les contrôleurs des données mettent en place des politiques et des procédures détaillées conçues pour garantir le respect des principes et règles de confidentialité des données pertinentes, ainsi que les ressources technologiques et organisationnelles correspondantes. **Évaluations de l'impact sur la vie privée (PIAs) :** Exiger que le traitement de données à haut risque fasse l'objet d'évaluations proactives de l'impact sur la vie privée, qui couvrent des questions telles que les opérations de traitement proposées et les risques et mesures d'atténuation y relatives. **Publicité :** Exiger que les politiques de protection de la vie privée et les évaluations de l'impact y relatif soient rendues publiques (par exemple, sur le site web du responsable du traitement des données). **Délégués à la protection des données :** Exiger que les contrôleurs des données désignent un délégué à la protection des données (DPO) chargé de superviser le respect des règles en matière de confidentialité des données et de servir de point focal pour les personnes concernées et les autorités de protection des données (DPO). Cette obligation peut ne s'appliquer qu'aux contrôleurs des données les plus importants.	

Certaines des mesures d'atténuation susmentionnées peuvent être controversées. Les avis divergent quant à l'efficacité ou à l'adéquation de certaines des mesures d'atténuation, ainsi que sur la question de savoir s'il existe un équilibre approprié entre les risques pertinents et les mesures d'atténuation.

Les exemples de ces controverses comprennent entre autres, la tension apparente entre les règles de minimisation des données et l'ère du big data et de l'apprentissage automatique [23] et le débat sur la question de savoir si le droit à l'oubli est réaliste compte tenu de la technologie de blockchain. [24]

PRISE DE DÉCISION AUTOMATISÉE

L'accent est davantage mis sur les risques associés au marquage automatisé des décisions, y compris les préjugés à l'encontre des femmes ou d'autres segments vulnérables et le profilage. En résumé, le problème réside dans le fait que les décisions prises sur une personne concernée sur la base d'un traitement automatisé et d'un profilage sans intervention humaine peuvent donner lieu à des discriminations et à des préjugés injustes.

Une autre préoccupation est que les personnes concernées ne sont pas susceptibles de comprendre les algorithmes complexes et en constante évolution utilisés dans ces processus.[25] L'encadré ci-dessous donne quelques exemples de différentes approches réglementaires de ces risques.

ENCADRÉ 6 : PRISE DE DÉCISION AUTOMATISÉE

Voici des exemples de règles concernant la prise de décision automatisée, y compris le profilage (en résumé).

UE : Règlement général sur la protection des données (2016) Une personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques ou qui, de façon similaire, affecte de manière significative la personne concernée.
(article 22). Des exceptions s'appliquent lorsque le consentement a été donné ou que la décision est nécessaire à
la conclusion d'un contrat ou lorsque son exécution ou le traitement a été expressément autorisé par la loi avec les garanties appropriées.

Le "profilage" désigne, en résumé, le traitement automatisé qui utilise des données à caractère personnel pour évaluer des aspects de la personnalité d'une personne (par exemple, pour analyser ou prédire le rendement au travail ou la santé, les résultats économiques, les préférences, les intérêts, la fiabilité, la localisation ou les déplacements) (article 4).

ENCADRÉ 6 : *SUITE*

Ghana : Loi sur la protection des données (2012)
Une personne peut exiger du contrôleur des données qu'il veille à ce que les décisions l'affectant de manière significative ne soient pas fondées uniquement sur un traitement automatisé des données. Le contrôleur des données dispose alors de 21 jours pour indiquer les mesures qu'il prendra pour se mettre en conformité. Il existe toutefois des exceptions à ces exigences, notamment lorsque le traitement est lié à une décision de conclure un contrat (article 41).

CONSENTEMENT

L'accent est de plus en plus mis sur la nécessité d'obtenir des consentements équitables et efficaces pour le traitement des données. De nombreux produits informatiques de l'AIF énumérés à l'annexe 5 font référence à cette question. Par exemple, le modèle stratégique de l'AIF pour la monnaie électronique 2019 préconise d'exiger des émetteurs de monnaie électronique qu'ils obtiennent un consentement éclairé pour l'accès aux informations démographiques ou personnelles (partie VI). De nombreuses lois exigent également le consentement de la personne concernée pour le traitement de ses données, à moins qu'une exception ne s'applique. Les exceptions les plus courantes sont les traitements requis ou autorisés par la loi ou les traitements nécessaires à l'exécution d'un contrat. D'une manière générale, l'accent est désormais mis sur la nécessité de :

- Consentement libre, éclairé et sans ambiguïté ;
- Consentement à donner dans un but précis ;
- Demandes de consentement séparées ;
- Possibilité de retrait du consentement; et
- Responsabilité du contrôleur ou du processeur des données de prouver que le consentement a été donné.

Voir les exemples dans l'encadré 7 de la page suivante.

Toutefois, la question de savoir si le modèle de consentement est "cassé" fait l'objet d'un débat permanent. Les préoccupations sont nées du fait que le consentement est le socle de nombreux cadres de protection de la vie privée et l'on se demande fondamentalement si les personnes concernées disposent de la capacité à donner un consentement libre et éclairé.

23 UIT : Initiative mondiale pour l'inclusion financière (FIGI) Groupe de travail sur l'infrastructure de sécurité et la confiance, Big data, machine learning, consumer protection and privacy (2018).

24 Finextra : Blog de Carlo R.W. de Meijer Économiste et chercheur chez De Meijer Independent Financial Services Advisory (MIFSA) : Blockchain versus GDPR et qui devrait s'adapter le plus (2018).

25 Blog de la FCI : Des données pour une finance inclusive : Tenir la promesse pour les consommateurs (2020)

ENCADRÉ 7 : EXEMPLES D'EXIGENCES RENFORCÉES EN MATIÈRE DE CONSENTEMENT

UE : Règlement général sur la protection des données (2016) Le traitement des données à caractère personnel n'est licite que dans la mesure où l'intéressé a donné son consentement spécifique à la finalité particulière du traitement ou si une autre exception s'applique (article 6).

Le concept de "consentement" est défini comme suit : "toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle l'intéressé accepte, par une déclaration ou par une action positive claire, que des données à caractère personnel la concernant fassent l'objet d'un traitement" (article 4, paragraphe 11).

D'autres règles du GDPR à l'article 7 exigent que la demande de consentement soit :

- "clairement distincte" des autres questions ;
- présentée sous une forme intelligible et facilement accessible ; et
- Dans un langage clair et simple.

L'intéressé doit également avoir le droit de retirer son consentement à tout moment et aussi facilement que lorsqu'il le donne.

Malaisie : Loi sur la protection des données personnelles et code de protection des données personnelles pour le secteur bancaire et financier (BFS code)
La loi énonce comme principe général que les intéressés doivent donner leur consentement pour le traitement des données à caractère personnel (à quelques exceptions près) (article 6).
Bien que le concept de "consentement" ne soit pas défini dans la loi, le BFS code obligatoire fournit des exemples de formes de consentement pour le démarrage d'un contrat (y compris le consentement présumé, ainsi que les signatures ou les coches indiquant le consentement, le consentement opt-in et le consentement verbal). Il est également prévu que les consentements soient obtenus par voie électronique, y compris par SMS, courrier électronique et systèmes de messagerie). Dans tous les cas, le formulaire de consentement doit être enregistré et conservé.

Pérou : Loi sur la protection des données personnelles (2011) et Règlement d'application de la loi (2013)
L'un des principes directeurs de la loi est que l' intéressé doit donner son consentement au traitement de ses données personnelles (sauf exceptions spécifiées).
Le consentement doit être "préalable, éclairé, explicite et non équivoque" et peut être retiré à tout moment (articles 5 et 13). Le règlement péruvien sur la protection des données personnelles contient des règles détaillées et des exemples sur la signification de ce concept de consentement et précise qu'il peut être donné par voie électronique.

Philippines : Loi de 2012 sur la protection des données personnelles et règles d'application et règlements
Le consentement est requis pour la collecte et le traitement des données à caractère personnel (sous réserve d'exceptions) (article 12). Le concept de "consentement de l'intéressé" est

ENCADRÉ 7 : *SUITE*

définie comme "... toute manifestation de volonté, libre, spécifique et informée, par laquelle l'intéressé accepte la collecte et le traitement d'informations à caractère personnel la concernant. Le consentement doit
être attestée par des moyens écrits, électroniques ou enregistrés. (article 3, point b)). Les règles et règlements de mise en œuvre
prévoient également que les consentements sont limités dans le temps et peuvent être retirés (article 19).

Afrique du Sud : Loi de 2013 sur la protection des informations personnelles
Le traitement des données à caractère personnel nécessite un consentement (sauf exception) (article 11). Il incombe à la partie responsable de prouver le consentement. Le concept de consentement est défini comme "toute manifestation de volonté délibérée, spécifique et informée par laquelle le traitement d'informations à caractère personnel est autorisé " (article 1). En outre, les consentements pour la prospection directe par communication électronique doivent être donnés sous une forme prescrite (article 69, règlement 6 et formulaire 4).

C'est particulièrement le cas dans le contexte de l'inclusion financière, où les intéressés sont susceptibles d'avoir de faibles capacités financières[26]Les principales préoccupations sont les suivantes **:**

- formulaires de consentement longs et complexes ;
- Consentements "noyés" dans de longues conditions générales ;
- Absence de choix - l' intéressé peut avoir l'impression qu'il est obligé de donner son consentement pour accéder aux SFN ;
- Consentements groupés, qui couvrent le traitement des données pour les SFN et, par exemple, le marketing direct ;
- Impossibilité de retirer son consentement ;
- Consentements qui sont adressés à plusieurs entités, par exemple le prestataire des SFN et les prestataires des autres services ;
- Impossibilité de conserver les formulaires de consentement pour référence ultérieure ; et
- Consentements rédigés dans une langue que intéressé ne comprend pas.[27]

26 Banque mondiale : Protection des consommateurs des services financiers et nouvelles formes de traitement des données au-delà des rapports de crédit (2018)

27 McDonald AM et Cranor LF The Cost of Reading Privacy Policies A Journal of Law and Policy for the Information Society, vol. 4, no. 3 (2008), 543-568 (2008). Cette étude a révélé qu'il faudrait en moyenne 244 heures par an à une personne pour lire les politiques de confidentialité en ligne !

Des alternatives au consentement sont désormais envisagées. Par exemple, le CGAP a préconisé à la fois une approche fondée sur les objectifs légitimes et une approche fiduciaire des données comme alternatives au modèle de consentement dans leur récente publication CGAP Making Data Work for the Poor (2020). La nécessité du consentement ne doit toutefois pas être complètement écartée, car il est probable qu'il soit toujours requis dans certains cas - par exemple, le consentement explicite pour le traitement d'informations sensibles et le consentement explicite à des fins de marketing direct ou de vente croisée. En outre, le consentement est le socle des nouvelles approches des systèmes bancaires ouverts.

Il existe des approches qui peuvent contribuer à atténuer les défauts susmentionnés du modèle de consentement. En voici quelques exemples :

- Imposer un principe général prépondérant de traitement loyal des données (ou un concept similaire)[28];
- Traiter les données financières comme une catégorie particulière qui nécessite un consentement explicite [29];
- Soutenir les exigences légales en matière de consentement décrites ci-dessus par des règles détaillées sur ce qui est nécessaire pour chaque élément de l'exigence (comme par exemple la signification des termes "librement donné", "préalable", "exprès" et "informé" et la présentation et la soumission des formulaires de consentement dans un environnement numérique);[30] et
- le recours à des tiers pour gérer le processus de consentement dans les systèmes bancaires ouverts (voir encadré 8).

LES CARTES D'IDENTITÉ NUMÉRIQUES ET LES RISQUES DE FRAUDE, D'ABUS D'IDENTITÉ ET D'ACCÈS INAPPROPRIÉ

Les avantages des systèmes d'identification numérique pour les objectifs de développement sont reconnus au niveau mondial. Comme indiqué dans le document Banque mondiale : Défi de l'identification numérique et de la protection des données:
Practitioner's Note (2019), ils peuvent inclure (en résumé) :

- La facilitation de l'accès aux "droits, services et opportunités économiques qui requièrent une preuve d'identité" (par ex. les SFN, notamment le crédit, les paiements, l'épargne, l' assurance et les pensions) ;
- Le renforcement de la gouvernance et de la prestation de services (par exemple, en minimisant la fraude du secteur public dans les paiements G2P tout en facilitant les transferts d'argent G2P) ;
- Le soutien au secteur privé pour qu'il se conforme aux exigences en matière d'identité, telles que les règles eKYC ; et
- La promotion de l'économie numérique (par exemple, en facilitant les transactions fiables et en créant des opportunités d'innovation).

