Unlocking Public and Private Finance for the Poor

Le rôle de la protection des données dans l'économie numérique

Les gouvernements, les organisations et les individus génèrent, collectent et traitent de plus en plus de données personnelles. Un cadre solide de protection des données contribue à favoriser la confiance des consommateurs et l'utilisation accrue des outils numériques, ce qui peut à son tour encourager l'investissement, la concurrence et l'innovation dans l'économie numérique.

Cette note, rédigé en étroite collaboration avec Macmillan Keck, cherche à identifier les attributs spécifiques d'un cadre de protection des données qui peut aider les décideurs politiques et les régulateurs à construire une économie numérique qui inclut - et sert - tout le monde.

BRIEF

Novembre 2021

Macmillan Keck

Seharish Gillani,
Ahmed Dermish, and
Jeremiah Grossman
of the UNCDF
Policy Accelerator

Résumé

Les gouvernements, les organisations et les particuliers génèrent, collectent et traitent de plus en plus de données personnelles.

La protection des données vise à équilibrer les avantages et les risques du traitement des données à caractère personnel[1] afin que les personnes aient la certitude que leurs données sont collectées et stockées en toute sécurité et utilisées uniquement à des fins légitimes.

Les lois sur la protection des données exigent généralement que le traitement des données personnelles soit légal, limité, transparent, précis et sécurisé. Elles cherchent souvent à protéger la vie privée des personnes[2] et leur accordent un certain contrôle sur la manière dont les données personnelles les concernant sont traitées. Elles établissent également des institutions dotées de pouvoirs leur permettant de mener des enquêtes et de faire respecter leurs obligations.

Un cadre solide de protection des données offre une sécurité qui peut encourager l'investissement, la concurrence et l'innovation dans l'économie numérique, ainsi que l'adoption de services numériques par les pouvoirs publics et le secteur privé.

Considérations à la lecture de cette note

1. Quels sont les défis liés à la protection des données et à l'économie numérique les plus importants sur votre marché, à la fois en général et pour les groupes marginalisés tels que les femmes et les personnes à faibles revenus ?

2. La réglementation en matière de protection des données dans votre pays s'applique-t-elle ?
   - **La numérisation** : L'application du règlement sur la protection des données à l'économie numérique
   - **L'inclusivité** : Les défis spécifiques de la protection des données auxquels sont confrontés les femmes, les personnes à faible revenu et/ou d'autres groupes marginalisés ?

3. Quelles sont les entités responsables de la réglementation de la protection des données ? Les responsabilités sont-elles claires, et des mécanismes sont-ils en place pour éviter l'arbitrage réglementaire ? Si ce n'est pas le cas, comment cela pourrait-il être amélioré ?

Pourquoi nous avons besoin de la protection des données

Des données pour le développement

Les technologies et les données numériques sont des catalyseurs potentiels du développement dans les domaines de la santé, de l'éducation, de l'agriculture, de la sécurité alimentaire, des services financiers, de la fabrication, du commerce et des infrastructures, ainsi que de l'économie numérique elle-même. Elles peuvent transformer les services publics et privés, éclairer les décisions politiques et améliorer le suivi des progrès et de l'impact.

Par exemple :

- Au Maroc, une participation électronique en ligne plateforme permet aux citoyens de soumettre et de voter des idées et de donner leur avis sur des propositions de loi visant à améliorer les services publics;[3]
- Les fournisseurs de services financiers numériques analysent les données relatives aux clients potentiels afin de leur proposer des services de paiement numérique, d'établir leur profil de risque en matière de crédit, de gérer leur identité et de détecter les transactions suspectes ;
- Les systèmes d'identification numérique collectent et échangent des données personnelles pour authentifier les personnes, réduisant ainsi la fraude et les obstacles à l'accès aux services ;
- Les données sur l'utilisation des services financiers par les particuliers dans le monde entier sont distillées pour produire le Global Findex, qui permet aux pays et à d'autres parties prenantes tels que[4,5] de suivre les progrès et d'élaborer des politiques en vue de : [6] et
- Les données ventilées par sexe sont un élément essentiel pour combler l'écart entre les sexes en matière d'inclusion financière.

Si une collecte, une organisation, une analyse, un stockage et un transfert plus efficaces des données (le cycle de vie qui comprend le ***traitement des*** données) peuvent améliorer leur utilisation productive, des mesures doivent être prises pour garantir la protection des données et la vie privée des consommateurs. De plus en plus, les gouvernements, les organisations et les particuliers génèrent, collectent et utilisent des données sur les personnes. 64,2 zettaoctets (ou 64,2 trillions de gigaoctets) de données ont été créés ou répliqués à l'échelle mondiale rien qu'en 2020, et on estime que cette quantité augmentera à un taux de croissance annuel composé de 23 % jusqu'en.[7] La plupart de ces données sont des ***données à caractère personnel***,[8] c'est-à-dire qu'elles concernent ou peuvent être utilisées pour identifier des personnes individuelles, appelées ***personnes concernées.***

Risque et confiance

La production et le traitement de grandes quantités de données personnelles comportent des risques. Les données personnelles peuvent être perdues, volées, divulguées sans consentement ou utilisées à mauvais escient. Il peut en résulter une usurpation d'identité,[9] des divulgations non souhaitées ou embarrassantes,[10] la perte d'informations importantes,[11] ou un marketing ou une sollicitation inopportuns.[12] Les données personnelles peuvent également être utilisées pour la surveillance du gouvernement[13] ou des entreprises,[14] ainsi que pour le traitement discriminatoire des personnes et des communautés vulnérables.[15]

Les particuliers peuvent ne pas savoir comment les données les concernant peuvent être utilisées ou à quelles entités elles peuvent être transférées, et leur confiance ne doit pas être considérée comme acquise. À mesure que les individus prennent conscience des risques liés à leurs données personnelles, ils peuvent éviter ou limiter l'utilisation des services numériques, ce qui peut entraver les efforts de développement et d'inclusion économiques.

