UTILISATION DES DONNÉES DE CARACTÈRE PERSONNEL DANS LES SERVICES FINANCIERS ET LE RÔLE DE L'ÉDUCATION FINANCIÈRE

UNE ANALYSE CENTRÉE SUR LE CONSOMMATEUR

OCDE

Utilisation des données de caractère personnel dans les services financiers et le rôle de l'éducation financière

Une analyse centrée sur le consommateur

Merci de citer cet ouvrage comme suit :

OCDE (2020), *Utilisation des données de caractère personnel dans les services financiers et rôle de l'éducation financière : une analyse centrée sur le consommateur*
www.oecd.org/financial/education/utilisation-des-donnees-de-caractere-personnel-dans-les-services-financiers-et-le-role-de-education-financiere.pdf.

La traduction de ce document en français a été possible grâce à une contribution financière de la Banque de France, opérateur de la stratégie d'éducation économique, budgétaire et financière en France.

Avant-propos

Les innovations technologiques ont fortement accru la capacité des prestataires de services financiers à recueillir, stocker, combiner et analyser un large éventail de données concernant leurs clients, comme leur situation financière, leurs préférences, leurs habitudes et leur localisation physique.

Si ces tendances peuvent procurer des avantages aux consommateurs, elles s'accompagnent de nouveaux risques spécifiques au secteur des services financiers qui pourraient requérir une réponse stratégique globale. Si des produits financiers moins chers et plus pertinents, ainsi que l'accès au crédit pour les personnes ne disposant pas d'antécédents de crédit traditionnels, font partie des conséquences positives, les consommateurs ne sont en revanche pas toujours conscients de la mesure dans laquelle leurs données sont utilisées. Par exemple, ils risquent de se retrouver marginalisés en raison de pratiques opaques et potentiellement déloyales en matière d'exploration de données, ou exposés à la fraude et à la cybercriminalité.

Le présent rapport examine les risques et les avantages de ces évolutions technologiques et propose des options stratégiques pour protéger les consommateurs, combinant, d'une part, une protection solide des données financières et personnelles et, d'autre part, une plus grande sensibilisation ainsi qu'une meilleure éducation financière des consommateurs. Il a été conçu dans le cadre du groupe de travail consacré à la culture financière numérique du Réseau international sur l'éducation financière (INFE) de l'OCDE (voir l'annexe A pour la liste des membres).

Le rapport a été préparé par Andrea Grifoni, analyste des politiques à la direction des affaires financières et des entreprises de l'OCDE.

Table des matières

Contexte

Introduction

L'importance des données de caractère personnel n'a cessé de croître dans nos économies et nos sociétés. Si les nouvelles technologies et l'utilisation responsable des données procurent à la société et à l'économie d'importants avantages, l'abondance, la granularité et la permanence des données de caractère personnel entraînent de nouveaux risques pour le respect de la vie privée des personnes physiques. Les données de caractère personnel sont de plus en plus utilisées selon des modalités qui n'étaient pas prévues lors de leur création et de leur collecte, et les citoyens n'ont pas toujours connaissance de la façon dont leurs données sont recueillies, stockées et utilisées.

Ces tendances ont une incidence sur le secteur des services financiers et sur les consommateurs de ces services. Les innovations technologiques ont fortement amélioré la capacité des prestataires de services financiers à recueillir, stocker, combiner et analyser un éventail très élargi de données concernant leurs clients, allant de la localisation actuelle ou antérieure de ces derniers à leurs comportements et leurs préférences. Si ces évolutions peuvent procurer des avantages aux consommateurs, elles s'accompagnent également de nouveaux risques qui sont propres au secteur des services financiers et qui pourraient requérir une réponse stratégique spécifique.

La réponse à apporter aux conséquences de l'utilisation de données de caractère personnel dans le secteur des services financiers va au-delà de l'éducation financière. Elle suppose un cadre solide de protection financière des consommateurs qui soit apte à protéger ces derniers dans les environnements numériques, ainsi que l'existence d'agences nationales de protection des données ou de stratégies nationales de protection des données, dotées de ressources et de pouvoirs d'exécution efficaces, et nécessite de tenir compte des niveaux de culture numérique et financière.

Le présent rapport contribue, du point de vue de l'éducation financière, à déterminer des approches visant à encourager les comportements susceptibles de protéger les consommateurs et les entrepreneurs contre les conséquences négatives de ces évolutions dans le secteur financier.

Le rapport met tout d'abord en évidence les différents éléments d'une réponse stratégique, avant de définir les données de caractère personnel et de présenter les évolutions technologiques, économiques et sociétales qui ont mené à une croissance exponentielle de la génération de données de caractère personnel et de la capacité en matière de traitement des données.

L'analyse se concentre ensuite plus spécifiquement sur le secteur des services financiers, en expliquant comment les prestataires de services financiers collectent et utilisent les données de caractère personnel des consommateurs, avant d'aborder les conséquences de cette situation pour les consommateurs. Le rapport décrit en particulier les risques que peuvent courir les consommateurs, les décisions discriminatoires fondées sur l'utilisation des données massives et les menaces découlant de la cybercriminalité, avant de présenter la réaction des consommateurs face à ces évolutions, sur la base d'éléments recueillis dans le cadre d'enquêtes mondiales et nationales portant sur leurs attitudes à l'égard de l'utilisation de leurs données de caractère personnel.

À la lumière de ces évolutions et des questions qu'elles soulèvent, le présent rapport décrit des éléments spécifiques liés aux données de caractère personnel qui peuvent compléter la liste de mesures à prendre figurant dans la note d'orientation du G20/OCDE-INFE sur la numérisation et la culture financière (OCDE, 2018a).

Éléments d'un cadre stratégique pour l'utilisation des données de caractère personnel dans le secteur des services financiers

Protection de la vie privée et des données de caractère personnel

L'OCDE a joué un rôle pionnier dans les travaux menés au niveau international en matière de protection de la vie privée et des données de caractère personnel[1]. Ce processus a abouti, en 1980, à la Recommandation concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, révisée en 2013 (OCDE, 2013). L'environnement sociétal et technologique pour lequel ces Lignes directrices ont été élaborées a toutefois connu des changements structurels. Comme il a été souligné lors des travaux menés en 2013 en vue de la révision des Lignes directrices et de ses principes en matière de protection de la vie privée, les économies actuelles présentent des différences considérables en ce qui concerne :

- le volume de données de caractère personnel collectées, utilisées et stockées
- la diversité des analyses basées sur les données de caractère personnel, permettant de comprendre les tendances, mouvements, intérêts et activités aux niveaux individuel et collectif
- la valeur des avantages sociétaux et économiques procurés par les nouvelles technologies et par les utilisations responsables des données de caractère personnel
- l'étendue des menaces qui pèsent sur la vie privée
- le nombre et la diversité des acteurs en mesure de compromettre ou de protéger la vie privée
- la fréquence et la complexité des interactions faisant intervenir des données de caractère personnel que les personnes physiques sont supposées comprendre et négocier
- la diffusion mondiale des données de caractère personnel, grâce à des réseaux et des plates-formes de communication permettant des transferts de données continus et multipoints.

Les principes préconisent entre autres :

- de mettre à la disposition des personnes physiques les moyens raisonnables pour exercer leurs droits

[1] Parmi les autres instruments pertinents de l'OCDE dans ce domaine figurent les Orientations en matière de politique des consommateurs en ce qui concerne les paiements mobiles et en ligne (OCDE, 2014), la Recommandation de l'OCDE sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale (OCDE, 2015c) et la Recommandation de l'OCDE sur la protection du consommateur dans le commerce électronique (OCDE, 2016b). Ces principes, ainsi que les pratiques en la matière, ont servi de base à la boîte à outils du G20/de l'OCDE pour la protection des consommateurs numériques (OCDE, 2018e).

- d'adopter des mesures complémentaires, notamment d'éducation et de sensibilisation, de développement des compétences et de promotion de mesures techniques aidant à protéger la vie privée.

Protection financière des consommateurs

La protection de la vie privée et des données en rapport avec les services financiers peut être considérée comme faisant partie d'un cadre plus large de protection financière des consommateurs. Les principes de haut niveau G20/OCDE sur la protection financière des consommateurs (G20, 2011) abordent cette question au moyen du principe 8 « Protection des données relatives aux consommateurs et de leur vie privée ». Conformément à ce principe :

« Les informations financières et personnelles des consommateurs devraient être protégées grâce à des mécanismes appropriés de contrôle et de préservation. Ces mécanismes devraient être assortis de règles définissant dans quel but des données peuvent être recueillies, traitées, détenues, utilisées et communiquées (en particulier à des tiers). Ils devraient également reconnaître les droits des consommateurs à être informés des échanges de données, à accéder aux données et à obtenir la correction rapide ou la destruction des données inexactes ou bien recueillies ou traitées de manière illégale ».