ENCADRÉ 8 : CGAP : LA NOUVELLE APPROCHE DE L'INDE EN MATIERE DE PARTAGE DES DONNEES PERSONNELLES (2020)

Le consentement et le modèle indien d'agrégation de comptes

"Le partage des données entre les prestataires de services financiers (PSF) peut permettre à ces derniers d'offrir plus efficacement une gamme plus large de produits financiers mieux adaptés aux besoins des clients, y compris les clients à faibles revenus. Toutefois, il est important de s'assurer que les clients comprennent et consentent à l'utilisation de leurs données.

La solution indienne pour relever ce défi est l'agrégation de comptes (AA). La Reserve Bank of India (RBI) a créé les AA en 2018 afin de simplifier le processus de consentement pour les clients.
Dans la plupart des régimes de banque ouverte, les fournisseurs d'informations financières (FIP) et les utilisateurs d'informations financières (FIU) procèdent à un échange direct de données. Ce modèle direct d'échange de données - par exemple entre une banque et un établissement de crédit - ne permet pas aux clients d'avoir un contrôle complet et une visibilité illimitée sur les données partagées et leur finalité.
Les AA ont été conçues pour s'intercaler entre les FIF et les UIF afin de faciliter l'échange de données de manière plus transparente. Malgré leur nom, les AA n'ont pas le droit de voir, le stockage, l'analyse ou l'utilisation des données relatives aux clients. En tant qu'intermédiaires impartiaux et de confiance, ils se contentent de gérer les consentements et de servir de canaux par lesquels les données circulent entre les PSF.
Lorsqu'un client donne son consentement à un fournisseur par l'intermédiaire de l'AA, ce dernier récupère les informations pertinentes des comptes financiers du client et l'envoie par des canaux sécurisés à l'institution requérante".

- **Voir aussi :** Banque de réserve de l'Inde : Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions (2016)

En revanche, les risques liés à la confidentialité associés aux cartes d'identité numériques sont reconnus. L'ampleur de ces risques est potentiellement énorme, compte tenu de la taille des ensembles de données et de la centralisation des données.[31] Ces risques peuvent être résumés comme suit :

- La fraude à l'identité est particulièrement préoccupante avec les cartes d'identité numériques, qui reposent sur la biométrie car elles ne sont pas secrètes et les données d'identité biométriques compromises ne peuvent pas être corrigées;

28 Philippines : Personal Data Protection Act (2012) (section 11(2)) et Rule IV section 19(b) of Implementing Rules and Regulations

29 Mexique : Loi fédérale sur la protection des données personnelles détenues par des parties privées (2010) (articles 8, 10 et 37) et Règlement (article 15)

30 Voir, par exemple, Pérou : Loi sur la protection des données personnelles (2011) et Règlement d'application de la loi (2013) (voir en particulier l'article 7 du Règlement et les chapitres I et II du Titre III).

31 Banque mondiale : L'identification numérique et le défi de la protection des données : Practitioner's Note (2019)

- Identification sans consentement - cela peut se faire par:
  - L'utilisation non autorisée de données biométriques telles que les empreintes digitales, les scans de l'iris ou les éléments de reconnaissance faciale ;
  - L'identification d'une personne dans plusieurs domaines de service grâce à l'utilisation de son identifiant numérique ;
- la surveillance illégale des personnes par l'utilisation d'identifiants numériques ;
- les demandes inappropriées adressées à un client pour qu'il s'identifie en fournissant sa carte d'identité numérique, avec les risques d'exploitation commerciale qui en découlent; et
- L'utilisation abusive d'informations d'identification numérique dans le domaine public par le biais d'une utilisation et d'un partage inappropriés entre les agences gouvernementales.[32]

Les risques susmentionnés sont particulièrement pertinents pour les SFN. Il peut s'agir, par exemple, d'une usurpation d'identité pour obtenir un crédit, des subventions publiques ou des transferts d'argent, pour ouvrir un compte d'épargne utilisé pour des activités illégales ou pour accéder à des fonds sur des comptes d'investissement ou de retraite en ligne. Ces risques ont entraîné des demandes de cadres de protection de la vie privée.

Pour une discussion plus approfondie sur les avantages et les risques liés aux systèmes d'identification numérique, voir : le rapport spécial de l'AIF sur les FinTech pour l'inclusion financière : A Framework for Digital Financial Transformation (2018) (Pilier 1) et également AFI : KYC Innovations, Financial Inclusion and Integrity In Selected AFI Member Countries (2019) (Innovations KYC, inclusion financière et intégrité dans certains pays membres de l'AFI).

CONFIDENTIALITÈ DÈS LA CONCEPTION

Les règles proactives de à peine dès la conception constituent une autre innovation importante, qui peut minimiser les risques liés au DP4DFS pour les intéressés. Les principes qui sous-tendent ces règles sont bien connus, [33] mais ils viennent à peine de commencer à être introduits dans les cadres relatifs à la confidentialité. En résumé, l'idée est que les prestataires de SFN doivent disposer de mécanismes de gouvernance, de politiques, de procédures et de ressources documentés pour s'assurer qu'ils respectent à tout moment les règles relatives à la confidentialité. En outre, le paramétrage par défaut des systèmes devrait garantir la conformité (par exemple, avec la règle selon laquelle seules les données minimales nécessaires à la finalité autorisée de la collecte sont traitées). Dans la pratique, le respect de ces exigences par les prestataires des SFN peuvent être vérifié par les régulateurs lors de l'examen des demandes de licence ou d'enregistrement, des demandes d'approbation de nouveaux produits de SFN ou dans un contexte de bac à sable réglementaire.

La nouvelle loi kényane sur la protection des données (2019) nous en donne un exemple, à l'article 41 "Protection des données dès la conception ou par défaut". Ces exigences, qui sont similaires à celles de l'article 25 du GDPR, requièrent (en résumé) que les contrôleurs et les processeurs de données mettent en place des mesures techniques et organisationnelles appropriées pour :

- Mettre en œuvre les principes de protection des données du Kenya et les garanties nécessaires ; et
- Veiller à ce que, par défaut, uniquement les données à caractère personnel nécessaires à chaque finalité spécifique soient traitées, en tenant compte de facteurs spécifiques tels que la quantité de données à caractère personnel collectées, l'étendue du traitement, la période de conservation et les coûts de traitement.

La loi kenyane sur la protection des données impose également aux controleurs et aux processeurs des données de prendre en compte les risques liés aux données personnelles, les garanties, la pseudonymisation et le cryptage des données personnelles, ainsi que la capacité de restaurer les données.

Un autre exemple d'exigences en matière de confidentialité dès la conception se trouve dans le projet de loi indien sur la protection des données personnelles (2019). Le projet de loi exige que chaque fiduciaire de données prépare une politique détaillée de respect de la confidentialité dès la conception. La politique peut être soumise à la DPA pour certification et toute politique certifiée doit être publiée sur le site web du fiduciaire des données et de l'Autorité (article 22). La publication de la politique est une exigence importante car elle est susceptible d'améliorer la transparence à l'intention des intéressés et des investisseurs, ainsi que pour l'autorité de protection des données et d'autres régulateurs et agences gouvernementales.

ÉVALUATIONS D'IMPACT SUR LA CONFIDENTIALITÉ DES DONNÉES

Certains pays exigent également d'évaluer l'impact sur la confidentialité d'une opération particulière de traitement de données. Ces exigences peuvent s'ajouter à celles de la (Privacy by Design)confidentialité dés la conception. Par exemple,
La loi kenyane sur la protection des données (2019) exige qu'une "évaluation de l'impact sur la protection des données" soit réalisée pour un traitement susceptible d'entraîner "un risque élevé pour les droits et libertés d'une personne concernée, en raison de sa nature, de sa portée, de son contexte et de ses finalités".[34] En résumé, elle exige une description systématique des exigences de traitement proposées, de leur nécessité et de leur proportionnalité, ainsi que des risques liés aux droits et libertés des personnes concernées et des mesures à prendre pour les atténuer.

32 Pour un examen de ces questions, voir la décision de la Cour suprême de l'Inde dans l'affaire Justice K.S. Puttaswamy vs. Union of India (2017) 10 SCC 1 qui a invalidé les dispositions législatives permettant aux entreprises et aux particuliers de demander une identification via l'identifiant Aadhaar de l'Inde - voir https://www.scobserver.in/court-case/constitutionality-of-aadhaar-act/ plain-englishsummary-of-judgment.

33 Cavoukian, Ann 'Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices' (2011)

34 Loi kényane sur la protection des données (2019) (article 31).

Il est **également prévu que le commissaire à la protection des données soit consulté et qu'il publie des lignes directrices.**[35] Le Bureau du commissaire australien à l'information a publié un Guide to Undertaking Privacy Impact Assessments et des conseils connexes sur l'évaluation des risques liés à la confidentialité, ainsi qu'un cours d'apprentissage en ligne.[36] Le projet de loi indien sur la protection des données personnelles (2019) est également assez spécifique en exigeant qu'un fiduciaire de données important réalise une évaluation de l'impact sur la protection des données dans les cas suivants : lorsque le traitement implique de nouvelles technologies ou un traitement à grande échelle ou l'utilisation de données sensibles (telles que des données génétiques ou biométriques) ou si le traitement comporte un risque de "préjudice important "[37].

ENREGISTREMENT DES CONTROLEURS ET FOURNISSEURS DE DONNÉES

Certains pays en développement exigent désormais que les contrôleur des données soient enregistrés. La loi ghanéenne sur la protection des données (2012), comme indiqué ci-dessus, exige l'enregistrement de tous les contrôleurs des données.[38] La loi kenyane sur la protection des données (2019) stipule que le commissaire chargé des données (Data Commissioner) peut prescrire des seuils pour l'enregistrement obligatoire des contrôleurs et processeurs des données[39] Les considérations pertinentes pour exiger l'enregistrement comprennent :

- La question de savoir si et dans quelle mesure l'enregistrement contribuera à la réalisation des objectifs en matière de protection de la confidentialité;
- L'obligation d'enregistrement constitue-t-elle une réponse proportionnée aux risques liés à la confidentialité des donneés? et
- la capacité de surveillance et la disponibilité de ressources pour superviser le processus d'enregistrement.

RESPONSABLES DE LA PROTECTION DES DONNÉES

Des dispositions sont de plus en plus prévues pour la nomination de responsables de la confidentialité (ou de la protection) des données (DPO). Par exemple, les régimes réglementaires relatifs à la protection des données au Ghana, au Kenya, au Mexique et au Brésil comportent de telles dispositions. Dans certains cas la nomination semble être facultative. Dans d'autres, elle dépend de la question de savoir si la nature, la portée, le contexte et les finalités des activités du responsable du traitement sont suffisamment importants et/ou significatifs, ainsi que de la nature de données traitées. Par exemple, le traitement de données sensibles peut suggérer la désignation d'un DPO.

Les fonctions des DPO varient mais, de manière générale, elles peuvent inclure:

- Donner des orientations sur le respect du cadre réglementaire ;
- être un point focal pour les personnes concernées qui ont des questions ou des réclamations à faire;
- servir de point focal pour le DPA et les autres régulateurs et agences compétents;
- être consulté sur les évaluations de l'impact sur la vie privée ; et
- Faciliter le renforcement des capacités du personnel et des agents.

SIGNALER LES VIOLATIONS DE LA CONFIDENTIALITÉ DES DONNÉES

L'obligation de signaler tout accès non autorisé à des données à caractère personnel est en cours d'introduction. Par exemple, la loi kényane sur la protection des données (2019) prévoit, à quelques exceptions près, qu'en cas d'accès non autorisé à des données à caractère personnel et de "risque réel de préjudice" pour l'intéressé, le commissaire chargé des données doit être informé dans les 72 heures. L' intéressé doit être notifié par écrit dans un "délai raisonnablement praticable" et recevoir des informations suffisantes pour prendre des mesures adéquates de protection.[40] D'autres pays comme le Ghana, le Mexique, le Pérou et l'Australie qui imposent l'obligation de notifier l'autorité de protection des données et/ou les personnes concernées.