Des études récentes montrent que, dans les pays à revenu élevé comme dans les pays à faible revenu, les consommateurs apprécient la protection de leurs données personnelles. Une majorité de clients à faible revenu au Kenya étaient prêts à payer une prime pour une plus grande protection de leurs données personnelles dans les services de prêts numériques, et les clients en Inde étaient susceptibles de refuser les remises sur les envois de fonds proposées en échange du partage de leurs données personnelles.[16] De même, une enquête mondiale menée auprès de plus de 5 000 consommateurs a révélé qu'un sur dix " s'attendait à ce que son engagement global envers la technologie diminue au cours des six prochains mois " en raison des préoccupations relatives aux violations de données et à la protection de la vie privée.[17]

Les femmes peuvent avoir des préoccupations différentes en matière de confidentialité des données et être plus soucieuses de leur vie privée en raison de leur vulnérabilité aux atteintes à la réputation. Des recherches récentes suggèrent que les préoccupations des femmes sont parallèles aux défis et aux menaces qu'elles rencontrent dans leur vie physique, comme la localisation et le harcèlement sexuel.[18] De même, un élément dissuasif important pour les femmes d'utiliser SFN est le fait qu'elles doivent partager des informations personnelles, comme les numéros de téléphone mobile, avec des agents qui pourraient en faire un mauvais usage.[19] Les préoccupations concernant leurs données et leur sécurité peuvent conduire les femmes à réduire leur utilisation de différents services et à autocensurer leur comportement. Les femmes peuvent également manquer de connaissances sur la manière de sauvegarder leurs données personnelles et s'en remettre aux membres masculins de leur famille et à des personnes plus instruites pour obtenir des conseils sur la manière de protéger leurs photos, leurs messages sur les médias sociaux, etc.[20] Les décideurs politiques doivent tenir compte de ces préoccupations propres aux femmes lors de l'élaboration d'un cadre de protection des données et de la vie privée.

Tendances internationales

La protection des données est de plus en plus mandatée dans les lois nationales et les lois et accords régionaux à travers les pays à revenu élevé et faible. En avril 2020, 66 % des pays avaient adopté une législation sur la protection des données et de la vie privée.[21] Un exemple largement cité est le Règlement général sur la protection des données 2016 de l'Europe (GDPR). Ces lois cherchent généralement à équilibrer les avantages et les risques du traitement des données personnelles afin que les individus aient confiance que les données personnelles les concernant sont collectées et stockées en toute sécurité et utilisées uniquement à des fins légitimes.

Qui doit se conformer à la protection des données

Les cadres de protection des données conçus dans la tradition du GDPR imposent des obligations à deux acteurs principaux :

- Les ***contrôleurs*** sont les personnes ou entités qui déterminent l'objectif et les moyens du traitement des informations personnelles. Par exemple, une banque qui collecte des informations personnelles sur les titulaires de comptes serait un contrôleur.
- Les ***sous-traitants*** sont les personnes ou entités qui effectuent le traitement de données à caractère personnel sous la direction ou pour le compte d'un responsable du traitement. Par exemple, l'entité qui exploite le logiciel que la banque utilise pour accéder à ses dossiers et les stocker serait le sous-traitant.

Les exemples de la Commission européenne sur les contrôleurs et les sous-traitants fournissent un contexte supplémentaire pour cette distinction.

Il convient de noter que les responsables du traitement peuvent traiter leurs propres données, mais que les sous-traitants agissent toujours pour le compte d'un responsable du traitement.

Les éléments clés de la protection des données

Licéité du traitement

Les cadres de protection des données exigent généralement que le traitement des données à caractère personnel soit effectué de ***manière licite***, ce qui signifie que la base du traitement est expressément autorisée par la loi.

Le ***consentement*** de la personne concernée est souvent invoqué comme base juridique. Le consentement doit être volontaire, donné librement et attesté par une action affirmative de la personne concernée ; il ne devrait donc pas suffire de donner à la personne concernée des cases pré-cochées ou des paramètres par défaut. Le consentement est aussi généralement considéré de manière étroite. Par exemple, le consentement donné pour la collecte et le stockage de dossiers médicaux personnels ne peut pas être considéré comme un consentement à la génération et à la réception de courriels de marketing sans rapport.

Le consentement présente certaines faiblesses en tant que moyen de légitimer le traitement des données. Les personnes ne peuvent pas lire de manière réaliste toutes les informations fournies par les responsables du traitement, et elles peuvent ne pas comprendre les implications du consentement au traitement des données personnelles. Les personnes peuvent également donner leur consentement parce que la seule alternative est de renoncer au service, ce qui signifie qu'elles n'ont pas vraiment le choix. Néanmoins, le consentement reste la seule base de traitement dans laquelle la personne concernée a un certain contrôle sur le traitement de ses données personnelles et des efforts sont faits pour rendre le consentement plus significatif, de sorte qu'il reste une caractéristique importante d'un cadre de protection des données.

Une autre base légale couramment utilisée pour le traitement des données personnelles est l'***intérêt légitime*** du responsable du traitement ou d'un tiers. Il s'agit de la base légale la plus souple et elle peut s'appliquer à pratiquement tout type de traitement pour toute finalité raisonnable. Toutefois, elle exige du responsable du traitement qu'il mette en balance ces intérêts avec les intérêts et les droits et libertés fondamentaux de la personne concernée en appliquant un test en trois parties:[22]

1. **Finalité** : le traitement repose-t-il sur un intérêt légitime ?
2. **Nécessité** : Dans l'affirmative, le traitement proposé est-il nécessaire à cette fin ?
3. **Mise en balance** : Cet intérêt légitime est-il prépondérant par rapport aux intérêts ou aux droits et libertés fondamentaux de la personne concernée ?

D'autres bases légales pour le traitement sur lesquelles les responsables du traitement se fondent comprennent (entre autres) lorsque le traitement est :

- Nécessaire pour exécuter un contrat avec la personne concernée (par exemple, pour fournir un produit adapté à ses besoins) ;
- Nécessaire pour satisfaire à une obligation légale du responsable du traitement (par exemple, si une société de télécommunications est tenue de conserver des enregistrements des services des clients à des fins de facturation) ;
- Nécessaire à l'exécution d'une tâche effectuée dans l'intérêt public ou dans l'exercice de l'autorité publique dont est investi le contrôleur (par exemple, l'administration de la justice) ; ou
- Essentiel à la vie de la personne concernée ou d'un tiers (par exemple, pour informer le médecin d'un état médical en cas d'urgence).