La mise en œuvre de ce principe implique souvent l'existence d'autorités disposant d'un mandat légal pour assurer la protection des données de caractère personnel. De plus en plus, dans l'ensemble des juridictions, ce rôle incombe à une autorité chargée de la protection de la vie privée et des données (OCDE, 2019c). Ces autorités publiques indépendantes supervisent, grâce à leurs pouvoirs d'enquête et de rectification, l'application de la législation sur la protection des données, fournissent des conseils d'experts sur les questions relatives à la protection des données et traitent les plaintes.

Dans le cadre de ses travaux en cours sur la protection financière des consommateurs dans l'environnement numérique, le Groupe de réflexion sur la protection financière des consommateurs du G20/OCDE est en train d'élaborer des orientations stratégiques sur la protection des données et de la vie privée des consommateurs en ce qui concerne les consommateurs de services financiers, qui prendront la forme d'approches efficaces actualisées pour soutenir la mise en œuvre du principe 8.

Sensibilisation et éducation aux questions financières

La nécessité de renforcer la culture financière et la sensibilisation aux questions relatives aux données de caractère personnel a été abordée dans les travaux menés par l'OCDE/INFE et son groupe de travail sur la culture financière numérique.

Les orientations du G20/OCDE-INFE sur la numérisation et la culture financière (OCDE, 2018a), transmises aux dirigeants du G20 en juillet 2018, préconisent le développement de compétences de base spécifiques en matière de culture financière qui aideraient les consommateurs dans leur utilisation des services financiers numériques[2]. Deux aspects en particulier présentent un intérêt dans le contexte de l'utilisation des données de caractère personnel par les prestataires de services financiers :

- donner aux consommateurs, y compris aux plus vulnérables d'entre eux, les moyens de contrer les nouveaux types d'exclusion liés à l'utilisation abusive de

[2] Voir également le cadre G20/OCDE-INFE de compétences fondamentales en matière de culture financière pour les adultes (OCDE, 2016a) et pour les jeunes (OCDE, 2015a).

diverses sources de données, dont les données massives et le profilage numérique, et

- protéger les consommateurs et les petites entreprises contre une exposition accrue à la criminalité numérique, telle que l'hameçonnage, le piratage de compte et le vol de données.

1. Données de caractère personnel et services financiers

1.1. Qu'entend-on par « données de caractère personnel » ?

Les données de caractère personnel sont définies, par les Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (OCDE, 2013), comme « toute information relative à une personne physique identifiée ou identifiable (personne concernée) ». Toutes les données qui ne concernent pas une personne physique identifiée ou identifiable sont donc des données « de caractère non personnel ». Toutefois, l'analyse des données a facilité la mise en relation de données de caractère apparemment non personnel avec une personne physique identifiée ou identifiable, estompant ainsi les frontières entre les données de caractère non personnel et les données de caractère personnel (OCDE, 2015b).

En effet, le règlement général de l'Union européenne sur la protection des données (RGPD) (Union européenne, 2016) (voir encadré 6) définit les données de caractère personnel comme des « informations se rapportant à une personne vivante identifiée ou identifiable » et souligne que « différentes informations, dont le regroupement permet d'identifier une personne en particulier, constituent également des données à caractère personnel ». Le cadre de l'Union européenne souligne également que des données de caractère personnel qui ont été rendues anonymes ou chiffrées, mais qui peuvent être utilisées pour identifier à nouveau une personne, constituent toujours des données de caractère personnel et sont couvertes par la législation.

1.2. Quelles sont les contributions aux « données massives » dans le secteur des services financiers et comment sont-elles collectées ?

Dans les économies modernes, le secteur des services financiers est l'un des plus gourmands en données (OCDE, 2015b).

D'un point de vue centré sur le consommateur, les flux de données de caractère personnel entre le consommateur et les prestataires de services financiers peuvent être répartis en grandes catégories fondées sur la connaissance que le consommateur a ou non de ces flux (voir tableau 1).

Tableau 1. Canal de collecte de données en fonction de la connaissance qu'en a le consommateur

Connaissance du consommateur	Canaux de collecte de données
Le consommateur a connaissance des flux de données	Données fournies par le consommateur lors du processus de vérification de l'identité Données transmises par le consommateur à l'appui d'un achat de produit spécifique Données transmises par le consommateur pour utiliser un service spécifique comme les outils d'agrégation des données Données collectées lorsque le consommateur utilise des produits financiers spécifiques, tels que les services de paiement
Le consommateur n'a pas connaissance des flux de données	Données collectées par le prestataire lors des interactions avec les clients Données collectées par le prestataire à partir de sources d'information accessibles au public (réseaux sociaux) Données partagées avec le prestataire par des tiers, tels que les bureaux d'évaluation du risque de crédit

Comme on le verra dans la section suivante, la quantité d'informations que les consommateurs fournissent sans en avoir conscience (ou sans y avoir consenti) est en constante augmentation, en raison des évolutions technologiques qui imprègnent tous les aspects de nos sociétés et qui déterminent la génération et la capacité d'analyse de volumes croissants de données de caractère personnel.

Il importe toutefois de noter que même les informations fournies consciemment par les consommateurs contribuent à la création d'un référentiel de données concernant ces derniers : la numérisation des interactions des consommateurs avec les prestataires de services financiers permet à ces prestataires de recueillir et de stocker indéfiniment des informations sur les échanges entre clients et prestataires, leur nature, leur durée et leur contenu. Même l'appel d'un client au directeur de sa banque contribue à alimenter le référentiel de données relatives aux clients.

1.3. Accroissement de la génération de données de caractère personnel et de la capacité de traitement de celles-ci

1.3.1. Génération de nouvelles données de caractère personnel

Accès quasi universel au haut débit mobile et aux smartphones, mais avec des différences régionales et socio-économiques

Au cours de la dernière décennie, on a assisté à une augmentation constante et significative du nombre d'utilisateurs de l'internet. L'évolution de la technologie mobile a également accru les possibilités d'accéder au réseau « en déplacement », ainsi qu'à domicile. Les citoyens utilisent de plus en plus l'internet dans leur vie quotidienne, pour réaliser des transactions financières de toute nature et interagir avec les autorités publiques. Ces activités donnent lieu à la génération de nouvelles données de caractère personnel qui, à des degrés divers, peuvent être collectées et analysées par des tiers.

En 2005, environ 56 % de la population adulte des économies de l'OCDE avait accès à l'internet, et 30 % l'utilisait tous les jours. En 2016, ces pourcentages étaient respectivement passés à 83 % et 73 % (OCDE, 2017a). Que ce soit dans les économies matures ou dans les économies émergentes, le nombre d'abonnés à la téléphonie mobile a suivi la même tendance à la hausse et, d'ici 2025, le nombre d'abonnés uniques devrait atteindre 5.9 milliards de personnes, soit 71 % de la population mondiale (GSMA, 2018).

Ces tendances générales masquent toutefois des différences entre les pays et les secteurs de la population. Ainsi, en 2016, parmi les pays de l'OCDE, plus de 97 % de la population adulte avait accès à l'internet au Danemark, en Islande, au Japon, au Luxembourg et en Norvège, mais ce pourcentage était de 60 % ou moins au Mexique et en Turquie. Il existe également des différences d'utilisation : en Islande, en Italie, au Luxembourg et en Norvège, la part des utilisateurs quotidiens est très proche de celle des utilisateurs totaux, alors qu'au Mexique et en Turquie, de nombreux utilisateurs accèdent à l'internet de manière peu fréquente (OCDE, 2017a).

Les différences entre groupes d'utilisateurs sont principalement liées à l'âge et au niveau d'instruction, souvent combinés aux revenus. Si l'adoption de l'internet par les jeunes générations est presque universelle, la situation diffère pour les clients plus âgés : dans les pays de l'OCDE, plus de 95 % des 16-24 ans utilisaient l'internet en 2016, contre moins de 63 % des 65-74 ans. Chez les personnes plus âgées, le niveau d'instruction est le principal facteur influençant l'utilisation de l'internet : les taux d'utilisation pour les 55-74 ans ayant un diplôme de l'enseignement supérieur sont généralement supérieurs ou équivalents à ceux de la population générale, et, dans certains pays, ils sont proches de ceux observés chez les 16-24 ans.

L'internet des objets

Les objets et appareils connectés que les consommateurs achètent et utilisent constituent une autre source de données relatives aux consommateurs. L'internet des objets (IDO) désigne l'ensemble des appareils et objets dont l'état peut être modifié via l'internet, avec ou sans la participation active des utilisateurs. Bien que les objets connectés puissent nécessiter l'utilisation d'appareils considérés comme faisant partie de l'« internet traditionnel », cette définition exclut les ordinateurs portables, tablettes et smartphones, qui relèvent déjà des indicateurs actuels de l'OCDE concernant le haut débit (OCDE, 2018c).