SYSTEME BANCAIRE OUVERT

Des régimes de systèmes bancaires ouverts sont introduits dans divers pays et régions, y compris dans les économies en développement et émergentes, ce qui suscite d'importantes questions en matière de protection de la confidentialité.[41]En résumé, le concept de " système bancaire **ouvert**" fait généralement référence aux systèmes de partage des données des clients par les institutions financières avec des tiers (tels que d'autres institutions financières, des fournisseurs de services de paiement, des agrégateurs de données et des partenaires commerciaux). Les questions préoccupantes en matière de confidentialité des données incluent la nécessité d'un consentement explicite et la nécessité de garantir que les intéressés comprennent ce qu'ils acceptent. Bien entendu, il existe également des problèmes de protection des données (comme les questions de sécurité), qui dépassent la portée de la présente note sur la directive. De exemples de tels régimes sous des formes différentes
se trouvent dans les règles de partage des données de la loi mexicaine sur les institutions de technologie financière (2018)[42] ; dans les dispositions concernant la capacité des systèmes de paiement et des prestataires de services à accéder aux données à caractère personnel, à les traiter et à les conserver dans la directive 2015/2366 de l'UE, dans

35 La nouvelle commissaire à la protection des données du Kenya (Mme Immaculate Kassait) a prêté serment le 6 novembre 2020. Voir https://www.capitalfm.co.ke/ news/2020/11/immaculate-kassait-sworn-in-as-inaugural-data- commissioner/

36 https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-entreprendre des évaluations de l'impact sur la vie privée/

37 le Projet de loi de l'Inde sur la protection des données personnelles (2019) (article 27 et voir la définition de "préjudice important" à l'article 3).

38 Article 27

39 Article 18

40 Article 43

41 BRI Comité de Bâle sur le contrôle bancaire : Rapport sur l'Open Banking et les interfaces de programmation d'applications (2019)

42 Article 76

Payments Services (PSD2)[43] ; et dans les règles bancaires ouvertes de l'Australie et le droit aux données des clients y relatifs.[44]

RECOURS DES CONSOMMATEURS

Des dispositions sont prévues pour que les utilisateurs de données puissent déposer des plaintes en cas de violation de leurs droits en matière de données. Par exemple, comme indiqué ci-dessus, les règlements pris en application de la loi mexicaine sur la protection des données privées détenues par des parties privées (2012) contiennent des dispositions détaillées sur les procédures d'exercice des droits de l'ACRO. Un autre exemple est fourni par le chapitre III du titre IV "Procédure de protection" du règlement pris aux fins de la loi philippine sur la protection des données (2012).

Il est courant d'autoriser le dépôt de plaintes auprès de l'autorité de protection des données compétente. Ces droits ne peuvent généralement être exercés si la réclamation a d'abord été soumise au contrôleur ou au processeur des données et que celui-ci a rendu une décision défavorable ou n'a pas traité la réclamation dans un délai raisonnable. Par exemple, en vertu de la loi sud-africaine sur la protection des informations personnelles (2013), des plaintes peuvent être déposées auprès du régulateur de l'information. En outre, une indemnisation peut être accordée sur la base d'une action civile intentée par la personne concernée ou par le régulateur de l'information à la demande de intéressé. Il est également prévu que les codes de conduite publiés par l'autorité de régulation comprennent des dispositions relatives au traitement des plaintes, qui doivent être conformes aux normes prescrites et à toutes les lignes directrices publiées par l'autorité de régulation. D'autres pays couvrent également une partie ou la totalité de ces questions. Les lois sur la protection des données du Ghana, de la Malaisie, du Mexique et des Philippines en sont des exemples.

Les dispositions permettant à l'autorité de protection des données d'engager des actions au nom des personnes concernées sont rares. L'Afrique du Sud en est un exemple. L'OIAC d'Australien peut également prendre l'initiative d'enquêter sur une ingérence dans la vie privée et décider d'une indemnisation ou exiger d'autres mesures correctives. Il est important que les autorités de protection des données disposent de tels pouvoirs dans le contexte de l'inclusion financière, étant donné que les personnes concernées sont susceptibles de ne pas disposer de ressources ou de capacités nécessaires pour intenter de telles actions, ou d' être mal informées de leurs droits.

CONFIDENTIALITÉ DES DONNÉES DANS LES SITUATIONS D'URGENCE

Certains pays s'affranchissent des règles strictes des cadres de protection de la vie privée pour permettre la circulation des données dans les cas de situations d'urgence (par exemple, le COVD-19). Un exemple rare nous vient d'Australie. En résumé, la partie VIA de la loi australienne sur la protection de la vie privée (1988) permet de faire des annonces d'urgence qui autorisent la collecte, l'utilisation et la divulgation d'informations dans un but autorisé. Ces objectifs comprennent notamment aider les personnes à obtenir une assistance financière ou une autre forme d'assistance humanitaire. Les annonces peuvent s'appliquer pour une période limitée allant jusqu'à 12 mois. Lorsqu'une entité s'appuie valablement sur une telle annonce, elle ne sera pas tenue responsable de la violation de lois ou de codes spécifiques, y compris les principes australiens de protection de la vie privée ou un code enregistré.

Des agences internationales ont également fourni des orientations sur les questions de confidentialité des données dans le contexte de COVID-19. Le cadre politique de l'AIF pour l'exploitation des services financiers numériques dans les cas des urgences mondiales - Cas du COVID-19 (2020), par exemple, suggère que "les fournisseurs de services financiers numériques doivent s'assurer que les données des consommateurs sont protégées et ne sont pas partagées avec des tiers". Dans des circonstances exceptionnelles, si des données des clients doivent être extraites (pour la recherche des contacts et le confinement de la transmission), cela doit se faire de manière volontaire. En outre, ces mesures doivent être temporaires. (Règlement d'habilitation du pilier III).

L'OCDE a également formulé un certain nombre de recommandations sur la confidentialité des données dans ses orientations sur le COVID-19. Les principales recommandations sont les suivantes (en résumé) :

- Les gouvernements doivent promouvoir l'utilisation responsable des données personnelles ;
- Les gouvernements doivent consulter les autorités chargées de la protection de la vie privée(PEA) avant d'introduire des mesures qui risquent de porter atteinte aux principes établis en matière de protection de la vie privée et des données ;
- Les PEA doivent tenir compte des incertitudes réglementaires ;
- Sous réserve des garanties nécessaires et proportionnées, les gouvernements doivent soutenir la coopération nationale et internationale en matière de collecte, de traitement et de partage des données de santé à caractère personnel ; et
- Les gouvernements et les contrôleurs des données doivent être transparents et responsables.[45]

ENCADRÉ 9 : OCDE : GARANTIR LA CONFIDENTIALITÉ DES DONNÉES DANS LA LUTTE CONTRE LE COVID-19 (2020)

Les décideurs politiques, en consultation avec les autorités chargées de veiller au respect de la vie privée, doivent évaluer les compromis possibles dans l'utilisation des données pendant cette crise (en conciliant les risques et les avantages), mais ils doivent veiller à ce que des mesures extraordinaires soient proportionnées aux risques et mises en œuvre en toute transparence, en toute responsabilité et en s'engageant à cesser immédiatement ou à annuler les utilisations exceptionnelles de données une fois la crise terminée".

43 Article 94

44 Voir https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0

45 OCDE Garantir la confidentialité des données dans le cadre de la lutte contre le COVID-19 (2020)

La GSMA a également publié les lignes directrices COVID-19 sur la protection de la vie privée à l'intention des opérateurs de réseaux mobiles. [46] Ces lignes directrices peuvent s'appliquer aux SFN par téléphone mobile et aux questions liées à la confidentialité. L'accent est mis sur les divulgations à l'intention des gouvernements et des agences. Les lignes directrices couvrent des questions telles que la nécessité de se conformer à des considérations éthiques ainsi qu'à la loi, la transparence des divulgations et la divulgation de métadonnées et de données agrégées non identifiables.

SANCTIONS

Des sanctions importantes sont également prévues dans les nouveaux cadres réglementaires relatifs à la protection de la vie privée. Des sanctions à grande échelle peuvent inciter au respect des règles, ainsi qu'une incitation à investir dans les technologies d'amélioration de la confidentialité (qui dépassent le champ d'application de la présente note sur la directive).

Il existe plusieurs approches pour déterminer les pénalités. Dans certains cas, elles sont basées sur un pourcentage du chiffre d'affaires annuel. Par exemple, le GDPR de l'UE prévoit une sanction maximale pouvant aller jusqu'à 4 % du chiffre d'affaires annuel global de l'entité. La nouvelle loi kényane sur la protection des données (2019) adopte une approche moins stricte en prévoyant que la sanction maximale est la moins élevée des deux suivantes : une sanction maximale de cinq millions de shillings (environ 45 700 USD)[48] ou un pour cent du chiffre d'affaires annuel de l'exercice précédent. D'autres pays, comme la Malaisie, prévoient une amende d'un montant maximal et/ou une peine d'emprisonnement.
La loi fédérale mexicaine sur la protection des données personnelles détenues par des parties privées adopte une approche intéressante
dans la mesure où les amendes potentielles sont un multiple du salaire minimum de la ville de Mexico, le montant variant en fonction de l'infraction. Un dernier exemple nous vient du Pérou, où les infractions sont classées comme légères, graves ou très graves, le niveau de l'amende variant en conséquence.

BACS À SABLE RÉGLEMENTAIRES

Les bacs à sable réglementaires mis en place par les régulateurs financiers ne semblent pas de manière courante prendre spécifiquement en compte les innovations en matière de DP4DFS. Un bac à sable réglementaire, en bref, est un mécanisme de plus en plus populaire pour tester les innovations FinTech dans un environnement supervisé. Toutefois, il ne semble pas courant de tester les innovations liées à la confidentialité des données dans des bacs à sable ou dans des forums d'innovation similaires mis en place par les régulateurs financiers. Au lieu de cela, des pays tels que l'Australie, par exemple, indique clairement que les entités qui se prévalent d'exemptions de bac à sable réglementaire doivent toujours se conformer aux lois sur la confidentialité des données. [49]

Toutefois, il existe quelques exemples d'utilisation du concept de bac à sable dans des circonstances pertinentes pour le DP4DFS. [50] Par exemple :

- L'Information Commissioner's Office (ICO) du Royaume-Uni a mis en place un bac à sable, et ses principaux domaines d'intervention pour 2020-2021 comprennent notamment les innovations liées au partage des données, y compris dans le domaine de la finance. [51] Il est important de noter que l'ICO et la Financial Conduct Authority du Royaume-Uni disposent également d'un protocole d'accord de 2019 établissant un cadre pour la coopération, la coordination et le partage d'informations entre les régulateurs. [52]
- Il existe également des bacs à sable thématiques couvrant des objectifs spécifiques en matière de politique de confidentialité des données. Des exemples de bacs à sable réglementaires thématiques existants, dont certains concernent l'inclusion financière et les technologies "NextGen", sont mis en évidence dans le CGAP : Blog - Une tendance croissante dans la régulation financière : Thematic Sandboxes (2019).

Des bacs à sable réglementaires pour les innovations en matière de confidentialité des données peuvent également être prévus par la législation. Le projet de loi indien sur la protection des données personnelles (2019) en est un exemple rare : il exige que la DPA crée un " bac à sable ". Il s'agit " d'encourager l'innovation dans le domaine de l'intelligence artificielle, de l'apprentissage automatique ou de toute autre technologie émergente dans l'intérêt public " (article 40). Les fiduciaires de données dont les politiques de protection de la vie privée ont été certifiées par l'autorité de protection des données sont éligibles à l'inclusion dans le bac à sable (sous réserve des règles qui doivent encore être élaborées).

RÈGLES ET ORIENTATIONS SECTORIELLES SUR LES DP4DFS

Outre les lois d'application générale mentionnées ci-dessus, il existe quelques exemples de cadres réglementaires, de codes de pratique, de stratégies nationales et d'interventions politiques qui s'appliquent spécifiquement à certains aspects du DP4DFS. Quelques exemples sont présentés ci-dessous.