Souvent, le traitement est licite parce qu'il est expressément autorisé par une loi particulière distincte du cadre de protection des données, comme la collecte de données à caractère personnel par un système national d'identification en vertu d'une loi nationale sur l'identification.

Minimisation des données

Le thème de la ***minimisation des données*** traverse de nombreux éléments de la protection des données. Il s'agit de réduire le traitement des données à caractère personnel à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.[23]

Un cadre de protection des données exige généralement que toute collecte de données à caractère personnel soit effectuée dans un but spécifique et explicite qui doit être « légal » ou « légitime ». Cette exigence de ***spécification de la finalité*** limite le traitement ultérieur des données au-delà de cette finalité spécifiée. Cette limitation permet d'éviter le « détournement d'usage », c'est-à-dire l'utilisation de données personnelles collectées à l'origine pour une finalité donnée à d'autres fins. Par exemple, une grande surface disposant d'une pharmacie ne doit pas utiliser les données relatives aux médicaments prescrits par les clients pour commercialiser des articles de sport sans rapport avec ces derniers.

Une fois qu'une finalité a été spécifiée, de nombreux cadres exigent que le traitement des données à caractère personnel soit limité uniquement à ce qui est nécessaire pour atteindre la finalité spécifiée, ce que l'on appelle parfois le ***principe de proportionnalité.*** Cependant, certains cadres ne vont pas aussi loin, exigeant seulement que le traitement ne soit pas « excessif » ou simplement qu'il soit « pertinent » par rapport à la finalité spécifiée.[24] Par exemple, un employeur peut avoir besoin de conserver des informations médicales détaillées sur les employés effectuant des travaux dangereux en usine en cas d'accident, mais ne pas exiger ces données de son personnel administratif dans un bureau situé ailleurs.[25]

Les ***limitations de la conservation des données*** minimisent également le traitement en exigeant des contrôleurs et des processeurs qu'ils ne conservent les données personnelles que le temps nécessaire à la réalisation de l'objectif spécifié. Cela réduit les risques de violation des données et de partage non autorisé qui découlent d'un stockage inutile. Par exemple, l'UE exige que les banques conservent les données de leurs clients pendant cinq ans et autorise les États membres à étendre cette durée jusqu'à 10 ans.[26] En revanche, une agence pour l'emploi ne devrait pas conserver les CV des personnes à la recherche d'un emploi pendant des décennies, car cela n'est pas proportionné à l'objectif de trouver un emploi pour ces personnes à court et moyen terme.[27]

Certains cadres exigent que les systèmes de traitement des données intègrent le r***espect de la vie privée dès la conception*** ou ***par défaut.*** Ces termes font référence à la mise en œuvre de mesures administratives et techniques qui appliquent des principes de minimisation des données dans l'architecture et les processus du système de données. Par exemple, les dossiers des patients d'un hôpital peuvent être pseudonymisés lors de leur stockage ou de tout autre traitement afin de réduire le risque de divulgation en cas de violation des données.

Transparence

Les cadres de protection des données exigent généralement que le traitement des données soit ***équitable et transparent***, et que les personnes concernées soient obligatoirement informées lorsque des données les concernant sont collectées, quelle que soit la base juridique de cette collecte et de ce traitement. Certains cadres exigent que ces informations soient communiquées à la personne concernée même si les données personnelles sont obtenues auprès d'un tiers ou de sources accessibles au public. Ces informations doivent généralement indiquer l'identité du responsable du traitement, l'objectif de la collecte des données à caractère personnel, les tiers auxquels elles peuvent être communiquées et les droits individuels dont dispose la personne concernée. Les exigences de notification équitables et transparentes sont étroitement liées à la protection des consommateurs, comme nous l'expliquons dans notre note de synthèse sur la protection des consommateurs.

Qualité des données

Les cadres de protection des données exigent aussi généralement que les responsables du traitement maintiennent activement la ***qualité*** des données à caractère personnel qu'ils traitent. Cela peut créer une obligation positive de veiller à ce que les données personnelles soient et restent exactes, complètes et à jour.

Marketing direct

Les cadres de protection des données intègrent souvent des ***limitations aux activités de marketing direct*** ciblant les personnes concernées par les responsables du traitement. Certains cadres interdisent les activités de marketing direct à moins qu'une personne concernée n'ait expressément choisi d'y participer, avec quelques exceptions pour les relations clients existantes.[28] D'autres prévoient seulement qu'une personne concernée peut s'opposer ou refuser.[29]

Sécurité des données

Les cadres de protection des données exigent généralement des responsables du traitement et des sous-traitants qu'ils évaluent et maintiennent la sécurité de

leurs systèmes de données, notamment en divulguant les violations de données à l'autorité de protection des données et, dans certains cas, aux personnes concernées. Ce sujet est abordé dans le document d'information sur la cybersécurité et la sécurité des données.

Flux de données transfrontaliers

L'utilisation efficace et innovante des données peut impliquer le transfert de données au-delà des frontières nationales. Cela peut être nécessaire, par exemple, pour la fourniture de services numériques et de commerce électronique transfrontaliers, l'exploitation de chaînes d'approvisionnement internationales, la gestion des relations avec la clientèle par des prestataires de services internationaux, l'accès à un traitement des données de meilleure qualité ou à moindre coût, ou la mise en commun de données pour une meilleure analyse.

D'autre part, il est difficile de contrôler et de faire respecter les exigences en matière de protection des données si celles-ci quittent le pays. De nombreux cadres de protection des données imposent donc des conditions et des restrictions au transfert de données en dehors de la juridiction. Ce point est abordé plus en détail dans le document d'information sur la localisation et la résidence des données.

Données personnelles sensibles

Certaines données sont considérées comme des ***données personnelles sensibles***, telles que les attributs personnels concernant le corps et les comportements d'une personne (biométrie, état de santé, sexualité), son ascendance (race, ethnie) ou ses croyances spirituelles, sa philosophie et ses opinions (religion, convictions politiques). Ces données font généralement l'objet d'une protection renforcée parce qu'elles peuvent être embarrassantes ou inconfortables pour la personne concernée si elles sont divulguées, ou risquent d'être utilisées pour un profilage indésirable ou un traitement discriminatoire à l'encontre des membres d'un groupe potentiellement vulnérable. Les protections renforcées impliquent généralement des exigences accrues en matière d'obtention du consentement de la personne concernée pour le traitement des données et des restrictions plus strictes sur le transfert de ces données à l'étranger.