Ce réseau d'objets connectés à l'internet est en mesure de collecter et d'échanger des données à l'aide de capteurs intégrés et de contribuer à la collecte d'informations sur la localisation et les comportements des clients : systèmes d'assurance télématiques qui enregistrent les comportements des conducteurs de voitures, équipements portables intelligents capables d'enregistrer des informations relatives à la santé, telles que la distance parcourue chaque jour ou l'activité physique, et systèmes domotiques intelligents. À l'échelle mondiale, le nombre d'appareils connectés devrait atteindre 50 milliards d'ici à 2020, contre 9 milliards en 2013 (OCDE, 2017a).

Il est possible que les consommateurs ne puissent pas choisir ce qu'ils partagent au moyen d'un appareil connecté à l'IDO ; l'appareil capte et transfère en permanence des informations, de manière discrète et en arrière-plan (OCDE, 2018d), ce qui crée de nouveaux risques pour les consommateurs. Alors qu'un nombre sans cesse croissant d'appareils deviennent « intelligents » (c'est-à-dire connectés), les individus risquent de ne plus être en mesure de comprendre la quantité de données partagées et leurs conséquences en matière de respect de la vie privée, et encore moins de surveiller le flux de ces données et d'exercer un certain contrôle sur celles-ci. Il est en outre peu probable que les consommateurs aient pleinement conscience de ce qui est fait avec les données collectées (Rosner et Kenneally, 2018). De plus, les données de l'IDO pourraient être plus facilement piratées.

Biométrie

Les données biométriques constituent une source supplémentaire de données de caractère personnel. Elles proviennent principalement des processus d'authentification de l'identité au moyen de caractéristiques physiques ou comportementales uniques (par exemple, reconnaissance faciale, empreintes digitales ou reconnaissance vocale). Ces données n'avaient jamais été générées auparavant et, si elles l'avaient été (comme les empreintes digitales), elles n'avaient pas été numérisées, ce qui signifie qu'elles peuvent exister sans cadre stratégique clair.

La biométrie comporte encore un autre risque. À l'inverse des mots de passe, qui peuvent être modifiés après un piratage, l'authentification biométrique n'est pas si facile à modifier.

Encadré 1. Les données massives

Les activités économiques et sociales ont déjà migré ou migrent de plus en plus vers l'internet. Cette évolution se déroule sur fond d'une baisse spectaculaire et continue du coût de la collecte, du stockage et du traitement des données. En outre, de nouvelles sources de données apparaissent et des volumes toujours plus importants de données seront générés par l'internet des objets, les appareils intelligents et les communications autonomes entre machines.

Ces énormes volumes de données générés, atteignant des niveaux sans précédent dans l'histoire de l'humanité, sont souvent appelés « données massives ». L'OCDE définit les données massives comme suit :

> *L'expression « données massives » désigne les volumes considérables de données générées par les activités menées dans l'environnement électronique et les communications intermachines (données produites dans le cadre des activités sur les médias sociaux, des processus de production, etc.).*
>
> *Les caractéristiques des données massives se résument en « 3V » (volume, variété et vélocité) :*
>
> - *le premier V fait référence aux volumes considérables de données générés dans le temps*
> - *le deuxième renvoie à la variété des formats des données complexes, qui peuvent être structurées ou non (textes, vidéos, images, voix, documents, données de capteurs, journaux d'activités, historique de parcours sur le web, coordonnées, etc.)*
> - *le troisième V désigne la vitesse à laquelle les données sont générées, sont mises à disposition et évoluent dans le temps* (OCDE, 2015b).

Les données massives contrastent avec le traitement de données axé sur des ensembles de données peu diversifiés, (relativement) limités en volume et statiques, comme les enquêtes de satisfaction des clients.

1.3.2. Progrès dans l'analyse des données

Ces volumes importants de données n'auraient aucune valeur économique ou sociale, ni de conséquence pour les consommateurs de services financiers, s'ils n'étaient pas accompagnés de capacités d'analyse croissantes.

L'analyse prédictive renvoie globalement aux technologies et procédures utilisées pour traiter de grands volumes de données afin de mettre au jour des schémas ou des corrélations, et, surtout, de prédire les événements à venir de manière plus précise et en temps opportun.

Les progrès sont les plus significatifs, et ont les conséquences les plus importantes pour le secteur des services financiers, dans les domaines suivants (OCDE, 2015a) :

- *Exploration de données* : l'ensemble de techniques utilisées pour dégager des schémas d'information à partir d'ensembles de données.
- *Profilage* : l'utilisation de l'analyse de données pour établir des profils et classer les consommateurs individuellement dans des profils spécifiques. L'évaluation du risque de crédit, la différenciation des prix et les publicités ciblées sont des exemples typiques d'activités faisant appel au profilage.
- *Apprentissage automatique ou statistique* : sous-domaine de la science informatique, et plus particulièrement de l'intelligence artificielle. Il a trait à la conception, au développement et à l'utilisation d'algorithmes[3] qui permettent aux ordinateurs d'« apprendre » c'est-à-dire, de réaliser certaines tâches tout en améliorant leurs performances avec chaque ensemble de données empiriques qu'ils analysent. L'apprentissage automatique implique des activités telles que la classification de formes, l'analyse par grappes et la régression.

Ces progrès permettent aux prestataires de services financiers de déduire des informations sensibles à partir de données qui ne sont pas liées au profil d'un individu en matière de services financiers, telles que le comportement d'achat passé de cet individu, sa consommation électrique ou les activités de ses cercles de contacts sur les réseaux sociaux.

[3] On peut décrire un algorithme comme « une procédure de calcul bien définie qui utilise, comme entrée, une certaine valeur, ou un certain ensemble de valeurs, pour produire, comme sortie, une certaine valeur ou un certain ensemble de valeurs. L'algorithme est donc une séquence d'étapes de calcul qui permet de transformer l'entrée en sortie » (Cormen et al., 2009).

Encadré 2. Le développement des technologies des chaînes de blocs*

Bien qu'il ne s'agisse pas à proprement parler d'une innovation entraînant la génération de données de caractère personnel, mais plutôt d'un moyen de stocker ces dernières, les chaînes de blocs constituent une évolution à prendre en considération par les personnes chargées de définir les politiques en matière d'éducation financière lorsqu'elles se penchent sur les questions liées à l'utilisation des données de caractère personnel.

Les chaînes de blocs constituent une technologie présentant un très fort potentiel dans un large éventail d'applications. Elles reposent sur la technologie des registres distribués (DLT) pour stocker des informations vérifiées par cryptographie, validées au moyen d'un protocole de réseau prédéfini, souvent sans le contrôle d'une autorité centrale. Cette technologie peut être utilisée pour sécuriser le transfert et la traçabilité de valeurs ainsi que le transfert de données. La nature distribuée de ses nœuds la rend attrayante du point de vue de la cybersécurité et de la protection de la vie privée.

Le point essentiel à noter en ce qui concerne cette technologie est que les informations de caractère personnel stockées sur la chaîne de blocs, étant donné la nature décentralisée de cette dernière, constituée de blocs immuables, ne peuvent pas être supprimées, ces blocs étant conçus pour durer indéfiniment.

* Pour en savoir plus sur les évolutions de la technologie et de la politique liées aux chaînes de blocs, voir www.oecd.org/daf/blockchain/.

1.4. Utilisation des différentes sources de données de caractère personnel par les prestataires de services financiers

La masse croissante de données de caractère personnel des consommateurs, et la possibilité de les analyser au moyen d'outils de plus en plus sophistiqués et de l'intelligence artificielle, peuvent être utilisées par les prestataires de services financiers, en fonction du cadre réglementaire, aux fins des activités et services suivants en particulier :

- Profilage des clients : les données provenant du comportement en ligne, des outils de géolocalisation, des paiements électroniques et des dispositifs portables peuvent fournir aux prestataires de services financiers des informations précieuses sur la vie financière de leurs clients et permettre une segmentation plus fine de leur clientèle.
- Évaluation des risques : les données contribuent à l'évaluation des risques sur la base de sources multiples.
    - Crédit : dans les juridictions où des systèmes d'évaluation positive du risque de crédit existent (c'est-à-dire dans lesquelles une autorité centrale n'indique pas seulement les notes de crédit négatives), les données massives et les analyses étendues ont permis l'émergence d'outils d'évaluation du risque de crédit qui intègrent des milliers de points d'information sur les individus.
    - Assurances : les prestataires pourraient utiliser l'agrégation des données aux fins de l'évaluation des risques dans de nombreux domaines, pour parvenir à une segmentation des risques et une tarification fondée sur les risques plus précises. Par exemple, les données générées par les capteurs d'activité ou les traceurs d'activité physique sur un téléphone portable peuvent être utilisées pour déterminer l'espérance de vie potentielle d'un preneur d'assurance. L'analyse des données peut également être appliquée aux données télématiques qui suivent le comportement des preneurs d'assurance et utilisée pour atténuer

les risques à l'avance, par exemple, en fonction de la localisation. Cela peut s'appliquer à une série de produits d'assurance, tels que l'assurance santé (où le comportement du consommateur est suivi et récompensé au moyen de dispositifs portables et/ou de capteurs connectés à domicile), l'assurance automobile (assurance au kilomètre et télématique) ou l'assurance habitation (OCDE, 2017b).