ENCADRÉ **10 :** CADRE POLITIQUE DE L'AIF POUR UN CRÉDIT NUMÉRIQUE RESPONSABLE (2020)

La protection des données du consommateur est essentielle pour garantir que le crédit numérique, ainsi que d'autres services financiers, donne aux consommateurs l'assurance que leurs données sont confidentielles et utilisées de manière appropriée. (Principe 6 : Protection des données et de la vie privée)

46 GSMA COVID-19 - Lignes directrices sur la protection de la vie privée (2020)

47 Pour une réflexion sur le STPGV et les questions connexes, voir UIT : Groupe de travail sur l'infrastructure de sécurité et la confiance de l'Initiative mondiale pour l'inclusion financière (FIGI), Big data, machine learning, consumer protection and privacy (2018).

48 Au 15 novembre 2020 https://www.xe.com/

49 ASIC : INFO 248 Bac à sable réglementaire amélioré (2020)

50 Centre pour le leadership en matière de politique de l'information : Bacs à sable réglementaires en matière de protection des données : Engagement constructif et réglementation innovante dans la pratique (2019)

51 https://ico.org.uk/sandbox

52 https://ico.org.uk/media/about-the-ico/documents/2614342/autorité-de-conduite-financière-ico-mou.pdf

RÈGLES DU SECTEUR FINANCIER CONCERNANT LES DP4DFS

Des règles spécifiques au secteur peuvent également être émises pour couvrir les questions de DP4DFS d'intérêt particulier. Un exemple récent vient des Philippines (voir encadré 11).

ENCADRÉ 11 : CIRCULAIRE NO. 20-10 DE LA COMMISSION NATIONALE DE LA PROTECTION DE LA CONFIDENTIALITÉ DES PHILIPPINES (GUIDELINES ON THE PROCESSING OF PERSONAL DATA FOR LOAN RELATED TRANSACTIONS (2020))

La Commission nationale de la protection de la confidentialité des Philippines a récemment publié la circulaire susmentionnée à la suite de milliers de reclamations concernant l'utilisation de téléphones portables et d'ordinateurs portables et les données des médias sociaux par les prêteurs en ligne, y compris à des fins de recouvrement de créances. Elle s'applique aux sociétés de prêt et de financement et contient des règles interdisant l'utilisation des coordonnées à des fins de recouvrement de créances, restreignant l'utilisation de photos et d'autres règles limitant la collecte, l'utilisation, la divulgation et la conservation d'informations personnelles. La NCP a ordonné séparément la cessation des activités de traitement par divers prêteurs en ligne[53]et par ailleurs, la Securities and Exchange Commission a également pris des mesures pour révoquer l'autorisation d'exercer de certains de ces prêteurs. [54]

Les cadres réglementaires relatifs aux banques, aux paiements et à la monnaie électronique peuvent également contenir des règles en matière de protection de données personnelles. En voici quelques exemples :

- Le devoir de confidentialité du banquier-client ; [55]
- Les règles sur la confidentialité et la protection des informations personnelles des clients dans les règles de protection du consommateur de produits financiers ; 56
- L'obligation pour les demandeurs d'agréments de monnaie électronique de se conformer aux normes applicables en matière de sécurité et de confidentialité des données ; [57]
- L'obligation de garantir la confidentialité des informations sur les clients relatives aux instruments de paiement, y compris les informations en possession des agents ; [58]
- La capacité des systèmes de paiement et des prestataires de services de paiement à accéder aux données à caractère personnel, à les traiter et à les conserver (dans le cas de la DSP2 de l'UE, cela nécessite un consentement explicite, sous réserve d'exceptions telles que la détection des fraudes [59]) ; et
- Le droit des utilisateurs de services de paiement d'utiliser les services d'information sur les comptes (la DSP2 exige également un consentement explicite dans ce cas, ainsi que le respect d'autres conditions). [60]

CODES DE L'INDUSTRIE

Des codes de confidentialité des données peuvent être élaborés pour les services financiers, y compris les SFN. Dans les cadres réglementaires généraux de CD, il est des codes spécifiques à élaborer par des groupes sectoriels et/ou le régulateur de la protection des données. des exemples figurent dans les cadres DP de l'UE, de l'Australie, du Brésil, du Ghana, du Kenya, de la Malaisie, du Mexique, des Philippines et de l'Afrique du Sud.
Afrique. Toutefois, étant donné que ces lois pertinentes relatives à la confidentialité des données (CD) sont probablement assez récentes, les exemples de codes spécifiques aux services financiers sont rares. La Malaisie en est un exemple (voir encadré 12).

Les codes de bonnes pratiques générales du secteur financier peuvent également contenir des dispositions sur la confidentialité. Par exemple, le code bancaire philippin pour la protection du consommateur, qui a été élaboré par les différentes associations bancaires, traite des questions de confidentialité concernant la divulgation d'informations à des tiers non liés à des fins de marketing et d'activités de télémarketing par courrier électronique, appels téléphoniques et messages textes (section 2 (e)).
Un autre exemple est le code des pratiques bancaires de l'Afrique du Sud, qui prévoit des dispositions relatives à la confidentialité des informations personnelles (section 6.1).

ENCADRÉ 12 : MALAISIE : CODE DE PRATIQUE SUR LA PROTECTION DES DONNÉES PERSONNELLES POUR LE SECTEUR BANCAIRE ET FINANCIER (2017)

La loi malaisienne sur la protection des données personnelles prévoit l'enregistrement de " forums d'utilisateurs de données " qui peuvent ensuite élaborer un code de pratique obligatoire de leur propre initiative ou à la demande du commissaire à la protection des données personnelles (partie II, section 3). Le code sera enregistré si le commissaire estime qu'il est conforme à la loi et que les finalités du traitement des données ont été dument pris en compte par les utilisateurs de données concernés, les personnes concernées et à les autorités de régulation compétentes (telle que la Banque Centrale de Malaysie (BNM)), et que le code offre dans l'ensemble un niveau de protection adéquat. Toute infraction au code est passible d'une amende n'excédant pas 100 000 ringgit (environ 2 425[61] dollars américains) et/ou d'une peine d'emprisonnement pouvant aller jusqu'à un an.

53 https://www.privacy.gov.ph/2019/10/npc-shuts-down-26-online-lending-entreprises/

54 Par exemple, https://www.sec.gov.ph/pr-2020/sec-revokes-fcash-global-lendings-license/

55 Par exemple : Afghanistan : Loi bancaire (1974) et Philippines : Loi sur le secret des dépôts bancaires (1955)

56 Par exemple : Philippines : BSP Circular 857 - Regulation on Financial Consumer Protection (Chapitre II, section (b) Protection of Client Information)

57 Par exemple : Règlement de la Banque d'Indonésie sur la monnaie électronique (2018)

8 Par exemple : Inde : Reserve Bank of India - Master Direction on Issuance and Operation of Prepaid Payment Instruments (2017) et Ghana : Payments Systems and Services Act (2019)

59 Article 94

60 Article 67

61 À partir du 15 novembre 2020 - https://www.xe.com/currencyconverter/convert/?Amount=10%2C000&From=MYR&To=USD

ENCADRÉ 12 : *SUITE*

Le Code de pratique sur la protection des données personnelles pour le secteur bancaire et financier (2017) (Code BFS) est enregistré en vertu des dispositions susmentionnées. Le Code s'applique à toutes les banques et institutions financières agréées et a été élaboré par l'Association des banques de Malaisie. Le Code résume les dispositions pertinentes de la loi, les règlements connexes et les lignes directrices de la BNM en matière de transparence et de divulgation des produits, et fournit des exemples sectoriels de leur mise en application. L'accent est mis sur l'explication des définitions des données personnelles, sensibles et préexistantes et sur les règles concernant le marketing direct et la vente croisée, la prise de contact avec la personne concernée et le transfert de données à l'étranger. Des modèles sont également fournis pour un avis de confidentialité, un formulaire de demande d'accès aux données et un formulaire de demande de correction des données.

ORIENTATIONS POLITIQUES NATIONALES ET INTERNATIONALES

Les autorités nationales chargées de la protection des données fournissent des orientations politiques relatives à la DP4DFS. Par exemple, les sites web de la Commission nationale de protection de la confidentialité des Philippines [62] et de la Commission de protection des données du Ghana [63] fournissent des directives sur les droits et les responsabilités en vertu des lois pertinentes, sur les cas de violations signalés, comment formuler une réclamation et présenter des mises à jour sur l'exercice de leurs fonctions.

Le Ghana offre un rare exemple de cadre politique national spécifique aux SFN. L'encadré 13 décrit les sections pertinentes de la DP4DFS.

Les agences internationales fournissent également des directives sur les politiques réglementaires et questions relatives à la DP4DFS. Par exemple, les bonnes pratiques de la Banque mondiale en matière de protection des consommateurs des services financiers (2017) fournissent des orientations sur les questions de protection des données et de confidentialité applicables aux paiements de détail. Elles ont été élaborées en tenant compte de l'environnement " Big Data " et d'autres innovations liés à la FinTech. (voir annexe A, section D). En résumé, il est suggéré de mettre en place des cadres réglementaires applicables aux prestataires de services de paiement (PSP)qui :

- Autorisent les prestataires de services de paiement à collecter les données des clients dans les limites fixées par la loi ou par le consentement ;
- Établissent des règles pour la collecte et la conservation des données à caractère personnel ;
- Limitent l'utilisation des données à caractère personnel aux fins spécifiées au moment de la collecte, conformes à la loi ou expressément acceptées par le client ;
- Exiger des prestataires de services de paiement qu'ils assurent la confidentialité et la sécurité des

ENCADRÉ 13 : POLITIQUE EN MATIÈRE DE SERVICES FINANCIERS NUMÉRIQUES (2020) DU MINISTÈRE DES FINANCES DU GHANA

En mai 2020, le Ghana a lancé une politique quadriennale (2020-2023) en matière de SFN, que le CGAP considère comme la première au monde. Elle est conçue pour servir de modèle à la manière dont le Ghana peut tirer parti de la finance numérique pour atteindre ses objectifs d'inclusion financière, en complément de sa stratégie nationale d'inclusion financière et de développement. La confidentialité et la sécurité des données ont été jugées " particulièrement importantes " dans le contexte des SFN, avec le commentaire suivant : " Il existe manifestement des risques spécifiques aux SFN qui doivent être traités par le cadre de protection des données. " Les propositions spécifiques sur ce point étaient (en résumé) :

- Mettre des ressources supplémentaires à disposition de la Commission de protection des données (CPD) pour mener à bien le processus d'enregistrement des contrôleurs de données en vertu de la loi ghanéenne sur la protection des données (2012).
- Renforcer la capacité technique de la CPD par une formation sur les spécificités des données dans l'écosystème des SFN.
- Faciliter la coopération entre la CPD, les régulateurs financiers et l'Autorité nationale des communications par un protocole d'accord.
- Evaluer l' utilisation de données alternatives dans le secteur financier afin de déterminer s'il est nécessaire de prévoir des réglements supplémentaires.

- Rendre les PSP légalement responsables de l'utilisation abusive des données personnelles et de toute violation de la sécurité des données ;
- Interdire aux PSP de partager des données avec un tiers à quelque fin que ce soit (y compris le télémarketing ou le marketing direct) sans consentement écrit préalable, sauf si le tiers agit pour le compte du PSP et que les informations sont utilisées à des fins compatibles avec l'objectif initial de la collecte (à moins qu'une exception ne s'applique, telle qu'une obligation légale) ;
- permettre aux consommateurs de refuser de partager des données dont le partage a été autorisé précédemment ; et
- Élaborer des règles spécifiques pour les tiers tels que les autorités publiques, les registres de crédit et les agences de recouvrement.

D'autres organisations internationales ont également élaboré des orientations sur les bonnes pratiques relatives à la DP4DFS. Des exemples figurent à l'annexe 4.

62 https://www.privacy.gov.ph/
63 https://www.dataprotection.org.gh/

PRINCIPES DIRECTEURS POUR L'INTRODUCTION D'UN CADRE GLOBAL DE DP4DFS

Les principes directeurs sont destinés à servir comme orientations non contraignantes pour un cadre réglementaire global fondé sur le risque, proportionné pour la DP4DFS.