Droits individuels

Dans un nombre croissant de juridictions, les principes de la protection des données ne se traduisent pas simplement par des obligations pour les responsables du traitement et les sous-traitants, mais par des droits exécutoires pour les personnes concernées. Ces droits donnent aux personnes concernées un certain degré de contrôle sur la manière dont les données personnelles les concernant sont traitées et sont généralement censés pouvoir être exercés gratuitement ou à un coût nominal. Ces droits sont similaires aux autres droits accordés aux consommateurs en général dans le cadre de la protection des consommateurs.

Les droits des personnes comprennent généralement le ***droit de vérifier si leurs données personnelles sont traitées*** par un responsable du traitement et, par conséquent, le ***droit d'accéder à une*** copie de ces données personnelles ***et de la consulter.*** Les personnes peuvent ensuite avoir le droit de rectifier toute donnée personnelle périmée, trompeuse ou incomplète qu'elles identifient. Le droit de vérifier, d'examiner et de rectifier les données à caractère personnel qu'une organisation détient sur une personne serait

important, par exemple, lorsque les données sont utilisées pour évaluer l'éligibilité à un prêt et que des données incorrectes pourraient nuire à ses perspectives.

Dans certains cadres, les personnes concernées se voient accorder un ***droit à l'effacement des données*** à caractère personnel détenues par un responsable du traitement. Lorsqu'il est prévu, ce droit ne peut généralement être exercé que si les données à caractère personnel ont été obtenues de manière illicite, si le responsable du traitement n'a plus de base valable pour conserver les données ou si la conservation des données n'est plus nécessaire (c'est-à-dire que ce droit met en œuvre les principes relatifs à la base légale du traitement et à la minimisation des données évoqués ci-dessus). Par exemple, une société de services publics peut avoir besoin de l'adresse résidentielle d'un abonné, mais il se peut qu'il n'y ait plus de base légale pour conserver ces données personnelles une fois que l'abonné a désactivé le service. Dans ce cas, l'abonné serait fondé à demander l'effacement des données à caractère personnel.

Certains cadres incluent un ***droit à la portabilité des données***: la possibilité de déplacer, copier ou transférer facilement des données personnelles d'un contrôleur à un autre. La portabilité vise à réduire le risque que la personne concernée soit enfermée dans un service ou un fournisseur de services particulier parce que ce dernier a accumulé des données personnelles utiles ou nécessaires. Elle réduit ainsi les obstacles au passage à un autre fournisseur de services. Par exemple, si une personne suit ses données d'activité physique à l'aide d'un dispositif portable lié à une application, elle devrait pouvoir transférer ces données à une application concurrente.

Certains pays introduisent des exigences de portabilité des données dans les services financiers. De nombreux services de crédit numérique prennent des décisions de crédit sur la base des historiques de transactions d'argent mobile liés. Un droit à la portabilité des données permettrait aux clients d'un service d'argent mobile d'utiliser leurs historiques de transactions avec un service de crédit numérique non lié. Cela peut être particulièrement pertinent pour les femmes qui sont moins susceptibles que les hommes de posséder des actifs physiques qu'elles peuvent utiliser comme garantie de prêt, mais qui peuvent tirer parti de leur historique de transactions numériques comme source alternative pour prouver leur solvabilité.[30]

Certains traitements de données personnelles intègrent des algorithmes informatiques qui trient et analysent les données pour prendre des décisions concernant les personnes concernées. Ces décisions peuvent être entachées d'erreurs et de biais résultant de données d'apprentissage erronées, obsolètes ou biaisées, de données erronées concernant la personne concernée ou d'erreurs ou de biais dans les algorithmes eux-mêmes. Certaines décisions reposant sur un ***profilage*** fondé sur des facteurs tels que la race, l'origine ethnique ou la religion seraient illégalement discriminatoires si la décision était prise par une personne. Pour faire face à ces risques, de nombreux cadres prévoient que les personnes concernées ont ***le droit de ne pas être soumises à des décisions fondées uniquement sur le traitement automatisé*** des données à caractère personnel qui entraînent des conséquences juridiques pour la personne concernée. Il s'agit par exemple du refus automatique des prêts soumis via des candidatures en ligne et des pratiques de recrutement électronique qui sont conclues sans intervention humaine.

Les cadres de protection des données donnent généralement aux personnes concernées le ***droit de s'opposer au traitement*** des données à caractère personnel.[31] Lorsqu'une telle objection est valablement formulée, le responsable du traitement doit généralement cesser le traitement.

Ce que couvre la protection des données

Connexions géographiques

Il existe des limites pratiques et juridiques à l'application du droit national en dehors de la juridiction. Les lois sur la protection des données exigent généralement un niveau minimum de connexion avec le territoire. Dans de nombreux pays, la loi ne s'applique que lorsque les contrôleurs et/ou les processeurs sont établis sur le territoire, que le traitement a lieu sur le territoire ou que les personnes concernées sont ciblées ou surveillées sur le territoire. L'applicabilité fondée uniquement sur la localisation de la personne concernée est souvent considérée comme un dépassement des limites.

Par exemple, un contrôleur de données étranger exploitant un site web, mais n'ayant aucun lien avec le territoire ou ne souhaitant pas engager ses résidents ne voudrait pas être soumis aux obligations locales en matière de protection des données simplement parce qu'un résident se trouve à naviguer sur ce site web à l'insu du contrôleur de données. Par conséquent, certaines juridictions appliquent leurs cadres de protection des données aux contrôleurs de données étrangers uniquement lorsque le contrôleur s'engage dans un ciblage actif, un marketing ou un suivi des résidents de cette juridiction.