La technologie de reconnaissance faciale et les données relatives à la longévité peuvent être utilisées pour la souscription des assurances vie. La technologie de reconnaissance faciale est utilisée pour prédire des facteurs tels que l'âge chronologique, le genre, les habitudes de tabagisme et l'indice de masse corporelle (IMC) (OCDE, 2017b).

- Robot-conseils utilisés pour élaborer un plan financier personnel en vue d'une épargne, d'une épargne-retraite ou d'un investissement. Les données relatives aux consommateurs sont traitées par les plates-formes de robot-conseil afin de mieux comprendre les besoins de clients et d'évaluer leur tolérance au risque, ainsi que de suivre et d'ajuster le plan financier (OCDE, 2017c).
- La détection des fraudes, grâce au suivi presque instantané autorisé par l'intelligence artificielle (IA) et, en particulier, l'apprentissage automatique, qui permet une analyse continue des schémas de dépenses et de gestion des comptes.
- L'agrégation de comptes, c'est-à-dire le regroupement d'informations provenant de différents comptes (comptes-chèques, investissements, comptes d'épargne) en un seul endroit pour faciliter la gestion des finances personnelles (voir encadré 3).

Encadré 3. Outils d'agrégation de comptes

Les outils d'agrégation de comptes, qui permettent aux consommateurs d'accéder à leurs comptes (comptes bancaires, comptes d'épargne, investissements, etc.) en un seul endroit, par l'intermédiaire d'un site internet ou d'une application mobile, peuvent fonctionner au moyen de deux mécanismes :

- La capture de données d'écran (*screen scraping*), par laquelle les clients fournissent à des tiers leurs données de connexion, mots de passe et autres informations de sécurité, comme les questions personnelles, que ces tiers pourront utiliser pour se connecter à la place des clients.
- La banque ouverte, comme dans l'Union européenne (Union européenne, 2015). Dans ce cas, les clients ne doivent pas fournir leurs mots de passe à des tiers pour qu'ils accèdent à leurs comptes en leur nom, et les mots de passe ne sont pas partagés. Les tiers, qui sont agréés par l'autorité responsable des services financiers, se connectent directement aux banques des clients, au moyen d'interfaces de programmation (API) standard.

La banque ouverte peut offrir des capacités renforcées au marché et permettre aux consommateurs d'accéder à tous leurs comptes (comptes en banque, compte d'épargne, investissements, etc.) en un seul endroit, par l'intermédiaire d'un site internet ou d'une application mobile. Elle peut ainsi contribuer à l'émergence de produits et services améliorés et innovants, au renforcement du contrôle que les consommateurs ont sur leur vie financière et à un accroissement de la concurrence dans la fourniture des services financiers, avec l'entrée de nouveaux acteurs sur le marché et, en réaction, l'innovation des acteurs en place.

Le principal aspect à prendre en considération du point de vue de l'éducation financière est le consentement* et l'autorisation des consommateurs, ainsi que les questions liées au contrôle des consommateurs. Tout prestataire souhaitant accéder aux informations financières liées au compte d'un consommateur doit demander une autorisation, qui peut se limiter à l'extraction des informations, ou aller plus loin et porter également sur des services de paiement, par exemple.

Les consommateurs ne devraient pas se sentir forcés d'accorder l'accès à des informations de caractère personnel sensibles, comme les anciens extraits de compte, à moins qu'ils en aient conscience et en comprennent les conséquences. Ils devraient également savoir que, selon des modalités différentes en fonction de la réglementation applicable, ils ont le droit de révoquer l'autorisation d'accès à leurs données ainsi que d'utilisation ou de stockage de celles-ci.

* Voir, par exemple, le cadre réglementaire introduit par la Reserve Bank of India pour les agrégateurs de comptes en septembre 2016 (RBI, 2016), qui prévoit, entre autres, des dispositions concernant le consentement explicite des clients, ainsi que la garantie de la protection des droits des clients, la sécurité des données et un mécanisme de réparation des préjudices pour les clients.

1.5. Quelles sont les conséquences pour les consommateurs ?

Les conséquences de l'utilisation accrue de données de caractère personnel dans les services financiers peuvent être positives pour les consommateurs, si cette utilisation s'inscrit dans un cadre solide de protection financière des consommateurs et s'accompagne d'une culture et d'une sensibilisation financières suffisantes. Toutefois, l'utilisation accrue des données de caractère personnel entraîne également de nouveaux risques, qui appellent une réponse intégrée englobant l'éducation et la sensibilisation aux questions financières et la protection financière des consommateurs[4].

1.5.1. Produits moins chers et sur mesure, d'une portée élargie

Les avantages qu'apportent aux consommateurs la numérisation des finances et l'utilisation croissante qui peut être faite des données de caractère personnel ont été présentés dans la note d'orientation du G20/OCDE-INFE sur la numérisation et la culture financière. Parmi ces avantages, ceux qui sont le plus influencés par la disponibilité accrue de données de caractère personnel et l'amélioration des outils d'analyse de données sont les suivants :

- l'accès à certains services financiers pour des consommateurs qui en sont actuellement exclus, par exemple grâce à l'utilisation des données massives qui peuvent exploiter des points d'information non financière pour élaborer un autre système d'évaluation du risque de crédit pour les consommateurs qui n'ont pas d'antécédents de crédit ;
- l'offre de transactions plus pratiques, plus rapides, sûres et intervenant en temps voulu ;
- l'élargissement de la gamme de prestataires, avec l'entrée de nouvelles entreprises de technologie financière sur le marché.

Cette évolution a déjà eu des effets bénéfiques pour les consommateurs :

- une baisse des coûts, grâce à une concurrence accrue et à l'émergence d'entreprises de technologie financière, en particulier dans les secteurs des paiements et des prêts ;
- des services d'agrégateur qui utilisent les données financières et de paiement provenant des comptes bancaires des consommateurs pour offrir des produits de type « tableau de bord » et des produits comptables ;
- des robot-conseils, grâce auxquels les consommateurs qui n'avaient pas les moyens d'obtenir les conseils financiers d'un acteur humain ont pu bénéficier de conseils financiers (OCDE, 2017c) ;
- la possibilité de créer des incitations personnalisées intégrées dans les outils de gestion financière personnelle utilisés par les consommateurs.

Toutefois, la disponibilité accrue de données de caractère personnel et la capacité de traitement renforcée donnent également aux prestataires de services financiers (qu'il s'agisse d'entreprises traditionnelles ou d'entreprises de technologie financière) la possibilité d'envoyer des offres ciblées, ce qui peut compliquer la comparaison des produits

[4] Pour une analyse des risques en matière de respect de la vie privée et de sécurité courus par les consommateurs dans l'environnement numérique, voir également les orientations en matière de politique des consommateurs en ce qui concerne les paiements mobiles et en ligne (OCDE, 2014).

pour les consommateurs, en particulier pour ceux qui ont un faible niveau de culture et de connaissances financières.

1.5.2. Utilisation des données massives et de l'apprentissage automatique pour éclairer les décisions en matière de crédit ou d'assurance

En fonction du cadre réglementaire applicable dans chaque juridiction, les données massives et l'apprentissage automatique peuvent être utilisés pour déterminer le profil de risque des consommateurs ou alimenter ce profil, notamment dans le domaine du crédit et de l'assurance.

Si l'analyse des données de caractère personnel pour déterminer le profil de risque des clients n'est pas une pratique nouvelle, elle peut désormais se faire au moyen d'une série de points de données recueillis à propos des consommateurs individuels, dont ceux-ci peuvent ne pas être pleinement informés. Selon l'algorithme utilisé, cette analyse peut également prendre la forme de la déduction d'informations sur le consommateur à partir de données relatives aux consommateurs figurant dans des ensembles de données similaires.

De plus en plus souvent, les méthodes d'analyse établissent un lien entre différents ensembles de données et éléments d'information provenant de sources différentes, d'une manière qui n'était pas possible auparavant. De ce fait, la distinction entre données de caractère personnel et autres données est brouillée et des données de caractère non personnel permettent de plus en plus de remonter jusqu'aux individus, ce qui élargit les possibilités d'analyse des prestataires de services financiers (OCDE, 2019b).