Le cadre a été élaboré en partant de l'hypothèse qu'il n'existe pas de loi générale sur la protection des données. Les principes reflètent les tendances émergentes de haut niveau en matière de droits et de responsabilités dans le domaine de la confidentialité. Toutefois, ils ne doivent pas être considérés comme des bonnes pratiques. Selon le contexte national, en particulier, il est nécessaire que les dispositions réglementaires soient plus ou moins détaillées que celles proposées et qu'elles fassent l'objet de réserves et d'exceptions. Enfin, bien que les principes directeurs aient été élaborés en tenant compte spécifiquement du traitement des données dans le contexte des SFN, ils peuvent être plus généralement pertinents, y compris en ce qui concerne les services financiers traditionnels.

Les principes directeurs peuvent être mis en œuvre de différentes manières. Elles comprennent :

- Une nouvelle loi ;
- les règlements adoptés ou les orientations données aux fins d'une loi existante sur le secteur financier ; ou
- Un code de pratique obligatoire à élaborer par les associations sectorielles et/ou les régulateurs concernés.

La pertinence des principes directeurs pour un pays donné dépendra de plusieurs facteurs. Il peut s'agir des risques identifiés en matière de confidentialité, du cadre juridique et réglementaire existant, des priorités politiques, du mandat et des pouvoirs des régulateurs, de la capacité de contrôle et des ressources, et de l'existence d'associations sectorielles susceptibles de soutenir efficacement l'élaboration, la mise en œuvre et l'application d'un code de bonnes pratiques.

L'option privilégiée doit faire l'objet d'une consultation des parties prenantes des secteurs public et privé, et du public en général. Il peut s'agir d'une consultation
avec les ministères et les régulateurs financiers, ceux du secteur des télécommunications, de la concurrence, de la protection du consommateur et de l'innovation en général. Il convient également de consulter le secteur privé (y compris les fournisseurs de SFN traditionnels et de la FinTech) et les acteurs de la société civile (tels que les groupes de consommateurs).

Des initiatives régionales en matière de protection des données personnelles peuvent également être prises en compte. Comme indiqué dans le cadre politique de l'AIF pour un crédit numérique responsable (2020), " lorsque cela est possible, les initiatives régionales transfrontalières peuvent renforcer la confiance entre les pays, faciliter le partage des meilleures pratiques entre les décideurs politiques et permettre aux régulateurs de la confidentialité des données de détecter et de traiter plus facilement les cas de non-conformité " (principe 6).

Une proposition a été incluse à la fin des lignes directrices pour un régime DP4DFS " minimaliste " basé sur le risque et proportionné, qui sera supervisé par le principal régulateur financier (tel que la Banque centrale). La présente proposition suggère des priorités provisoires en partant de l'hypothèse que la capacité et les ressources de surveillance
qui peuvent être appliquées à la DP4DFS sont limitées et qu'il n'existe également pas de loi générale sur la protection des données.

LES PRINCIPES DIRECTEURS ÉNONCÉS CI-DESSOUS SONT ORGANISÉS EN SIX PILIERS.

Ils comprennent des recommandations clés pour chaque pilier. Le cas échéant, les recommandations clés sont organisées sur la base du principe selon lequel celles qui sont considérées comme les plus faciles pour la mise en œuvre doivent être prioritaires.

PILIER 1 : POLITIQUE DE LA DP4DFS ET CADRE RÉGLEMENTAIRE

PILIER 2 : CONTRÔLEUR ET PROCESSEUR DES DONNÉES OBLIGATIONS

PILIER 3 : DROITS DES PERSONNES CONCERNÉES

PILIER 4 : SENSIBILISATION DES CONSOMMATEURS ET RECOURS

PILIER 5 : SUPERVISION ET APPLICATION

PILIER 6 : DP4DFS DANS LES SITUATIONS D'URGENCE MONDIALES ET NATIONALES

PILIER 1 : CADRE RÉGLEMENTAIRE ET POLITIQUE DE DP4DFS

Ce pilier est destiné à couvrir le processus de mise en place du cadre réglementaire et politique de DP4DFS et les principes qui s'y rapportent.

1.1. PRINCIPE DIRECTEUR : METTRE EN PLACE DES MÉCANISMES DE GOUVERNANCE ET DE CONSULTATION

RECOMMANDATIONS CLÉS :

> Établir un comité de pilotage avec le régulateur principal de la DP4DFS et des représentants des autres régulateurs financiers et des autres ministères et agences publiques pertinents (par exemple, pour la finance / les télécommunications / la concurrence / la protection du consommateur / l'innovation), ainsi que des représentants de l'industrie (y compris le secteur financier traditionnel et les entités FinTech) et des consommateurs (par exemple, les associations de consommateurs).

> Veiller à ce que les représentants du comité directeur disposent de, ou qu'ils y aient accès à, une expertise couvrant les SFN, les questions de confidentialité des données et les innovations FinTech en matière de traitement des données pour les SFN.

> Recruter des experts externes si nécessaire, par exemple des scientifiques des données ou des experts en matière de confidentialité des données.

> Mener des vastes consultations sur le nouveau cadre auprès des intervenants des secteurs public et privé et du grand public.

1.2. PRINCIPE DIRECTEUR : ÉVALUER LE CADRE JURIDIQUE ET RÉGLEMENTAIRE ACTUEL DES SFN ET LE MARCHÉ

RECOMMANDATIONS CLÉS :

> Entreprendre une analyse diagnostique du cadre juridique et réglementaire existant applicable à la DP4DFS, y compris :
- les lois générales sur la confidentialité des données et la protection du consommateur
- les lois sur la protection du consommateur de produits financiers
- les dispositions sectorielles spécifiques, par exemple dans les lois sur la monnaie électronique et les paiements
- les codes de pratique de l'industrie
- les stratégies nationales (par exemple, pour les SFN, le développement du secteur financier ou l'inclusion financière)
- les lignes directives politiques et réglementaires

> Évaluer les lacunes/chevauchements dans le cadre réglementaire et le mandat et les pouvoirs de surveillance connexes en se référant aux principes directeurs.

> Examiner le marché des SFN et les risques liés à la confidentialité des données, y compris les types de fournisseurs, de contrôleurs et de processeurs de données personnelles, les produits des SFN, les formes de consentement, les politiques de confidentialité, les types de données et les techniques d'analyse des données utilisées, ainsi que les questions spécifiques à la FinTech.

> Prendre en compte les besoins des groupes vulnérables, tels que les femmes, la jeunesse, les personnes âgées, les personnes handicapées et les personnes déplacées.

> Évaluer les problèmes systémiques liés aux réclamations concernant la DP4DFS.

> Documenter les principaux avantages et risques de l'environnement actuel pour les principaux intervenants (en particulier les intéressés et les contrôleurs et processeurs de données).

1.3. PRINCIPE DIRECTEUR : ÉTABLIR DES PRINCIPES POLITIQUES ET RÉGLEMENTAIRES GÉNÉRAUX

RECOMMANDATIONS CLÉS :

> Clarifier les principes réglementaires pour guider la conception du cadre de la DP4DFS.

> Envisager en particulier des règles fondées sur le risque et proportionnées, qui assurent un équilibre entre la vie privée, la protection des données, l'innovation, la concurrence et l'équité et qui sont :
- claires et accessibles
- fondées sur des principes
- neutres sur le plan technologique
- axées sur les résultats

> Exiger que le nouveau cadre soit basé sur l'activité afin de créer des conditions de concurrence équitables et de minimiser le risque d'arbitrage réglementaire (sous réserve des points suivants).

> Déterminer si certaines obligations doivent s'appliquer uniquement qu'aux contrôleurs de données " importants ", telles que les obligations concernant :
- L' inscription
- La désignation d'un délégué à la protection des données
- La préparation d'une évaluation l'impact sur la confidentialité pour les opérations de traitement à haut risque
- La notification des violations aux régulateurs et aux personnes concernées
- Le évaluations indépendantes de la conformité

> Si certaines règles ne s'appliquent qu'aux contrôleurs de données " importants ", il convient d'établir des critères pour les définir, par exemple :
- Nature des produits ou du modèle d'affaires des SFN.
- Volume et sensibilité des données traitées.

- Nombre de personnes concernées.
- Rotation.
- Risque de préjudice pour les personnes concernées, par exemple sur la base d'une discrimination ou d'un préjugé.
- Utilisation de nouvelles technologies pour le traitement des données, telles que le traitement automatisé et le profilage.

1.4. PRINCIPE DIRECTEUR : ÉLABORER UN CADRE JURIDIQUE POUR LA DP4DFS

RECOMMANDATIONS CLÉS :

> Tenir compte des bonnes pratiques régionales/internationales pertinentes pour la DP4DFS.

> Appliquer le cadre aux entités publiques et privées.

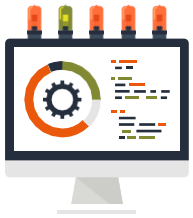
> Établir des définitions et des concepts clés (voir les suggestions à l'annexe 3).

> Tenir compte des exceptions qui peuvent s'appliquer, par exemple pour les données couvertes par d'autres lois telles que les rapports de crédit ou le recouvrement de dettes, pour le traitement de données autorisé ou exigé par une autre loi ou lorsqu'il existe des considérations impérieuses telles que la sécurité nationale.

> Prévoir une période de transition pour permettre à l'industrie de modifier les processus, les procédures et les systèmes informatiques et de sensibiliser le public.

> Mener une campagne de sensibilisation du public sur le nouveau cadre DP4DFS et sur les droits et responsabilités qui y sont associés.

PILIER 2 : OBLIGATIONS DU CONTRÔLEUR ET DU PROCESSEUR DE DONNÉES



Ce pilier propose des suggestions concernant les principales obligations à imposer aux contrôleur et processeurs des données, y compris les principes clés du traitement des données.

2.1 PRINCIPE DIRECTEUR : EXIGER DES DISPOSITIONS EFFICACES EN MATIÈRE DE GOUVERNANCE INTERNE DE DP4DFS

RECOMMANDATIONS CLÉS :

- Exiger que les contrôleurs des données :
  - Veillent à ce que les employés et les agents soient formés et conscients des règles du DP4DFS
  - Élaborent et maintiennent des politiques et des procédures documentées conformes aux règles du DP4DFS
  - Assurent la surveillance par la direction générale/le conseil d'administration de la conformité du DP4DFS
  - Disposent de systèmes et de ressources technologiques et organisationnels adéquats

> Exigent que la fonction d'audit interne vérifie le respect de toutes les règles de la DP4DFS.

> Exigent une évaluation indépendante annuelle de la conformité aux règles de la DP4DFS.

2.2 PRINCIPE DIRECTEUR : ÉLABORER DES PRINCIPES GÉNÉRAUX DE TRAITEMENT DES DONNÉES

RECOMMANDATIONS CLÉS :

> Assurer la mise en œuvre de principes proactifs de protection de la confidentialité dès la conception (Privacy by Design) sur une politique approuvée et contrôlée par l'organe directeur de l'entité concernée et publiée sur son site web et éventuellement sur celui de l'autorité chargée de la protection des données.[64]

> Définir l'obligation générale de s'assurer que le traitement est toujours (indépendamment du consentement) équitable, légitime et transparent.

> Établir d'autres principes relatifs au traitement des données, notamment :
  - Limitation du traitement : exiger que le traitement soit effectué avec le consentement de l'intéressé, sauf s'il est strictement nécessaire aux fins des SDF

64 Voir également le Groupe de la Banque mondiale. Identification numérique et défi de la protection des données : Note du praticien. 2019

contrat ou comme requis ou autorisé par la loi

- Minimisation des données : exiger que les données soient limitées aux finalités du traitement
- Exactitude : exiger que les données soient exactes et à jour et qu'elles soient corrigées ou effacées si ce n'est pas le cas
- Limitation de la conservation : exiger que les informations ne soient conservées que pour une durée compatible avec la finalité du traitement
- Registres : exiger que des registres de toutes les activités de traitement soient conservés
- Sécurité : exiger que le traitement soit effectué de manière à réduire au minimum le risque de traitement non autorisé ou illégal et de perte ou de détérioration accidentelle

> Exiger que des évaluations documentées des impacts la vie privée, fondées sur les risques, soient réalisées pour les activités de traitement susceptibles de présenter un risque élevé pour la vie privée des personnes concernées, compte tenu notamment de :
  - L'utilisation des nouvelles technologies
  - De la nature, de l'ampleur et des finalités du traitement des données
  - Des capacités et besoins des personnes concernées et en particulier les groupes vulnérables

> Inclure l'obligation spécifique de veiller à ce que les processus et les technologies connexes n'aboutissent pas à des décisions discriminatoires ou partiales et mettre la charge de la preuve sur le contrôleur de données/traiteur pour prouver qu'il n'y a pas eu de violation de cette obligation.