Champ d'application des activités de traitement

Étant donné l'ampleur des concepts de « données à caractère personnel » et de « traitement », la protection des données pourrait être interprétée comme s'appliquant à un vaste éventail d'activités humaines. De nombreux cadres exemptent explicitement le traitement de données personnelles pour des ***affaires personnelles, domestiques, familiales ou récréatives***. Le traitement de données à caractère personnel aux fins d'activités telles que l'organisation d'équipes de sport amateur ou la planification de réunions de famille n'est pas susceptible de causer un préjudice et la réglementation de ce traitement constituerait une intrusion massive dans la vie privée des individus.

Certaines activités ne sont pas soumises à la loi sur la protection des données car elles offrent des avantages sociétaux qui devraient être autorisés, sous réserve de certaines protections. Il s'agit par exemple du traitement de données à des ***fins journalistiques, artistiques ou littéraires***. Le traitement par les pouvoirs publics de données à caractère personnel à des fins de ***sécurité nationale ou publique, d'application de la loi*** ou d'autres ***fonctions gouvernementales sensibles*** peut également être exclu, bien qu'il soit généralement assorti de garanties visant à limiter les abus.

Anonymisation

Lorsque les données à caractère personnel peuvent être rendues anonymes de sorte qu'il est plus difficile, voire impossible, d'identifier la personne à laquelle elles se rapportent, la raison de protéger ces données diminue considérablement et elles peuvent être traitées sans être soumises aux exigences de la protection des données. L'anonymisation exige que tous les liens avec la personne concernée soient supprimés

de manière permanente et irrévocable. En revanche, les données qui sont simplement dépersonnalisées, ce qui signifie par exemple que les informations d'identification sont remplacées par des informations codées qui pourraient être décodées pour ré-identifier la personne, ne seraient pas considérées comme anonymes. Toutefois, l'anonymisation est un domaine dynamique où le seuil ne cesse de s'élever à mesure que les nouvelles technologies trouvent de nouveaux moyens de relier les données anonymes à la personne concernée.

Les institutions qui soutiennent la protection des données

Autorités chargées de la protection des données

Les cadres de protection des données désignent généralement une agence qui fait office d'***autorité de protection des données*** ou exerce une fonction similaire. De nombreux cadres exigent que l'autorité de protection des données soit ***indépendante*** afin d'éviter qu'elle ne soit captée par des influences politiques ou commerciales. Cela est d'autant plus important que les organismes publics collectent, utilisent et enregistrent de nombreuses données personnelles sur la population lorsqu'ils lui fournissent des services publics.

Les fonctions et les pouvoirs de ces autorités varient selon les juridictions. Ils comprennent généralement le contrôle de la conformité, la réception de plaintes et la conduite d'enquêtes, l'envoi d'avis d'exécution, l'imposition d'amendes administratives, l'émission ou le conseil sur l'émission de règlements, l'engagement dans des efforts de sensibilisation du public et le conseil aux législateurs et aux décideurs sur les questions de protection des données. Une autorité est généralement financée par une combinaison d'allocations versées par le corps législatif et du produit des droits ou des amendes.

Certains cadres exigent des responsables du traitement, et même des sous-traitants, qu'ils s'enregistrent auprès d'une autorité de protection des données afin de renforcer les informations de l'autorité sur les activités liées aux données et de lui permettre de percevoir des droits. Pour éviter les charges administratives, cette ***obligation d'enregistrement*** ne s'applique généralement que lorsque certains seuils sont atteints ou que le traitement concerne des questions particulièrement sensibles.

Les cadres de protection des données prévoient généralement des ***appels ou un contrôle judiciaire*** des décisions défavorables prises par une autorité de protection des données. Parfois, les appels sont faits auprès d'un organisme d'appel ad hoc comme étape intermédiaire, d'autres fois directement auprès d'un tribunal.

Sanctions et remèdes

L'efficacité des obligations et des protections dans un cadre de protection des données dépend de la menace crédible de conséquences en cas de violation. De nombreux cadres habilitent une autorité de protection des données à imposer des ***amendes administratives*** aux responsables du traitement et aux sous-traitants en cas de violation. Le montant des amendes est souvent limité par un plafond monétaire ou un pourcentage du chiffre d'affaires annuel de l'entité (national ou mondial), ou les deux. Certains cadres autorisent les particuliers à engager des ***poursuites civiles*** directes devant les tribunaux nationaux contre les responsables du traitement et les sous-traitants pour les dommages résultant de violations.

Certains cadres prévoient des ***sanctions pénales*** consistant en des amendes et/ou des peines d'emprisonnement et sont applicables aux personnes physiques telles que les administrateurs, les dirigeants et les gestionnaires de personnes morales. Les sanctions pénales sont plus courantes dans les juridictions qui ont moins confiance dans l'efficacité des amendes administratives et des actions civiles.

Société civile, éducation et culture

Outre un cadre juridique, l'engagement, l'éducation et la professionnalisation de la société civile sont souvent essentiels pour faire évoluer la compréhension et la conduite des organismes publics et des organisations commerciales et à but non lucratif.

Par exemple, le Nubian Rights Forum au Kenya a fait pression pour que des lois sur la protection des données protègent les données utilisées dans les systèmes d'identification numérique proposés.[32] Certaines juridictions, comme l'UE, ont créé une catégorie professionnelle spécifique de ***délégués à la protection des données*** (DPD) que les organisations d'une taille ou d'une nature particulière sont tenues d'engager. Les DPD ont certaines responsabilités, remplissent diverses fonctions, sont censés avoir reçu une formation adéquate et s'enregistrer auprès des autorités de protection des données. Ces exigences, ainsi que d'autres exigences similaires, favorisent le développement d'une communauté de professionnels compétents ayant une compréhension et des approches communes, intégrée dans les institutions publiques et privées.