Dans le secteur des assurances, la segmentation des risques et l'efficacité accrue de la sélection des risques peuvent permettre aux assureurs de déterminer à l'avance quels preneurs d'assurance sont susceptibles de subir des sinistres. Sur cette base, certains clients peuvent se voir proposer d'excellents tarifs, tandis que d'autres peuvent être exclus des services d'assurance.

Dans le secteur du crédit, l'utilisation de données de substitution peut avoir d'importantes conséquences sur les évaluations du risque de crédit. Les informations traditionnelles en matière de crédit, obtenues à partir de l'utilisation des cartes de crédit et de l'historique des paiements, peuvent être combinées avec des points de données provenant des activités en ligne et hors ligne des consommateurs. La plupart de ces données n'ont pas nécessairement de lien direct avec la solvabilité des individus ; il peut s'agir de l'endroit où les consommateurs font leurs achats, de ce qu'ils achètent, de leurs réseaux sociaux et des activités de leurs contacts sociaux et/ou de personnes sur des réseaux numériques similaires. Les fournisseurs de crédit aux États-Unis ont fait état d'une augmentation de 15 % de la fiabilité des prévisions concernant les consommateurs[5].

Les recherches menées sur la solvabilité des clients en ligne d'une entreprise allemande de commerce électronique (Berg et al., 2018) montrent le pouvoir discriminatoire supérieur d'un modèle utilisant à la fois les notations des agences d'évaluation du crédit et les variables de l'empreinte numérique[6], ce qui donne à penser qu'un prêteur qui utilise des

[5] « Equifax and SAS leverage AI and deep learning to improve consumer access to credit », Forbes, 20 février, https://www.forbes.com/sites/gilpress/2017/02/20/equifaxand-sas-leverage-ai-and-deep-learning-to-improve-consumer-access-tocredit/2/#2ea15ddd7f69.

[6] Les variables prises en compte par l'étude se concentrent uniquement sur les interactions avec cette entreprise et sont les suivantes : le type d'appareil (tablette ou téléphone portable), le système d'exploitation (iOS ou Android), le canal par lequel le client arrive sur le site internet (par exemple moteur de recherche ou site de

informations provenant des deux sources peut prendre des décisions de prêt plus rentables, mais aussi plus exclusives.

Toutefois, des recherches récentes mettent également en évidence d'éventuels effets discriminatoires supplémentaires découlant de l'utilisation des données massives, tels que l'exclusion « par association », c'est-à-dire lorsque les liens sociaux, familiaux ou religieux des consommateurs ont une incidence sur l'évaluation de leur solvabilité (Hurley et Adebayo, 2017). En outre, il est possible que la manière dont des données non traditionnelles sont utilisées et analysées, qui n'est pas toujours réglementée dans toutes les juridictions, ne soit pas transparente pour les consommateurs (ni pour les régulateurs), car reposant sur des outils analytiques propriétaires. Le traitement de ces données est susceptible de se dérouler sans les protections concernant l'exactitude, les limitations d'utilisation, l'accès et les litiges applicables, par exemple, aux agences d'évaluation du risque de crédit. Dans ces cas, les consommateurs ne sont pas en mesure de contester ce qui pourrait constituer une décision injuste, ni de comprendre ce qu'ils peuvent faire pour obtenir une meilleure évaluation de leur solvabilité.

comparaison des prix), une variable fictive « do not track » égale à un si le client applique des paramètres qui ne permettent pas de suivre les informations sur l'appareil, le système d'exploitation ou le canal utilisés, le moment de la journée où l'achat est effectué (par exemple le matin, l'après-midi, le soir ou la nuit), le fournisseur de courrier électrique (par exemple Gmail ou Yahoo), deux informations concernant l'adresse de courrier électronique choisie par l'utilisateur (inclut le prénom et/ou le nom de famille et inclut un chiffre), une variable fictive « minuscule » si l'utilisateur écrit systématiquement en minuscules et une variable fictive en cas d'erreur de frappe lors de la saisie de l'adresse de courrier électronique.

Encadré 4. Approche responsable à l'appui d'une IA digne de confiance

En septembre 2018, l'OCDE a créé un groupe d'experts sur l'IA composé de plus de 50 membres, rassemblant des représentants de 20 gouvernements et des responsables du monde des entreprises et du travail, de la société civile, des milieux universitaires et de la communauté scientifique.

La raison d'être de la création de ce groupe et des travaux ultérieurs réside dans la reconnaissance du fait que l'IA a des incidences mondiales généralisées et profondes qui transforment les sociétés et les secteurs économiques. Ces incidences ont le potentiel d'améliorer la prospérité et le bien-être, mais pourraient également avoir des effets disparates au sein de nos sociétés et de nos économies, notamment en termes de mutations économiques, de concurrence, de transitions sur les marchés du travail, d'inégalités, et de conséquences sur la démocratie et les droits de l'homme, la protection de la vie privée et la confidentialité des données, et la sécurité numérique.

Les efforts déployés par les pays de l'OCDE dans ce domaine ont abouti à l'approbation, en juin 2019, de la Recommandation du Conseil sur l'intelligence artificielle (OCDE, 2019a), qui inclut les principes de l'OCDE en matière d'IA. Les membres de l'OCDE, ainsi que l'Argentine, le Brésil, la Colombie, le Costa Rica, le Pérou et la Roumanie, ont adhéré aux principes en matière d'IA.

Deux de ces principes sont particulièrement pertinents dans le domaine des données de caractère personnel et des services financiers :

Valeurs centrées sur l'humain et équité

- *Les acteurs de l'IA devraient respecter l'état de droit, les droits de l'homme et les valeurs démocratiques tout au long du cycle de vie des systèmes d'IA. Ces droits et valeurs comprennent la liberté, la dignité et l'autonomie, la protection de la vie privée et des données, la non-discrimination et l'égalité, la diversité, l'équité, la justice sociale, ainsi que les droits des travailleurs reconnus à l'échelle internationale.*
- *Pour ce faire, les acteurs de l'IA devraient instituer des garanties et des mécanismes, tels que l'attribution de la capacité de décision finale à l'homme, qui soient adaptés au contexte et à l'état de l'art.*

Transparence et explicabilité

Les acteurs de l'IA devraient s'engager à assurer la transparence et une divulgation responsable des informations liées aux systèmes d'IA. À cet effet, ils devraient fournir des informations pertinentes, adaptées au contexte et à l'état de l'art, afin :

- *de favoriser une compréhension générale des systèmes d'IA,*
- *d'informer les parties prenantes de leurs interactions avec les systèmes d'IA, y compris dans la sphère professionnelle,*
- *de permettre aux personnes concernées par un système d'IA d'en appréhender le résultat, et*
- *de permettre aux personnes subissant les effets néfastes d'un système d'IA de contester les résultats sur la base d'informations claires et facilement compréhensibles sur les facteurs, et sur la logique ayant servi à la formulation de prévisions, recommandations ou décisions.*

La Recommandation appelle également les pouvoirs publics à « travailler en étroite collaboration avec les parties prenantes en vue de préparer la transformation du monde du travail et de la société. Ils devraient donner aux personnes les moyens d'utiliser et d'interagir efficacement avec les systèmes d'IA au travers de leurs différentes applications, notamment en les dotant des compétences nécessaires ».

Source : OCDE (2019a), Recommandation du Conseil sur l'intelligence artificielle, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0449

1.5.3. Augmentation des risques de sécurité numérique

La numérisation de nos économies et de la finance enrichit le volume de données stockées par les institutions financières et offre de nouveaux moyens d'y accéder. En raison de la valeur des informations stockées dans leurs systèmes informatiques, les institutions financières sont des cibles rentables pour les cybercriminels (voir encadré 5). L'intensité de données (mesurée en volume moyen de données stockées par organisation) est la plus élevée dans le secteur des services financiers (couvrant les services liés aux valeurs mobilières et les services d'investissement, ainsi que les services bancaires) (OCDE, 2015b).

Rien qu'au Royaume-Uni, le nombre de violations de données signalé par les entreprises de services financiers à la Financial Conduct Authority (FCA) a augmenté de 480 % en 2018 par rapport à 2017, passant de seulement 25 à 145[7].