2.3 PRINCIPE DIRECTEUR : CRÉER UN MODÈLE DE CONSENTEMENT ÉCLAIRÉ ET EFFICACE

RECOMMANDATIONS CLÉS :

> Évaluer les obstacles locaux à l'obtention d'un consentement effectif, en tenant compte notamment des besoins des groupes vulnérables (par exemple, pour les consentements verbaux, l'utilisation des langues locales, l'accès aux formes numériques de consentement et la connaissance en finance)

> Exiger que tous les consentements :
  - Soient donnés librement, en connaissance de cause et sans ambiguïté
  - Soient formulés en termes simples et clairs et être aussi brefs que possible
  - Soient donnés à des fins spécifiques
  - Ne soient pas regroupés (en particulier, le consentement au traitement pour les services financiers numériques doit être séparé du consentement pour d'autres finalités)
  - Soient " opt-in " plutôt que " opt-out " (la valeur par défaut doit être " opt-out ")
  - Soient séparées des autres informations, par exemple les conditions générales de vente
  - Soient limités dans le temps
  - Puissent être retirés, le retrait étant aussi facile que l'octroi du consentement
  - Puissent être conservés pour référence ultérieure

> Appliquent les mêmes règles de consentement à tous les types de données (sensibles ou non).

> Élaborent des règlements/fournissent des lignes directrices sur la signification pratique de chaque élément des règles de consentement pour les SFN, avec des exemples.

> Prévoir qu'il incombe au contrôleur ou processeur des données de prouver le consentement.

2.4 PRINCIPE DIRECTEUR : EXIGER UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES LE CAS ÉCHÉANT

RECOMMANDATIONS CLÉS :

> Exiger la désignation d'un délégué à la protection des données indépendant et doté de ressources appropriées, lorsque la nature, la portée, le contexte et les finalités des activités de traitement sont suffisamment importants et/ou significatifs.

> Préciser les fonctions du délégué à la protection des données, par exemple :
  - Donner des orientations sur les règles du DP4DFS
  - Contrôler la conformité
  - Point focal pour les personnes concernées ayant des questions ou des réclamations à formuler
  - Point focal pour l'autorité chargée de la protection des données et les autres régulateurs
  - Faciliter le renforcement des capacités du personnel et des agents
  - Évaluations de l'impact sur la vie privée

PILIER 3 : DROITS DES PERSONNES CONCERNÉES

Ce pilier définit les principaux droits qui peuvent être accordés aux personnes concernées.

3.1 PRINCIPE DIRECTEUR : ÉTABLIR LES DROITS FONDAMENTAUX DES PERSONNES CONCERNÉES

RECOMMANDATIONS CLÉS :

- Droit à l'information sur les processeurs / contrôleurs des données concernés
- Droit à l'anonymat
- Droit d'accès
- Droit de rectification/correction
- Droit à l'effacement/droit à l'oubli
- Droit de restreindre le traitement ou de s'y opposer
- Droit à la portabilité des données
- Droit de ne pas faire l'objet d'une décision fondée uniquement sur un traitement de données automatisé (par exemple, à l'aide d'algorithmes et/ou de l'apprentissage automatique), y compris le profilage autrement qu'avec un consentement explicite ou si la loi l'autorise

3.2 PRINCIPE DIRECTEUR : PRÉCISER COMMENT LES DROITS PEUVENT ÊTRE EXERCÉS PAR LES PERSONNES CONCERNÉES

RECOMMANDATIONS CLÉS :

- Inclure des dispositions expliquant comment les droits peuvent être exercés par les personnes concernées; par exemple
  les processus applicables, les délais de réponse, les modèles, les droits de recours.

PILIER 4 : SENSIBILISATION DES CONSOMMATEURS ET RECOURS

Ce pilier couvre des propositions relatives aux systèmes internes et externes de réclamation et de règlement des litiges, aux droits de recours des personnes concernées et aux programmes de sensibilisation du public.

4.1 PRINCIPE DIRECTEUR : EXIGER DES PROCÉDURES INTERNES EFFICACES POUR LE TRAITEMENT DES RÉCLAMATIONS

RECOMMANDATIONS CLÉS :

- Exiger des contrôleurs et des processeurs des données qu'ils disposent de procédures documentées, transparentes, gratuites et efficaces pour le règlement des réclamations couvrant par exemple ; le règlement rapide des réclamations ; divers canaux pour déposer des réclamations ; et la publicité concernant les traitements des réclamations.

4.2 PRINCIPE DIRECTEUR : PRÉVOIR UN MÉCANISME EXTERNE DE RÉSOLUTION DES LITIGES POUR LES PERSONNES CONCERNÉES

RECOMMANDATIONS CLÉS :

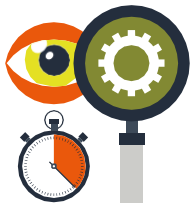
- Confier à un organisme externe (tel que l'autorité de protection des données, l'autorité de surveillance du secteur financier ou un organisme de médiation) (EDR) le pouvoir de traiter les litiges concernant le DP4DFS
- Permettre au EDR d'engager une enquête ou une action en justice au nom des personnes concernées (y compris un groupe), de sa propre initiative ou à la demande des personnes concernées.
- S'assurer que le EDR a le pouvoir de :
  - prendre des décisions contraignantes
  - d'accorder une indemnité
  - d' ordonner la correction des données
- Obliger l'EDR à rendre publiques les décisions relatives aux litiges.

4.4 PRINCIPE DIRECTEUR : PRENDRE EN COMPTE LA NÉCESSITÉ DE PROGRAMMES DE SENSIBILISATION DU PUBLIC

RECOMMANDATIONS CLÉS :

- Encourager les fournisseurs des SFN à promouvoir la sensibilisation aux questions de confidentialité des données, y compris les droits des personnes concernées et les principaux risques (par exemple, en ce qui concerne le vol d'identité et la fraude).
- Envisager le lancement d'une campagne de sensibilisation spécifique pour couvrir les droits et les responsabilités dans le nouveau cadre du DP4DFS.
- Prendre en compte les questions de confidentialité des données et les besoins spécifiques des groupes vulnérables dans les programmes d'éducation financière.

PILIER 5 : SUPERVISION ET APPLICATION



Ce pilier couvre une série de questions importantes relatives à la surveillance et à l'application, notamment la supervision basée sur les risques, le mandat, les pouvoirs, les capacités et les ressources de la surveillance, la nécessité de consultation et coordination permanentes, l'établissement d'une menace crédible d'application et la prise en compte de la confidentialité des données dans un environnement de bac à sable réglementaire.

5.1 PRINCIPE DIRECTEUR : ADOPTER UNE APPROCHE DE SUPERVISION BASÉE SUR LES RISQUES ET PROPORTIONNÉE

RECOMMANDATIONS CLÉS :

- Superviser les règles du DP4DFS sur une base du risque lié à l'entreprise et au marché.
- Élaborer une méthode d'évaluation des risques d'atteinte à la confidentialité dans les modèles d'affaires des SFN, par exemple en ce qui concerne les sources d'information, la sensibilité des informations, les cas d'utilisation et l'inter-connectivité des systèmes.

5.2 PRINCIPE DIRECTEUR : VEILLER À CE QUE LES AUTORITÉS DE SURVEILLANCE DISPOSENT D'UN MANDAT, DE POUVOIRS, DE CAPACITÉS, ET DE RESSOURCES EFFICACES

RECOMMANDATIONS CLÉS :

- Donner aux superviseurs un mandat clair en matière de DP4DFS.
- Veiller à ce que le superviseur disposer des pouvoirs appropriés, par exemple pour superviser, évaluer l'utilisation des technologies liées à la FinTech ou exiger des preuves de leur utilisation, infliger des amendes, accorder des dérogations, ordonner l'interdiction ou la suspension des pratiques de traitement des SFN, enregistrer ou annuler les contrôleurs de données et traiter les réclamations.
- Veiller à ce que le superviseur dispose des capacités et des ressources organisationnelles et technologiques nécessaires pour concevoir, mettre en œuvre et superviser le DP4DFS aujourd'hui et à l'avenir, en tenant compte des évolutions probables de la FinTech.
- Tenir compte de l'environnement actuel et des développements futurs probables, par exemple le système bancaire ouvert.

5.3 PRINCIPE DIRECTEUR : ÉTABLIR UN CADRE CLAIR DE CONSULTATION ET DE COORDINATION

RECOMMANDATIONS CLÉS :

- Assurer une consultation et une coordination permanentes avec les acteurs du secteur public sur les questions politiques et réglementaires, les innovations de la FinTech et les questions systémiques de DP4DFS.
- Mettre en place un mécanisme de consultation avec les groupes du secteur des SFN et de la société civile (par exemple, les défenseurs de la confidentialité et les associations de consommateurs).
- Déterminer s'il est souhaitable de créer un groupe consultatif de l'industrie[65]
- Établir des protocoles d'accord avec les principaux régulateurs et agences publiques.
- Envisager des initiatives régionales en matière de confidentialité des données.

5.4 PRINCIPE DIRECTEUR : PRENDRE EN COMPTE LES PROBLÈMES DE DP4DFS DANS LES ENVIRONNEMENTS RÉGLEMENTAIRES DE BAC À SABLE

RECOMMANDATIONS CLÉS :

- Tenir compte des questions relatives à la confidentialité des données lors de l'expérimentation d'innovations en matière de SFN dans des bacs à sable réglementaires.
- Envisager des " bacs à sable " réglementaires thématiques spécifiquement destinés aux innovations de DP4DFS.

5.5 PRINCIPE DIRECTEUR : ASSURER UNE MENACE CRÉDIBLE D'APPLICATION

RECOMMANDATIONS CLÉS :

- Veiller à ce que les sanctions soient suffisamment importantes pour être efficaces.
- Publier toutes les mesures d'application.
- Exiger la notification des violations importantes aux régulateurs et aux personnes concernées.
- Envisager de prendre des dispositions pour fixer des amendes correspondant à un pourcentage des bénéfices ou de la rotation et/ou à un montant forfaitaire déterminé.
- Envisager de fixer les amendes sur la base de la gravité des infractions.

65 Voir, par exemple, le Comité consultatif sur la protection des données personnelles de la Malaisie

PILIER 6 : DP4DFS DANS LES URGENCES MONDIALES ET NATIONALES

Ce pilier contient des recommandations sur la manière de traiter les questions relatives à la DP4DFS en cas d'urgence, telles que le COVID-19, mais également de manière plus générale.

6.1 PRINCIPE DIRECTEUR : FOURNIR DES ORIENTATIONS POLITIQUES SUR L'APPLICATION DU DP4DFS DANS LES SITUATIONS D'URGENCE

RECOMMANDATIONS CLÉS :

- Envisager des orientations réglementaires pour les contrôleur/processeurs des données sur les défis et les attentes spécifiques en matière de confidentialité.
- Assurer la coopération entre les régulateurs financiers et les autorités chargées de la protection des données.
- Tenir compte des défis posés par le DP4DFS dans les organes de coordination national.

6.2 PRINCIPE DIRECTEUR : VEILLER À CE QUE LE CADRE JURIDIQUE DU DP4DFS PRÉVOIE DES CLAUSES POUR LES SITUATIONS D'URGENCE

RECOMMANDATIONS CLÉS :

- Envisager de prendre des dispositions permettant de déroger aux règles du DP4DFS en cas d'urgence.
- Si des mesures n'existent pas actuellement, envisager une modification de la loi.