Comment la protection des données soutient l'économie numérique

Croissance de l'économie numérique

Une confiance accrue dans le domaine numérique est essentielle pour l'adoption et l'utilisation des services numériques. Les fournisseurs ont également besoin de certitude quant aux règles du jeu. La mise en œuvre d'un cadre de protection des données peut être une condition préalable précieuse pour investir dans les entreprises à forte intensité de données. Par exemple, immédiatement après la promulgation de la loi sur la protection des données, Kenya 2019 Data Protection Act, Amazon Web Services a annoncé de nouveaux investissements dans le pays, notamment en établissant une partie de son infrastructure de cloud de données à Nairobi. L'entreprise aurait caractérisé la nouvelle loi comme ouvrant la voie à cet investissement, notant qu'elle attendait une telle loi depuis sept ans.[33]

Confiance dans les services gouvernementaux

Un cadre de protection des données peut également renforcer la confiance dans le fait que les utilisations gouvernementales des données personnelles n'entraîneront pas de surveillance injustifiée, de profilage ou d'autres discriminations. Par exemple, les systèmes d'identification nationaux mis en place dans certains pays en développement ont été fortement critiqués lorsqu'ils ont été mis en œuvre sans un cadre solide de protection des données. En Inde,[34] en Jamaïque,[35] et au Kenya,[36] des décisions judiciaires récentes ont même invalidé ou limité l'adoption de systèmes d'identification nationaux, en grande partie en raison de la protection insuffisante des données personnelles. Les préoccupations relatives

à la protection des données sous-tendent le manque d'adoption des applications de recherche des contacts lors de la récente pandémie de Covid-19. Par exemple, une étude récente a montré que dans les pays où les individus ont tendance à se méfier de leurs gouvernements, ils ont été plus hésitants à télécharger et à utiliser les applications de recherche des contacts.[37]

Questions émergentes

L'*intelligence artificielle* (IA) désigne les systèmes informatiques capables d'effectuer des tâches qui requièrent normalement l'intelligence humaine, telles que la perception visuelle, la reconnaissance vocale, la prise de décision et la traduction entre langues.

L'*apprentissage automatique* fait référence à la capacité de ces systèmes à améliorer progressivement leurs propres performances en analysant de grands volumes de données, plutôt que par la programmation humaine. Ces technologies présentent des opportunités pour le développement de l'économie numérique, par exemple grâce à l'amélioration de l'évaluation du crédit qui favorise l'inclusion financière, ou à une meilleure détection des fraudes. Cependant, ces systèmes utilisent de grandes quantités de données, et il peut être difficile, voire impossible, de savoir quelles données sont traitées, comment elles le sont, ou comment sont générées les décisions concernant les individus. Ces systèmes présentent donc des défis pour bon nombre des protections clés des cadres de protection des données.

Par exemple, Amazon a découvert que son logiciel d'embauche automatisé basé sur l'IA favorisait involontairement les candidats masculins. Le logiciel a été « formé » sur des CV d'anciens candidats, qui étaient majoritairement des hommes, ce qui l'a conduit à pénaliser les candidates.[38] Les solutions potentielles à ce genre de problèmes consistent à s'attaquer au type de données de formation utilisées et à s'assurer qu'il y a un « humain au courant » lorsque des décisions sont prises. Voir le Center for Information Policy Leadership, Intelligence artificielle et protection des données en tension, 2018 ; Centre pour la démocratie et la technologie, IA et apprentissage automatique, 2020.

La *technologie de reconnaissance faciale* (TRF) désigne les systèmes informatiques capables de traiter les images de visages humains pour identifier, authentifier ou catégoriser un individu. Bien qu'elle offre des possibilités d'identification et de vérification numériques susceptibles de favoriser le développement de l'économie numérique, cette technologie soulève de nombreux problèmes de protection des données.

Premièrement, les caméras sont devenues de plus en plus omniprésentes grâce à la surveillance gouvernementale, aux systèmes de sécurité du secteur privé et aux produits de consommation tels que les sonnettes intelligentes et les smartphones. Les individus exposent leur visage chaque fois qu'ils sont en public, s'ouvrant ainsi à la surveillance et au traitement de leurs informations personnelles, souvent sans leur consentement.

Deuxièmement, grâce à sa nature, le TRF peut discerner les informations personnelles sensibles des personnes, notamment le sexe, la race, l'origine ethnique et l'état de santé (ainsi que des données qui ne sont pas sensibles, comme la localisation).

Enfin, le TRF n'est pas toujours précis, notamment lorsqu'il s'agit d'identifier les

visages de certains groupes de population, ce qui peut entraîner des erreurs d'identification susceptibles d'avoir des conséquences juridiques pour les individus.

Par exemple, une étude récente a montré que les technologies de reconnaissance faciale identifient les hommes à la peau claire presque sans erreur, mais ont un taux d'erreur de près de 35 pour cent lorsqu'il s'agit d'identifier des visages féminins à la peau plus foncée.[39] Voir National Conference of State Legislatures, La reconnaissance faciale gagne en popularité, 2020 ; Roussi, Antoaneta, Résister à l'essor de la reconnaissance faciale, 2020 ; Comment réglementer la technologie de reconnaissance faciale ? Nature, 2019 ; Wiewiórowski, Wojciech, La reconnaissance faciale : Une solution à la recherche d'un problème ?, Contrôleur européen de la protection des données, 2019.

Ressources supplémentaires

Modèles de protection des données

- Règlement général sur la protection des données de l'UE
- Cadre de protection de la vie privée de l'APEC
- Cadre de l'OCDE relatif à la protection de la vie privée
- Glossaire de l'IAPP

Pour en savoir plus

- Convention 108+ pour la protection des personnes à l'égard du traitement des données à caractère personnel., 2018
- Note d'orientation de l'UNSDG sur la confidentialité, l'éthique et la protection des données sur le Big Data pour la réalisation de l'Agenda 2030. 2017
- Big data, intelligence artificielle, apprentissage automatique et protection des données., 2016
- Vie privée et liberté d'expression à l'ère de l'intelligence artificielle, 2018

Organisations

- Association internationale des professionnels de la protection de la vie privée (IAPP)
- Commission européenne (page de ressources sur la protection des données)
- Centre pour le leadership en matière de politique de l'information
- Forum sur l'avenir de la vie privée
- ICO : Information Commissioner's Office (ROYAUME-UNI)
- Centre d'information sur la vie privée électronique (EPIC)
- Privacy International
- Centre pour la démocratie et la technologie
- Centre pour l'innovation des données
- Electronic Frontier Foundation

Références

[1] Le terme « traitement » désigne toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction, Article 4 GDPR

[2] Les termes « protection des données » et « confidentialité des données » sont parfois utilisés de manière interchangeable, mais peuvent avoir des significations différentes selon la tradition juridique. Pour simplifier, on peut considérer que la protection des données est motivée par les notions de dignité, de liberté et d'autonomie. Elle concerne les limites à la communication de données sur les individus à d'autres personnes, et peut chercher à permettre aux individus de déterminer le moment, la manière et l'étendue d'une telle communication. Une grande partie de la protection des données, qui régit la collecte, l'utilisation, le partage et le stockage des données à caractère personnel, consiste à garantir la confidentialité des données. Toutefois, comme indiqué ci-dessous, les politiques de protection des données traitent également de la sécurité des données (voir la discussion sur la sécurité des données ci-dessous et [le document d'information sur la cybersécurité et la sécurité des données]) et de la protection des consommateurs (voir la discussion sur les droits individuels dans ce document d'information et [le document d'information sur la protection des consommateurs]).