[7] https://www.rpc.co.uk/press-and-media/data-breaches-reported-by-financial-services-firms-rise-480-percent-in-a-year-to-145/

Encadré 5. Incidents de sécurité numérique dans les services financiers

Les incidents de sécurité numérique portant atteinte à l'intégrité, à la disponibilité et à la confidentialité des données stockées par les prestataires de services financiers sont devenus de plus en plus courants et sont en augmentation au niveau mondial. Ci-après figure une liste non exhaustive des incidents de sécurité majeurs ayant touché des entreprises de services financiers ces dernières années :

- En 2014, les données de 20 millions d'individus, soit 40 % de la population coréenne, ont été volées auprès de trois sociétés coréennes de cartes de crédit[1] (KB Kookmin Bank, Lotte Card et Nonghyup Bank). Les données de caractère personnel incluaient les numéros d'identification, les adresses et les numéros de carte de crédit.
- En 2014, JP Morgan Chase, la plus grande banque de détail aux États-Unis, a été victime d'un piratage qui a compromis les données de plus de la moitié des ménages américains, soit 76 millions, et de 7 millions de petites entreprises[2]. Ces données comprenaient des coordonnées (noms, adresses, numéros de téléphone et adresses électroniques) ainsi que des informations internes sur les utilisateurs.
- En 2016, Tesco Bank a été victime d'une cyberattaque qui a touché 8 261 des 131 000 comptes courants personnels de Tesco Bank[3]. Bien que les contrôles de la banque aient permis d'arrêter près de 80 % des transactions non autorisées, les titulaires de comptes courants personnels ont reçu très tôt le matin des SMS susceptibles de les inquiéter. Certains clients ont connu des désagréments, étant dans l'impossibilité d'effectuer des paiements au moyen de leurs cartes de débit.
- En 2017, des pirates ont volé les données de caractère personnel de près de 150 millions de personnes dans les bases de données de la société Equifax, une société d'évaluation du risque de crédit à la consommation[4].

1. www.economist.com/finance-and-economics/2014/01/25/card-sharps
2. https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/
3. www.fca.org.uk/publication/final-notices/tesco-personal-finance-plc-2018.pdf
4. www.gao.gov/assets/700/694158.pdf

1.6. Attitude des consommateurs à l'égard du respect de la vie privée et de la marchandisation des données

La réaction des consommateurs face à ces évolutions ainsi qu'aux possibilités et aux risques que représentent les données massives est contrastée : la majorité des consommateurs sont conscients des menaces qui pèsent sur le respect de leur vie privée, mais ils sont également disposés à partager des informations personnelles supplémentaires en échange de services de meilleure qualité et moins chers. Toutefois, des recherches récentes indiquent que, lorsque les consommateurs consentent à partager leurs données avec des prestataires, ils ne comprennent pas les modalités et conditions de ce partage, y compris la déclaration de confidentialité.

1.6.1. Préoccupations en matière de confidentialité des données et sensibilisation aux risques de sécurité numérique[8]

Les données disponibles indiquent que les consommateurs sont attachés au respect de leur vie privée et sont conscients de la manière dont il peut être compromis dans l'environnement technologique actuel. Ils s'inquiètent de la façon dont leurs données de caractère personnel peuvent être consultées et utilisées illégalement et sont conscients des risques que représente la cybercriminalité (accès à leurs comptes, utilisation malveillante de leurs données de caractère personnel).

Les consommateurs ont conscience des risques croissants qui pèsent sur l'intégrité de leurs données de caractère personnel et sur le respect de leur vie privée. Une enquête réalisée en 2018 par CIGI-Ipsos, intitulée « Global Survey on Internet Security and Trust »[9], a montré que plus de la moitié des internautes interrogés dans le monde étaient davantage préoccupés par le respect de leur vie privée en ligne qu'ils ne l'étaient l'année précédente. Dans un rapport Eurobaromètre spécial de 2014 sur la sécurité numérique, les consommateurs en ligne dans l'Union européenne ont indiqué que leurs deux principales préoccupations concernaient l'utilisation malveillante de leurs données de caractère personnel et la sécurité des paiements en ligne (CE, 2015). Les enquêtes nationales confirment ces tendances : au Royaume-Uni, par exemple, 42 % des personnes interrogées pensent qu'il est probable qu'elles soient victimes d'actes de cybercriminalité au cours des deux prochaines années (Ipsos MORI, 2019).

En fait, selon une étude mondiale récente menée par le secteur privé sur le comportement et les préférences des consommateurs de services financiers (Accenture, 2019), les préoccupations liées à la sécurité des données (fuites de données, piratage, etc.) constituent la deuxième raison principale pour laquelle un consommateur pourrait quitter son prestataire actuel.

En dépit de ces préoccupations, tous les consommateurs n'appliquent pas les mesures nécessaires pour protéger leurs données de caractère personnel en ligne. Au Royaume-Uni, par exemple, près de la moitié d'entre eux n'utilisent pas toujours un mot de passe fort et distinct pour leur compte de courrier électronique principal. En outre, seuls 15 % des consommateurs disent avoir des connaissances étendues sur la manière de se protéger contre les activités dommageables, 33 % environ indiquant faire appel à des amis ou de la famille pour obtenir de l'aide dans le domaine de la cybersécurité (Ipsos MORI, 2019).

Différences de perception des risques et de réaction entre les publics cibles

Pour les responsables des politiques en matière d'éducation financière, il importe de noter qu'il existe des différences de perception des risques de sécurité en ligne. Selon une enquête récente menée au Royaume-Uni (Ipsos MORI, 2019), 37 % des consommateurs interrogés sont d'accord avec l'affirmation selon laquelle « perdre de l'argent ou des données personnelles sur l'internet est inévitable de nos jours ». Les personnes qui sont tout à fait d'accord avec cette affirmation sont généralement des personnes de plus de 65 ans ou sans diplôme.

Il convient également de souligner des différences entre les publics cibles en ce qui concerne les stratégies adoptées par les consommateurs pour réduire au minimum la

[8] Pour de plus amples informations sur la sécurité numérique et le respect de la vie privée, voir www.oecd.org/going-digital/topics/digital-security-and-privacy/

[9] https://www.cigionline.org/internet-survey-2018

probabilité d'être victime de cybercriminalité. En effet, si les consommateurs sont préoccupés par le respect de leur vie privée, tous ne prennent pas de mesures pour protéger celle-ci. Des enquêtes menées aux États-Unis (Pingitore et al, 2017) et au Royaume-Uni (Ipsos MORI, 2019) montrent que les jeunes consommateurs prennent des mesures plus proactives pour protéger leur vie privée en ligne, par exemple en adaptant les paramètres de confidentialité sur leur téléphone portable ou sur les réseaux sociaux.

1.6.2. Échanger des données de caractère personnel contre des avantages supplémentaires

Les informations disponibles indiquent que les consommateurs sont également disposés à partager des données de caractère personnel supplémentaires avec les prestataires de services financiers si ce partage se traduit par des avantages perçus. Deux enquêtes mondiales menées par le secteur privé ont mis cette tendance en lumière.

La première porte sur le partage de données en général et n'est pas axée sur les seuls services financiers (GfK, 2017). Elle montre que plus d'un quart (27 %) des internautes dans 17 pays sont tout à fait d'accord pour partager leurs données de caractère personnel en échange d'avantages ou de récompenses, telles que des coûts moins élevés ou des services personnalisés. Le pourcentage d'internautes résolument opposés au partage de leurs données est d'environ 19 %. L'enquête révèle également que les internautes âgés de 30 à 40 ans sont les plus susceptibles de partager des données en échange de récompenses.

La seconde enquête porte spécifiquement sur le secteur des services financiers (Accenture, 2019). Elle révèle qu'environ 60 % des consommateurs interrogés dans le monde indiquent qu'ils partageraient plus de données avec les banques, les assureurs ou les sociétés de conseil en investissement si cela leur permettait de bénéficier de services prioritaires, de tarifs avantageux, de produits plus personnalisés ou de conseils financiers non réglementés. Ce pourcentage est plus élevé pour les catégories de consommateurs plus jeunes et plus férus de numérique. Ces consommateurs ne sont pas opposés à l'idée d'effectuer des transactions financières par l'intermédiaire des GAFA (Google LLC, Apple, Inc., Facebook, Inc. et Amazon.com). Pour ces consommateurs, et pour les générations nées après 1990 en particulier, les GAFA constituent également des solutions de remplacement attrayantes aux prestataires traditionnels de services financiers, 40 % d'entre eux indiquant qu'ils envisageraient d'effectuer des opérations bancaires avec Facebook, Google ou Amazon. Ce pourcentage est encore plus élevé sur des marchés tels que les États-Unis, où 50 % seraient disposés à franchir le pas (Accenture, 2019).

1.6.3. Le consentement n'est pas éclairé

Ces évolutions ont lieu bien que les consommateurs ne comprennent pas pleinement la valeur de leurs données de caractère personnel. Des recherches menées au Royaume-Uni (Financial Services Consumer Panel, 2018) visant à évaluer dans quelle mesure les consommateurs sont disposés à partager leurs données avec des tiers dans le cadre de la banque ouverte confirment que le consentement des consommateurs est mal éclairé. Plus de trois quarts des consommateurs (même parmi ceux ayant un niveau socio-économique et un niveau d'instruction assez élevés) déclarent ne pas se sentir informés lorsqu'ils lisent les modalités et conditions du partage de données. En outre, la plupart des consommateurs qui consentent au traitement de leurs données de caractère personnel par des prestataires tiers ne comprennent pas certaines des modalités et conditions qu'ils ont acceptées et indiquent donc que leur consentement n'est pas éclairé.