6.3 PRINCIPE DIRECTEUR : FAIRE PREUVE D'UNE SOUPLESSE APPROPRIÉE EN CE QUI CONCERNE L'APPLICATION DANS LES CAS APPROPRIÉS

RECOMMANDATIONS CLÉS :

- Envisager d'accorder aux entités du secteur public et du secteur privé un allègement réglementaire des lois existantes sur la confidentialité des données et de l'identité pour les besoins de l'urgence.
- Veiller à ce que les secours fournis soient :
  - Proportionnés aux risques
  - Clairs
  - Transparents pour le public
  - Spécifiques quant aux objectifs
  - De durée - limitée à la période de crise
- Définir clairement l'obligation de rendre compte des régulateurs qui fournissent des secours.
- Interdire le partage des données avec des tiers, sauf dans les cas où cela est explicitement autorisé.
- Encourager l'industrie à collaborer avec les autorités publiques, les autorités chargées de la protection des données et les autorités de surveillance du secteur financier sur les questions relatives à la DP4DFS.

APPROCHE DE DP4DS MINIMALISTE POUR LES RÉGULATEURS FINANCIERS

Cette proposition contient des suggestions relatives aux mesures minimales que les régulateurs financiers peuvent prendre dans la période intérimaire avant la mise en place d'une loi globale sur la protection des données.

1. EFFECTUER UNE ÉVALUATION DE HAUT NIVEAU DU MARCHÉ DES SFN ET DES RISQUES LIÉS À LA CONFIDENTIALITÉ DES DONNÉES

- Couvrir les secteurs public et privé, y compris les produits, les fournisseurs (traditionnels et basés sur la FinTech), les canaux de distribution, les segments de clientèle, les types de données utilisées et les outils d'analyse.
- Élaborer une méthode d'évaluation des risques liés à la confidentialité dans les modèles d'affaires des SFN, par exemple en ce qui concerne les sources d'information, la sensibilité de l'information, les cas d'utilisation et l'inter-connectivité des systèmes.
- Prendre en compte en particulier les besoins des groupes vulnérables.
- Prendre en compte les objectifs d'inclusion financière.

2. ÉTABLIR UN MÉCANISME DE CONSULTATION POUR LES NOUVELLES RÈGLES DE DP4DFS

Associer des représentants du secteur public et privé et de la société civile et veiller à ce que les entités traditionnelles et de la FinTech soient consultées.

3. ÉTABLIR DES CRITÈRES FONDÉS SUR LE RISQUE POUR DÉFINIR LES CONTRÔLEURS DE DONNÉES DES SFN " IMPORTANTS "

Ces critères peuvent couvrir, par exemple :

- Le volume et la sensibilité des données traitées
- Le nombre de personnes concernées
- La rotation
- Le risque de préjudice pour les personnes concernées, par exemple sur la base d'une discrimination ou d'un préjugé
- L' utilisation de nouvelles technologies pour le traitement des données, telles que le traitement automatisé et le profilage

4. ÉLABORER DE NOUVELLES RÈGLES DP4DFS

Les règles de priorité basées sur le risque peuvent couvrir :

- La confidentialité dès la conception et la gouvernance par défaut et les dispositions relatives aux ressources
- Des informations transparentes sur le traitement des données pour les personnes concernées
- Le consentement effectif et éclairé
- Les droits d'accès, de rectification et d'opposition au traitement
- Le recours pour les personnes concernées ayant déposé une réclamation (par exemple, en ce qui concerne l'indemnisation ou la correction des données)

5. PRENDRE ÉGALEMENT EN COMPTE LES RÈGLES RELATIVES À LA NOTION DE " SIGNIFICATIF " LES CONTRÔLEURS ET PROCESSEURS DES DONNÉES

Les règles peuvent couvrir, par exemple, les besoins d'enregistrement, le délégué à la protection des données, les évaluations d' impact de confidentialité, la notification des violations aux régulateurs et aux personnes concernées, et les évaluations indépendantes de la conformité.

6. SENSIBILISER LES CONSOMMATEURS AU DP4DFS

Mettre l'accent sur les divers besoins des groupes vulnérables, sur l'éducation aux risques liés à la confidentialité dans le cadre des SFN, ainsi que sur les droits et responsabilités connexes.

7. MAINTENIR DES ACCORDS DE COOPÉRATION PERMANENTE AVEC LES PRINCIPALES PARTIES PRENANTES

Par exemple : les principaux Ministères et régulateurs, les FinTech et les contrôleurs de données traditionnels des SFN et les associations de consommateurs.

ABRÉVIATIONS ET ACRONYMES

Droits de l'ACRO	Droits d' accès, de recertification, d'annulation, et d'opposition
AIF	Alliance pour l'inclusion financière
LBC/FT	Lutte contre le blanchiment d'argent et le financement du terrorisme
BTCA	Better Than Cash Alliance
CEMCWG	Protection des consommateurs et Groupe de travail sur la conduite de marché
CFI	Centre pour l'inclusion financière
CGAP	Groupe consultatif d'assistance aux pauvres
DP	Protection des données
DPA	Autorité de protection des données
DP4DFS	Confidentialité des données pour les services financiers numériques
SFN	Services financiers numériques
DFSWG	Groupe de travail sur les services financiers numériques
DPO	Responsable de la protection des données
G2P	De l'État à la personne
GDPR / Règlement général sur la protection des données	Règlement de l'UE 2016/79 relatif à la protection des personnes physiques à par rapport au traitement des données à caractère personnel et à la libre circulation de ces données
OCDE	Organisation de coopération et de développement économiques
DSP2	Directive 2015/2366 de l'UE sur les services de paiement sur le marché intérieur
WB	Groupe de la Banque mondiale

ANNEXE 1. LISTE DES ORGANISMES INTERROGÉS DANS LE CADRE DU PROJET

PAYS / RÉGION	ORGANISME	NOM	POSITION
GLOBAL	CFI	Mayada El Zohghbi	Directeur général
		Alexandra Rizzi	Directeur principal et responsable de la protection des données
GLOBAL	CRIF	Davide M. Meo	Directeur des marchés internationaux
		Valeria Racemoli	Spécialiste principal de la régulation
GLOBAL	CGAP	David Medine	Consultant
GLOBAL	CGAP	Ivo Jenik	Spécialiste du secteur financier
GLOBAL	GSMA	Brian Muthiora	Directeur de la réglementation, Afrique
GLOBAL	Vodacom	Judith Obholzer	Directeur général Politiques publiques
		Mpumi Simelane	Responsable de la protection de la vie privée du groupe
GLOBAL	Crédit à l'habitat	Lucas Frohlich	Gestionnaire juridique principal
		Vit Papousek	Responsable des affaires extérieures
AUSTRALIE	Université de New South Wales	Dr Katherine Kemp	Maître de conférences Faculté de droit
GHANA	Commission de la protection des données	Patricia Adusei-Poku	Directeur exécutif / Commissaire Commission de la protection des données
PHILIPPINES	Commission de la protection des données	Ivy Grace Villasoto et autres	Directeur, Bureau de la politique de confidentialité
	Bangko Sentral ng Pilipinas	Ellen Joyce Suficiencia et autres	Directeur, Centre pour l'inclusion et la stratégie de l'apprentissage

ANNEXE 2.
PRINCIPAUX CADRES RÉGLEMENTAIRES ANALYSÉS

PAYS	PRINCIPAUX CADRES RÉGLEMENTAIRES
AUSTRALIE	Loi sur la protection de la confidentialité (1988)
BRÉSIL	Loi sur la protection des données personnelles (2018)
L'UE	Règlement général sur la protection des données (2016)
GHANA	Loi sur la protection des données (2012)
INDE	Projet de loi sur la protection des données personnelles (2019) RBI Non - Banking Financial Company Account Aggregator Master Direction (2016) (mise à jour au 22 novembre 2019)
KENYA	Loi sur la protection des données (2019)
MALAISIE	Loi sur la protection des données personnelles (2010) Code de pratique sur la protection des données personnelles pour le secteur bancaire et financier (2017)
MEXIQUE	Loi fédérale sur la protection des données personnelles détenues par des personnes privées (2010) et règlements (2012)
PÉROU	Loi sur la protection des données personnelles (2011) et règlements (2013)
PHILIPPINES	Loi sur la protection des données (2012) et règles et règlements d'application Circulaire NPC n° 20-01 Lignes directrices sur le traitement des données personnelles pour les transactions liées aux prêts (2020)
AFRIQUE DU SUD	Loi sur la protection des informations personnelles (2013)

ANNEXE 3.
CONCEPTS CLÉS ET DÉFINITIONS

CONCEPT	DÉFINITION
CONTRÔLEUR	Une personne physique ou morale ou une autorité publique qui, seule ou conjointement avec d'autres, détermine la finalité ou la méthode de traitement des données à caractère personnel.
PERSONNE CONCERNÉE	Une personne dont les données personnelles sont ou peuvent être traitées.
FINTECH	L'application de la technologie à la finance (en bref, la "technologie financière").[66]
ID	Moyen officiel d'identification d'une personne.
SYSTEME BANCAIRE OUVERT	Les systèmes de partage de données basés sur le consentement du client lorsque les données sont partagées par les institutions financières avec des tiers (tels que d'autres institutions financières, des prestataires de services de paiement, des agrégateurs de données et des partenaires commerciaux).
DONNÉES PERSONNELLES	Les informations ou opinions relatives à une personne identifiée ou identifiable, qu'elle soit vraie ou non, conservée sous une forme matérielle ou non et automatisée ou non.
PROCESSEUR	Une personne physique ou morale ou une autorité publique qui traite des données à caractère personnel pour le compte du contrôleur.
TRAITEMENT	Toute opération effectuée en relation avec des données à caractère personnel, manuellement ou automatiquement, y compris la collecte, l'utilisation, la divulgation, le stockage, l'enregistrement, l'effacement ou autre, et les termes " traite ", " traité " et autres termes similaires ont une signification similaire, mais à l'exclusion du traitement : • exigé pour des activités déterminées (telles qu'une fonction judiciaire, l'application d'une réclamation, la sécurité nationale ou une préoccupation purement domestique ou ménagère) ; ou • à des fins requises ou autorisées par la loi.
PROFILAGE	Forme de traitement qui analyse, évalue ou prédit les aspects personnels d'une personne, y compris (sans s'y limiter) son comportement, ses attributs, ses préférences ou ses caractéristiques.
INFORMATIONS SENSIBLES	Informations ou opinions concernant les données financières, les données biométriques, l'identifiant officiel, les croyances ou l'affiliation religieuse, politique ou philosophique, l'appartenance à un syndicat, la race, l'appartenance ethnique, la caste, la santé et l'identité sexuelle d'une personne.
LES GROUPES VULNÉRABLES	Les personnes qui peuvent être particulièrement vulnérables dans le contexte du DP4DFS, telles que les femmes, la jeunesse, les personnes âgées, les personnes handicapées et les personnes déplacées.

66 Banque des règlements internationaux (BRI) Comité de Bâle sur le contrôle bancaire : Rapport sur l'Open Banking et les interfaces de programmation d'applications (2019) (Notes de bas de page 1 et 2)

ANNEXE 4. BONNES PRATIQUES INTERNATIONALES POUR LE DP4DFS

Les organisations internationales ont élaboré des orientations sur les bonnes pratiques en matière de DP4DFS.

En voici quelques exemples :

- **Banque mondiale :** Good Practices for Financial Consumer Protection (2017) (voir annexe A, section D)
- **Alliance Better Than Cash :** Responsible Digital Payments Guidelines (2016) (voir ligne directrice 7)
- **G20 :** Principes de haut niveau pour l'inclusion financière numérique (2016) (voir principes 2 et 5)
- **GSMA :** Guidelines on Mobile Money Data Protection (2018). Voir également GSMA : Data Protection in Mobile Money (2019) et GSMA : Smart Data Privacy Laws. Obtenir les bons résultats à l'ère numérique (2019)
- **OCDE (2020) :** L'utilisation des données personnelles dans les services financiers et le rôle de l'éducation financière : Une analyse centrée sur le consommateur (2020)

ANNEXE 5. RÉFÉRENCES

PRODUITS INFORMATIQUES DE L'AIF

AIF : Rapport spécial sur la création d'écosystèmes FinTech favorables : Le rôle des régulateurs (2020) https:// www.afi-global.org/publications/3181/Creating- Enabling-FinTech-Ecosystems-The-Role-of-Regulators

AIF: Cadre stratégique pour l'utilisation des services financiers numériques en réponse aux urgences mondiales - Cas du COVID-19 (2020) https://www.afi-global.org/sites/ default/files/publications/2020-10/AFI_DFSWG_COVID_ PF_AW4_digital.pdf

AIF : Modèle de politique de protection des consommateurs pour les services financiers numériques (2020) https://www.afi-global.org/publications/3465/Policy-Model-on-Consumer-Protection-for-Digital-Financial-Services

AIF : Cadre politique pour un crédit numérique responsable (2020) https://www.afi-global.org/publications/3216/ Policy-Framework-for-Responsible-Digital-Credit

AIF : Modèle de politique pour la monnaie électronique (2019) https://www.afi-global.org/publications/3088/Policy-Model-for-E-Money

AIF : KYC Innovations, Financial Inclusion and Integrity In Selected AFI Member Countries (2019) https://www. afi-global.org/sites/default/files/publications/2019-03/ KYC-Innovations-Financial-Inclusion-Integrity-Selected- AFI-Member-Countries.pdf (en anglais).