[3] Voir e-Government Program, Royaumde de Maroc, e-Participation Platform: FIKRA, disponible sur le site : http://www.egov.ma/en/e-participation-platform-fikra.

[4] Voir World Bank Universal Financial Access by 2020, disponible sur le site : https://www.worldbank.org/en/topic/financialinclusion/brief/achieving-universal-financial-access-by-2020.

[5] Voir United Nations' Sustainable Development Goals (SDG Target 8.10), disponible sur le site : https://sdg-tracker.org/economic-growth.

[6] World Bank. 2021. World Development Report 2021: Data for Better Lives. Washington, DC: World Bank. doi:10.1596/978-1-4648-1600-0. License: Creative Commons Attribution CC BY 3.0 IGO

[7] Data Creation and Replication Will Grow at a Faster Rate Than Installed Storage Capacity, According to the IDC Global DataSphere and StorageSphere Forecasts, Business Wire, 24 mars 2021, www.businesswire.com/news/home/20210324005175/en/Data-Creation-and-Replication-Will-Grow-at-a-Faster-Rate-Than-Installed-Storage-Capacity-According-to-the-IDC-Global-DataSphere-and-StorageSphere-Forecasts.

[8] Susan Aaronson, 2018, Data is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows, Working Papers 2018-10, The George Washington University Institute for International Economic Policy, disponible sur le site : https://www.cigionline.org/sites/default/files/documents/paper%20no.197_0.pdf.

[9] Par exemple, en 2020, la Commission fédérale du commerce des États-Unis a reçu 1,4 million de signalements de vol d'identité par l'intermédiaire de son site IdentityTheft.gov, soit environ deux fois plus qu'en 2019. "New Data Shows FTC Received 2.2 Million Fraud Reports from Consumers in 2020," Federal Trade Commission (4 February 2021). disponible sur le site : https://www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers.

[10] Par exemple, en 2015, AshleyMadison.com, un site de rencontres destiné aux personnes mariées à la recherche d'aventures extraconjugales secrètes, a été piraté. Les données personnelles de 36 millions de clients ont été divulguées, y compris les noms, adresses et numéros de téléphone. Voir, e.g., "Ashley Madison settles with FTC over data security," Federal Trade Commission (14 decembre 2016). disponible sur le site : https://www.ftc.gov/news-events/blogs/business-blog/2016/12/ashley-madison-settles-ftc-over-data-security.

[11] Par exemple, en 2020, 560 établissements de santé américains ont été victimes d'attaques par ransomware. Un hôpital du Colorado n'a pas voulu payer la rançon et n'a pas pu récupérer un nombre important de dossiers médicaux de patients. "Another banner year for cybercriminals," EMSISOFT Blog (18 janvier 2021). disponible sur le site : https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/.

[12] Jerich, Kat, "Ransomware attack leaves 5 years of patient records inaccessible at Colo. Hospital," HealthcareITNews (16 June 2020). disponible sur le site : https://www.healthcareitnews.com/news/ransomware-attack-leaves-5-years-patient-records-inaccessible-co-hospital.

[13] Par exemple, le bureau du commissaire à l'information du Royaume-Uni a constaté que les trois principales agences de notation de crédit du pays "utilisaient toutes des données personnelles collectées à des fins de référencement de crédit à des fins de marketing direct", contrairement aux exigences du GDPR. Investigation into data protection compliance in the direct marketing data brokering sector, Information Commissioner's Office (Octobre 2020). Disponible sur le site : https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf.

[14] Par exemple, les divulgations de documents classifiés par Edward Snowden en 2013 ont révélé des programmes massifs de surveillance gouvernementale, notamment que (1) l'Agence nationale de sécurité américaine (NSA) exigeait de l'entreprise de télécommunications Verizon qu'elle lui remette les métadonnées de millions d'appels téléphoniques de citoyens américains ; (2) la NSA avait un accès direct aux serveurs de certaines des plus grandes entreprises technologiques, notamment Apple, Facebook, Google, Microsoft, Skype, Yahoo et YouTube ; et (3) des types similaires de surveillance gouvernementale étaient entrepris par les gouvernements d'autres pays développés. Lyon, David, "Surveillance, Snowden, and Big Data: Capacities, consequences, critique," Big Data & Society, July-December 2014: 1-13. Disponible sur le site : https://journals.sagepub.com/doi/10.1177/2053951714541861.

[15] Voir, e.g., Christl, Wolfie, "Corporate Surveillance in Everyday Life, How Companies Collect, Combine, Analyze, Trade and Use Personal Data on Billions," Cracked Labs (2017). Disponible sur le site : https://crackedlabs.org/en/corporate-surveillance.

[16] Voir, e.g., Favaretto, Maddalena et al., "Big Data and Discrimination: Perils, Promises and Solutions. A Systematic Review," Journal of Big Data 6:12 (2019). disponible sur le site : https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0177-4.

[17] Fernandez Vidal, Maria, Data Privacy Concerns Influence Financial Behaviors in India, Kenya, CGAP, 29 septembre 2020, disponible sur le site : www.cgap.org/blog/data-privacy-concerns-influence-financial-behaviors-india-kenya.

[18] Voir PWC, "Four steps to gaining consumer trust in your tech," PWC website. Disponible sur le site : https://www.pwc.com/us/en/tech-effect/cybersecurity/trusted-tech.html.