Enfin, ils ne savent pas exactement dans quelle mesure ils peuvent exercer un contrôle sur l'utilisation de leurs données, pas plus qu'ils ne connaissent précisément les droits qu'ils ont sur ces dernières. Ce point est particulièrement pertinent pour les personnes chargées de définir les politiques en matière d'éducation et de sensibilisation aux questions financières, étant donné que les récentes évolutions marquantes dans la réglementation de la protection de la vie privée et de l'utilisation des données de caractère personnel visent à conférer davantage de contrôle et de droits aux consommateurs (voir encadré 6).

Encadré 6. Le règlement général sur la protection des données (RGPD) de l'Union européenne

Le RGPD est entré en vigueur en mai 2018 et vise à donner aux citoyens de l'Union européenne un contrôle accru sur leurs données de caractère personnel et sur la manière dont ces données sont consultées, traitées et utilisées. Le RGPD établit sept principes fondamentaux concernant les données de caractère personnel : licéité, loyauté et transparence, limitation des finalités, minimisation des données, exactitude, limitation de la conservation, intégrité et confidentialité (sécurité) et responsabilité.

Le RGPD confère également des droits spécifiques (et nouveaux) aux « personnes concernées », à savoir toutes les personnes physiques dont les données de caractère personnel sont traitées par un responsable du traitement ou un sous-traitant. Le règlement énonce les droits fondamentaux suivants de la personne concernée :

- droit d'accès
- droit de rectification
- droit à l'effacement ou droit à l'oubli
- droit à la limitation du traitement
- droit à la portabilité des données
- droit d'opposition
- droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, lorsque cette décision produit des effets juridiques ou affecte la personne concernée de manière significative.

2. Sensibilisation et éducation aux questions financières

Jusqu'à présent, les politiques publiques relatives aux données de caractère personnel des consommateurs de services financiers se sont principalement intéressées à la réglementation en matière de protection des données et de protection financière des consommateurs. Les stratégies nationales en matière d'éducation financière, à quelques exceptions notables près (voir encadré 7), doivent encore inclure systématiquement cet élément dans le contenu de leurs programmes.

Le développement de nouvelles compétences de base concernant les données de caractère personnel est d'autant plus pertinent que les modifications apportées récemment à la réglementation relative à la protection de la vie privée dans certaines juridictions visent à donner aux consommateurs les moyens d'agir et à leur conférer des droits spécifiques sur leurs données (voir encadré 6). Les consommateurs devraient posséder les connaissances et les compétences nécessaires pour comprendre l'utilisation qui est faite de leurs données de caractère personnel et exercer pleinement leurs droits de consommateurs dans ce domaine.

Encadré 7. Initiatives en matière de culture financière numérique parmi les membres de l'OCDE-INFE

Les membres de l'OCDE-INFE ont commencé à inclure dans leurs stratégies et initiatives nationales l'éducation et la sensibilisation aux questions financières en ce qui concerne l'importance des données de caractère personnel.

Allemagne

En Allemagne, le ministère fédéral de la justice et de la protection des consommateurs (BMJV), en tant qu'autorité compétente pour la politique des consommateurs en ce qui concerne, notamment, la société de l'information et les services financiers, a publié un article complet sur les droits des consommateurs à l'égard de leurs données. L'article comprend une section sur la protection de la personnalité par la protection des données, une section sur la manière dont un consommateur individuel peut obtenir des informations sur les données déjà collectées le concernant, ainsi que des orientations sur la manière d'éviter de fournir des données inutiles et d'utiliser l'internet en toute sécurité. Une brochure contenant des informations adaptées aux consommateurs âgés peut être téléchargée gratuitement[1].

L'autorité fédérale allemande de surveillance financière (BaFin) fournit aux consommateurs des orientations pratiques sur l'utilisation de leurs données de caractère personnel lorsqu'ils utilisent des services financiers. En 2019, la BaFin a organisé, à l'intention des personnes âgées, un séminaire en ligne consacré à la deuxième directive sur les services de paiement (DSP2)[2], expliquant l'incidence de la directive sur le paiement électronique et la banque en ligne, ainsi qu'aux autres solutions de paiement. Une attention particulière a été accordée aux questions de protection des données.

Portugal

La culture financière numérique figure parmi les principaux objectifs du plan stratégique 2017-2020 de la Banque centrale du Portugal. Cet objectif stratégique porte en particulier

sur l'utilisation sûre des canaux numériques. L'adoption de procédures de sécurité par les clients est encouragée par des campagnes de sensibilisation sur le site internet de la Banque réservé aux clients (https://clientebancario.bportugal.pt). Le site internet comporte également une page spécifique offrant des informations sur la sécurité numérique, comme les risques associés aux canaux numériques, et des explications sur ce que sont les données massives, ainsi que les avantages et les risques qu'elles comportent. Ces informations sont accessibles aux consommateurs dans un langage simple et au moyen d'une interface intuitive, étayée par des outils audiovisuels.

En 2018, la Banque centrale du Portugal a lancé une campagne d'éducation financière numérique destinée aux jeunes (#toptip), afin de sensibiliser les natifs du numérique aux précautions à prendre lors de l'utilisation des services financiers numériques. Le premier conseil, « Lorsque tu utilises l'internet, as-tu une idée des risques ? », donne des indications sur la manière dont les utilisateurs devraient protéger leur équipement et leur connexion internet contre les risques tels que l'hameçonnage, le dévoiement, les logiciels espions et l'hameçonnage par carte SIM. Le deuxième conseil, « Utilises-tu ton smartphone pour accéder aux réseaux sociaux ou au courrier électronique ? Ou pour la banque à domicile ? Fais-tu également des paiements avec ton téléphone portable ? », met l'accent sur l'importance de protéger la grande quantité d'informations confidentielles et privées que les utilisateurs stockent sur leur téléphone portable. Le troisième conseil, « Les réseaux sociaux sont-ils ta deuxième maison ? », met en garde contre les risques du partage des données de caractère personnel sur les réseaux sociaux. Le quatrième conseil, « Fais-tu tes achats en ligne en toute sécurité ? », précise les étapes que les utilisateurs devraient suivre avant, pendant et après un achat en ligne. Le cinquième conseil, « Que faire si tu es victime de fraude en ligne ? », aide les utilisateurs qui ont été (ou pensent avoir été) victimes de fraude en ligne. La campagne a également été diffusée sur le compte Instagram de la Banque centrale (@ bancodeportugalofficial). La Banque centrale a envoyé une brochure contenant ces conseils à toutes les écoles secondaires et organise régulièrement dans les écoles secondaires des séances d'éducation financière qui sont très demandées.

Espagne

La culture financière numérique figure parmi les principaux objectifs du plan national pour l'éducation financière mis en œuvre par la Banque centrale d'Espagne et la CNMV pour la période 2018-2021. La numérisation des produits et services financiers et la nécessité qui en découle de renforcer la culture financière numérique sont considérées comme des domaines d'action essentiels. Le plan pour l'éducation financière reconnaît en particulier les possibilités et les défis que présente la fourniture numérique de l'éducation financière, et des efforts seront déployés pour recenser et encourager les initiatives en matière d'éducation financière dans ce domaine. Des outils numériques, applications et logiciels seront utilisés pour améliorer l'accès à l'éducation financière, renforcer les compétences clés des utilisateurs de services financiers et accroître leurs aptitudes concernant la gestion et le contrôle de leurs finances.

En ce qui concerne les données de caractère personnel, le site internet de la stratégie nationale espagnole, *Finanzas para Todos* (www.finanzasparatodos.es), comprend une section complète consacrée à la protection des informations de caractère personnel, avec des réponses à des questions telles que : « Quelles informations personnelles dois-je protéger ? », « Que dois-je faire si je reçois un courriel me demandant de confirmer mes données personnelles ? », « Que sont les logiciels espions ? » et « Quelles précautions dois-je prendre avec la banque en ligne ? ». De même, une section sur la protection des informations de caractère personnel est incluse dans le programme d'éducation financière

pour les écoles, destiné aux élèves de 14 à 18 ans, et traite des questions susmentionnées. Ce programme comprend également des activités pratiques en classe, dont les objectifs d'apprentissage sont les suivants :

1. comprendre l'importance de protéger les informations de caractère personnel pour éviter d'être victime de fraude financière
2. recenser les précautions à prendre dans le cadre de la banque en ligne et des autres activités sur l'internet
3. savoir combien il est important de signaler le vol ou la perte de documents et de garder une trace écrite de ce signalement et
4. connaître les précautions à prendre pour la banque en ligne et les autres activités sur l'internet.