AIF : Rapport spécial sur les FinTech pour l'inclusion financière : Un cadre pour la transformation financière numérique (2018) https://www.afi-global.org/publications/2844/
FinTech pour l'inclusion financière : un cadre pour la transformation financière numérique Transformation financière

Bases de données mondiales des lois sur la confidentialité et la protection des données DLA Piper Lois sur la protection des données dans le monde
https://www.dlapiperdataprotection.com/

CNUCED Législation en matière de protection des données et de la vie privée dans le monde
https://unctad.org/page/data-protection- and-privacy-legislation-worldwide

AUTRES PUBLICATIONS

Arner DW, Buckley RP, Zetzsche, DA et Veidt, R : Sustainability, FinTech and Financial Inclusion Eur Bus Org Law Rev 21, 7-35 (2020) https://doi.org/10.1007/s40804-020-00183-y.

Australie : Attorney - General's Department : Privacy Act Review Issues Paper (2020) https://www.ag.gov.au/integrity/publications/review-privacy-act-1988-cth-issues-paper

Banque des règlements internationaux (BRI) Comité de Bâle sur le contrôle bancaire : Rapport sur l'Open Banking et les interfaces de programmation d'applications (2019) https://www.bis.org/bcbs/publ/d486.htm

Alliance Better Than Cash : Responsible Digital Payments Guidelines (2016) https://www.betterthancash.org/tools-research/case-studies/responsible-digital-payments-guidelines

Carpenter v. United States 585 U.S. (2018) https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

Centre pour l'inclusion financière (CFI) et Institut de la finance internationale : Accelerating Financial Inclusion with New Data (2018) https://www.centerforfinancialinclusion.org/accelerating-financial-inclusion-financière-avec-nouvelles-données-2

CFI : Blog - Protection des données et inclusion financière : Why It Matters (Introduction) (2020)https://www.centerforfinancialinclusion.org/data-protection-and-financial-inclusion-why-it-matters-introduction

CFI : Blog - Consentement aux données : Partageons le fardeau pour une protection efficace des consommateurs (2020)https://www. centerforfinancialinclusion.org/data-consent-lets-share- the-burden-for-effective-consumer-protection

CFI : Blog - Des données pour une finance inclusive : Delivering on the Promise for Consumers (2020)https://www.centerforfinancialinclusion.org/data-for-inclusive-finance-delivering-on-the-promise-for-consumers

CGAP : Blog - Une tendance croissante dans la régulation financière : Thematic Sandboxes (2019)https://www.cgap.org/blog/ growing-trend-financial-regulation-thematic-sandboxes

CGAP : Note de synthèse - La confidentialité des données est-elle bonne pour les entreprises ? (2019)https://www.cgap.org/sites/default/files/publications/2019_12_Focus_Note_Is_Data_Privacy_Good_for_Business.pdf

CGAP : Making Data Work for the Poor : New Approaches to Data Protection and Privacy (2020)https://www.cgap.org/research/publication/making-data-work-poor

CGAP : Blog - Open Banking : 7 Ways Data-Sharing Can advance Financial inclusion (2020)https://www.cgap.org/blog/open-banking-7-ways-data-sharing-can-advance-financial-inclusion

CGAP : Blog - Blog Les préoccupations en matière de confidentialité des données influencent les comportements financiers en Inde et au Kenya (2020)https:// www.cgap.org/blog/data-privacy-concerns-influence- financial-behaviors-india-kenya

CGAP : Blog - Open Data and the Future of Banking (2019)https://www.cgap.org/blog/open-data-and-future-banking

Centre pour le leadership en matière de politique de l'information : Bacs à sable réglementaires en matière de protection des données : Constructive Engagement and Innovative Regulation in Practice (2019) https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/07/cipl_white_paper_on_regulatory_sandboxes_in_data_protection_-_constructive_engagement_and_innovative_regulation in_pratique__8_mars_2019_.pdf

Covington and Burlington LLP : Overlap between the GDPR and PSD2 Inside Privacy (2018) https://www.insideprivacy.com/financial-institutions/overlap-between-the-gdpr-and-psd2/

Deloitte : Une fois la poussière retombée. Comment les services financiers adoptent une approche durable de la conformité au GDPR dans une nouvelle ère pour la vie privée, un an après https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-the-impact-of-gdpr-on-the-financial-services.pdf

Contrôleur européen de la protection des données : Le guide rapide du CEPD sur la nécessité et la proportionnalité (2020) https://edps.europa.eu/data-protection/our-work/ publications/factsheets/edps-quick-guide-necessity- and-proportionality_en

Parlement européen : Questions parlementaires : Référence de la question : E-000054/2019 (10 mars 2019) https://www.europarl.europa.eu/doceo/document/E- 8-2019-000054-ASW_FR.html

Kemp K, Université de Nouvelle-Galles du Sud : Big Data, Financial Inclusion and Privacy for the Poor. Forum de la finance responsable (2017) https://responsiblefinanceforum. org/big-data-financial-inclusion-privacy-poor/

Kemp K ; Buckley RP, "Protecting Financial Consumer Data in Developing Countries : An Alternative to the Flawed Consent Model, Georgetown Journal of International Affairs, vol. 18, pp. 35 - 46 (2017) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3237856

Finextra : Blog de Carlo R.W. de Meijer Économiste et chercheur chez De Meijer Independent Financial Services Advisory (MIFSA) : Blockchain versus GDPR and who should adjust most (2018) https://www.finextra.com/blogposting/16102/blockchain-versus-gdpr-and-who-who-should-adjust-most.

G20 : Principes de haut niveau pour l'inclusion financière numérique (2016) https://www.gpfi.org/publications/g20-high- level-principles-digital-financial-inclusion

Orientations politiques du G20 et de l'OCDE : Approches en matière de protection des consommateurs de produits financiers : Financial Consumer Protection in the Digital Age (2018) https://www.oecd.org/ finance/G20-OECD-Policy-Guidance-Financial-Consumer- Protection-Digital-Age-2018.pdf

GSMA : The Impact of Data Localisation Requirements on the Growth of Mobile Money - Enabled Remittances (2018) https://www.gsma.com/mobilefordevelopment/ wp-content/uploads/2019/03/GSMA_Understanding- the-impact-of-data-localisation.pdf

GSMA : Guidelines on Mobile Money Data Protection (2018) https://www.gsma.com/mobilefordevelopment/ wp-content/uploads/2018/09/GSMA-Guidelines-on- mobile-money-data-protection.pdf

GSMA : Data Protection in Mobile Money (2019) https://www.gsma.com/mobilefordevelopment/resources/data-protection-in-mobile-money/

GSMA : Lois intelligentes sur la confidentialité des données. Atteindre les bons résultats à l'ère numérique (2019) https://www.gsma. com/publicpolicy/wp-content/uploads/2019/06/GSMA_ Smart-Data-Privacy-Laws_Report_June-2019.pdf

GSMA : Rapport sur l'état du secteur de l'argent mobile (2019) https://www.gsma.com/sotir/wp-content/uploads/2020/03/GSMA-State-of-the-Industry-Report- on-Mobile-Money-2019-Full-Report.pdf

GSMA : Rapport sur l'état de la connectivité de l'internet mobile (2020) https://www.gsma.com/r/wp-content/uploads/2020/09/GSMA-State-of-Mobile-Internet-Connectivity-Report-2020.pdf

GSMA : Les lignes directrices de la GSMA COVID-19 sur la protection de la vie privée (2020) https://www.gsma.com/publicpolicy/resources/covid- 19-privacy-guidelines

Fonds monétaire international (FMI) : The Promise of FinTech Financial Inclusion in the Post COVID-19 Era (La promesse de l'inclusion financière par les FinTech dans l'ère post-COVID-19). No. 20/09 (2020) https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2020/06/29/The-Promise-of-Fintech-Financial-Inclusion-in-the-Post-COVID-19-Era-48623

FMI : Série spéciale sur COVID-19 - Les services financiers numériques et la pandémie : Opportunités et risques pour les économies émergentes et en développement (2020)

Union internationale des télécommunications (UIT) : Groupe de réflexion sur les services financiers numériques, Rapport du groupe de discussion sur les services financiers numériques communément identifiés
Thèmes de protection des consommateurs pour les services financiers numériques 05/2016 (2016) https://www.itu.int/fr/ITUT/focusgroups/dfs/Documents/09_2016/ConsumerProtectionThemesForBestPractices.pdf

UIT : Initiative mondiale pour l'inclusion financière (FIGI) Groupe de travail sur l'infrastructure de sécurité et la confiance, Big data, machine learning, consumer protection and privacy (2018) https://www.itu.int/en/ITU-T/extcoop/figisymposium/2019/Documents/Presentations/Big%20data,%20Machine%20learning,%20Consumer%20protection%20and%20Privacy.pdf.

McDonald AM et Cranor LF : Le coût de la lecture des politiques de confidentialité. A Journal of Law and Policy for the Information Society, vol. 4, no. 3 (2008), 543-568 (2008) https://kb.osu.edu/handle/1811/72839

OCDE : Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel (1980, mises à jour en 2013) http://www.oecd.org/digital/ieconomy/lignes directrices de l'ocde sur la protection de la vie privee et les flux transfrontaliers de donnees personnelles.htm

OCDE : Garantir la confidentialité des données dans le cadre de la lutte contre le COVID-19 (2020) https://read.oecd-ilibrary.org/view/?ref=128_128758-vfx2g82fn3&title=Ensuring-data-privacy-as-we-battle-COVID-19

OCDE : L'utilisation des données personnelles dans les services financiers et le rôle de l'éducation financière : Une analyse centrée sur le consommateur (2020) http://www.oecd.org/financial/education/Personal-Data-Use-in-Financial-Services-and- et le rôle de l'éducation financière.pdf

Centre de Toronto : Cloud Computing : Issues for Supervisors (2020) https://res.torontocentre.org/guidedocs/Cloud%20Computing%20FINAL.pdf

Banque mondiale : Financial Consumer Protection and New Forms of Data Processing Beyond Credit Reporting (2018) https://openknowledge.worldbank.org/handle/10986/31009

Banque mondiale : Bonnes pratiques pour la protection des consommateurs de services financiers (2017) https://www.worldbank.org/en/topic/financialinclusion/brief/2017-good-practices-for-financial-consumer-protection

Banque mondiale : L'identification numérique et le défi de la protection des données : Practitioner's Note (2019) https://openknowledge.worldbank.org/handle/10986/32629

Banque mondiale : Disruptive Technologies in the Credit Information Sharing Industry : Developments and Implications (2019) http://documents1.worldbank.org/curated/en/587611557814694439/pdf/Disruptive-Technologies-in-the-Credit-Information-Sharing- Industry-Developments-and-Implications.pdf

Organisation des Nations Unies (ONU) : Protection des données personnelles et principes de confidentialité(2018) https://unsceb.org/sites/default/files/UN-Principles-on-Personal-Data-Protection-Privacy-2018.pdf

Zetzsche, DA, Arner, DW. et Buckley, RP et Kaiser-Yücel, A : FinTech Toolkit : Smart Regulatory and Market Approaches to Financial Technology Innovation (mai 2020). Université de Hong Kong Faculté de droit Document de recherche n° 2020/027 https://ssrn.com/abstract=3598142

Alliance pour l'inclusion financière
AFI, Sasana Kijang, 2, Jalan Dato' Onn, 50480 Kuala Lumpur, Malaisie
t +60 3 2776 **9000e** info@afi-global.org www.afi-global.org
Alliance pour l'inclusion financière AFI.History @NewsAFI @afinetwork