[19] https://www.centerforfinancialinclusion.org/gender-and-digital-worldviews-divergent-user-perspectives-on-data-collection-and-use

[20] https://www.afi-global.org/sites/default/files/publications/2020-05/AFI_WFI_DFS_SR_AW_digital.pdf

[21] https://dalberg.com/our-ideas/privacy-line/

[22] VoirUnited Nations Conference on Trade and Development, Data Protection and Privacy Legislation Worldwide, disponible sur le site : https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[23] Voir Information Commissioner's Office, What is the 'legitimate interests' basis? (consulté le 6 octobre 2021).

[24] https://edps.europa.eu/data-protection/data-protection/glossary/d_en#:~:text=The%20principle%20of%20%E2%80%9Cdata%20minimisation,necessary%20to%20fulfil%20that%20purpose.

[25] Par exemple, le GDPR de l'UE et la loi kényane sur la protection des données de 2019 limitent tous deux le traitement des données personnelles à "ce qui est nécessaire" par rapport aux objectifs pour lesquels les données sont traitées. En revanche, la loi sud-africaine de 2013 sur la protection des informations personnelles et la loi malaisienne de 2010 sur la protection des données personnelles imposent une norme sans doute plus faible, exigeant que le traitement des données personnelles ne soit "pas excessif" compte tenu de la finalité pour laquelle les données sont traitées.

[26] Dérivé d'un exemple fourni par le site web de l'Information Communication's Office du Royaume-Uni, "Principle (c): Data minimisation." Disponible sur le site : https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/.

[27] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Art. 40.

[28] Dérivé d'un exemple fourni par le site web de la Commission européenne, "For how long can data be kept and is it necessary to update it?" Disponible sur le site : https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en.

[29] Par exemple, Section 69 du South Africa's Protection of Personal Information Act 2013.

[30] Par exemple, Section 41 du Malaysia's Personal Data Protection Act, 2010.

[31] https://www.gpfi.org/sites/gpfi/files/sites/default/files/saudig20_women.pdf

[32] GDPR Article 21

[33] Nubian Rights Forum, Kenya Human Rights Commission and Kenya National Commission on Human Rights v The Hon. Attorney General and Others [2020] at eKLR http://kenyalaw.org/caselaw/cases/view/189189/

[34] Oblultsa, G et Miriri, D., Kenya passes data protection law crucial for tech investments, Reuters, 8 Novembre 2019, disponible sur le site : https://www.reuters.com/article/us-kenya-dataprotection/kenya-passes-data-protection-law-crucial-for-tech-investments-idUSKBN1XI1O1

[35] Justice K.S. Puttaswamy (Retd.) v. Union of India, Writ Petition (Civil) No. 494 of 2012, 1 (Sup. Ct. India Aout. 24, 2017).

[36] Robinson v. Att'y Gen. of Jamaica [2019] JMFC Full 04 (Sup. Ct. Jamaica Avr. 12, 2019) https://supremecourt.gov.jm/content/robinson-julian-v-attorney-general-jamaica.

[37] M. Bano, D. Zowghi and C. Arora, Requirements, Politics, or Individualism: What Drives the Success of COVID-19 Contact-Tracing Apps?, in IEEE Software, vol. 38, no. 1, pp. 7-12, Jan.-Fev. 2021, doi: 10.1109/MS.2020.3029311.

[38] Dastin J, "Amazon scraps secret AI recruiting tool bias against women", Reuters, 10 octobre 2018, disponible sur le site : https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

[39] Joy Buolamwini, Timnit Gebru, Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91, 2018

À propos de l'UNCDF

L'UN Capital Development Fund (UNCDF) facilite l'accès aux capitaux publics et privés par les populations les plus démunies dans les 46 pays les moins avancés du monde (PMA).

Dans le cadre de son mandat de fourniture de capitaux et d'instruments d'investissement, l'UNCDF offre des modèles de financement du «last mile» permettant de débloquer les ressources publiques et privées, notamment au niveau national, afin de réduire la pauvreté et d'encourager le développement économique local.

Les modèles de financement de l'UNCDF ouvrent à travers trois axes, à savoir : 1) les économies numériques inclusives, qui connectent les personnes, les ménages et les petites entreprises aux écosystèmes financiers qui catalysent la participation à l'économie locale et fournissent des outils pour vaincre la pauvreté et gérer leur vie financière ; 2) le financement du développement local, qui permet aux municipalités de dynamiser l'expansion économique locale et le développement durable par le biais de la décentralisation fiscale, du financement municipal innovateur et du financement structuré de projets ; et 3) le financement d'investissements, qui fournit une structuration financière catalytique, une réduction des risques et le déploiement des investissements pour favoriser l'impact des ODD et la mobilisation des ressources au niveau national.

L'UNCDF Policy Accelerator travaille avec les gouvernements pour les aider à créer des politiques et des réglementations qui incluent tout le monde dans l'économie numérique, partage des outils et des guides pratiques basés sur notre modèle d'assistance technique et nos ressources de référence, et fourni des bourses aux décideurs politiques et aux régulateurs pour qu'ils puissent étudier avec nos organisations partenaires de classe mondiale.

À propos de Macmillan Keck

Macmillan Keck Attorneys & Solicitors conseille ses clients en matière de stratégie, de plaidoyer, d'affaires controverses et réformes dans l'économie numérique. Les clients du cabinet comprennent des opérateurs de télécom les fournisseurs de services financiers numériques, les fournisseurs de services de santé et d'éducation en ligne fournisseurs de contenu, d'applications et de services numériques, des gouvernements et des autorités de régulation de la concurrence et des organisations internationales. Le cabinet a mené à bien de nombreux projets complexes dans une majorité de pays sur tous les continents.

Clause de non-responsabilité

Les appellations utilisées sur cette carte et la présentation des données qui y figurent n'impliquent aucune prise de position de la part du Secrétariat de l'Organisation des Nations Unies ou de l'UNCDF quant au statut juridique des pays, territoires, villes ou zones.

Cette publication a été révisée pour la dernière fois en octobre 2021

Unlocking Public and Private Finance for the Poor

policy.accelerator@uncdf.org

policyaccelerator.uncdf.org | uncdf.org

FIND US