1. www.bmjv.de/DE/Verbraucherportal/DigitalesTelekommunikation/Datenschutz/Datenschutz_node.html

2. www.bafin.de/SharedDocs/Downloads/DE/Veranstaltung/dl_191017_digitaler_stammtisch_digitalisierung.html

Liste de mesures à prendre figurant dans les orientations du G20/OCDE-INFE : gros plan sur les données de caractère personnel

Compte tenu de la nécessité d'aborder l'utilisation des données de caractère personnel dans les programmes d'éducation financière et d'encourager les comportements positifs en matière de sensibilisation aux questions liées à ces données et de gestion de ces dernières, le présent rapport propose des éléments spécifiques relatifs aux données de caractère personnel à l'appui de la mise en œuvre de la note d'orientation du G20/ OCDE-INFE sur la culture financière numérique.

Ces nouveaux éléments devraient être considérés comme un outil de mise en œuvre supplémentaire pour les décideurs politiques et les concepteurs de programmes traitant de l'éducation financière et des données de caractère personnel, et devraient être lus dans le contexte du cadre réglementaire applicable et des niveaux de culture financière et numérique dans chaque juridiction.

Tableau 1. Nouveaux éléments relatifs aux données de caractère personnel dans certains volets sélectionnés de la note d'orientation du G20/OCDE-INFE

Volets sélectionnés de la note d'orientation du G20/OCDE-INFE	Éléments spécifiques relatifs aux données de caractère personnel
1. Préparer un diagnostic national	*Du côté de l'offre* Passer en revue le paysage actuel pour comprendre : • la manière dont les prestataires de services financiers utilisent les données de caractère personnel des clients, dans le cadre de la législation nationale applicable • l'existence de droits spécifiques pouvant donner lieu à une action en ce qui concerne les données de caractère personnel dans le cadre des services financiers, conformément à la législation relative à la protection financière des consommateurs et à la protection des données. *Du côté de la demande* Exploiter les données et analyses existantes ou faire réaliser des recherches pour comprendre : • les attitudes envers la protection de la vie privée et l'utilisation des données de caractère personnel • la compréhension de l'empreinte numérique par les consommateurs • le degré de connaissances et les comportements en matière de sécurité en ligne • le souhait de partager des données • la connaissance des droits pouvant donner lieu à une action en ce qui concerne les données de caractère personnel dans le cadre des services financiers, conformément à la législation relative à la protection financière des consommateurs et à la protection des données.
2. Assurer la coordination	Entre autorités publiques : • assurer la coordination avec l'autorité nationale chargée de la protection des données, si elle existe, ou avec les autorités publiques ayant un mandat légal et des moyens effectifs dans le domaine de la réglementation en matière de protection de la vie privée et des données[10], ou à tout moins, consulter ces autorités. Avec le secteur privé et à but non lucratif : • les autorités publiques devraient s'efforcer de tirer parti des connaissances du secteur privé, et en particulier des acteurs des technologies financières, afin de comprendre les nouvelles évolutions dans le domaine du partage des données de caractère personnel.

[10] Pour une liste mondiale des autorités nationales chargées de la protection des données, voir : https://www.dlapiperdataprotection.com/index.html?t=authority&c=AR&c2=

Volets sélectionnés de la note d'orientation du G20/OCDE-INFE	Éléments spécifiques relatifs aux données de caractère personnel
3. Soutenir l'élaboration d'un cadre de compétences de base national en matière de culture financière numérique	
3.a Donner aux consommateurs, y compris aux plus vulnérables d'entre eux, les moyens de contrer les nouveaux types d'exclusion liés à l'utilisation abusive de diverses sources de données, dont les données massives, et du profilage numérique	
• Gérer leur empreinte numérique de manière appropriée dans la mesure du possible.	• Les consommateurs devraient être conscients des possibilités d'analyse offertes par les données massives et du fait que toute activité en ligne peut être utilisée par les prestataires de services financiers pour personnaliser les offres et définir le coût et la gamme des produits offerts. • En particulier dans les pays où des systèmes d'évaluation positive du risque de crédit existent, les consommateurs doivent comprendre que les décisions en matière d'évaluation du risque de crédit peuvent être influencées par des informations personnelles qui ne sont pas liées à leurs antécédents en matière de crédit.
• Éviter de se livrer à des comportements à risque impliquant leurs données de caractère personnel et comprendre les conséquences du partage ou de la divulgation de numéros d'identification personnels, d'informations relatives aux comptes ou d'autres données d'identification telles que l'adresse, la date de naissance ou les numéros émis par les pouvoirs publics, que ce soit par voie numérique ou par d'autres canaux.	• Les groupes cibles les moins familiarisés avec les transactions en ligne et possédant les niveaux de culture numérique les plus faibles devraient être régulièrement incités à prendre des mesures efficaces pour protéger leurs données de caractère personnel et leur vie privée.
• Évaluer le type d'informations demandées par les prestataires de services (financiers) afin de décider si elles sont pertinentes et comprendre comment elles peuvent être stockées et utilisées.	• Les groupes cibles qui sont disposés à partager plus d'informations de caractère personnel avec les prestataires de services financiers en échange d'avantages, notamment les jeunes générations et ceux qui maîtrisent le mieux la technologie, devraient être conscients des conséquences pour leur vie privée et devraient partager des informations supplémentaires non essentielles sur la base d'un consentement éclairé.

Volets sélectionnés de la note d'orientation du G20/OCDE-INFE	Éléments spécifiques relatifs aux données de caractère personnel
• Accroître la connaissance que les consommateurs ont de leurs droits relatifs aux données de caractère personnel et du cadre réglementaire applicable, en particulier lorsque celui-ci confère aux consommateurs de nouveaux droits et un contrôle discrétionnaire sur leurs données de caractère personnel.	• Dans les juridictions où des modifications de la réglementation en matière de données de caractère personnel ont conféré de nouveaux droits aux consommateurs, ceux-ci devraient être informés au moyen de campagnes de sensibilisation. • Informer les consommateurs des mécanismes qui sous-tendent les décisions concernant leur vie financière, en particulier lorsque ces décisions sont prises sans intervention humaine. • Lorsque les consommateurs ont légalement le droit de contester une décision prise par un algorithme, il convient de les informer des voies de recours et des modalités y afférentes.
3.b Protéger les consommateurs et les petites entreprises d'une exposition accrue à la criminalité numérique, telle que l'hameçonnage, le piratage de compte et le vol de données.	
• Sensibiliser davantage les consommateurs à l'existence de la fraude en ligne et des risques en matière de cybersécurité lors du choix et de l'utilisation de services financiers numériques, de la réalisation de transactions financières en ligne et de l'utilisation d'outils d'agrégation de comptes (« capture de données d'écran »).	• Les consommateurs, et en particulier les groupes cibles les plus vulnérables, devraient être avertis de la nécessité d'utiliser des mots de passe forts pour protéger leurs données de caractère personnel et leurs transactions financières en ligne et être informés de ce qu'il convient de faire en cas de violation de la sécurité.
• Sensibiliser davantage les consommateurs aux possibilités offertes par les outils d'agrégation de comptes, ainsi qu'à la manière d'utiliser ces outils et d'arrêter de les utiliser en toute sécurité, étant donné qu'ils donnent accès à des informations sur leurs comptes à des tiers.	• Les consommateurs comprennent quelles sont les conditions de révocation du partage de données et quand révoquer les autorisations d'accès, d'utilisation ou de stockage des données. • Les consommateurs comprennent que, grâce à la capture de données d'écran, les mots de passe et les informations de connexion restent entre les mains du prestataire tiers même lorsqu'ils cessent d'utiliser le service, ce qui augmente la probabilité que le mot de passe soit volé ou utilisé de manière malveillante.

3. Conclusions

Dans les économies d'aujourd'hui, la capacité des prestataires de services financiers à recueillir, stocker, combiner et analyser un large éventail de données concernant leurs clients, comme leur situation financière, leurs habitudes ou leur localisation physique, a entraîné une adaptation des cadres de protection des données et de protection financière des consommateurs. Si cette adaptation est certes nécessaire, les politiques publiques devraient également viser à sensibiliser davantage les consommateurs aux conséquences de l'utilisation de leurs données de caractère personnel et à encourager les comportements susceptibles de protéger ces données tout en les aidant à adopter une attitude proactive en matière de partage de données, qui soit conforme à leurs propres préférences. Une telle approche centrée sur le consommateur répond également à l'évolution du contexte réglementaire, qui donne aux individus de nouveaux droits en rapport avec leurs données de caractère personnel.

L'analyse effectuée dans le présent rapport expose les conséquences de l'utilisation de données de caractère personnel dans les services financiers du point de vue des consommateurs. Elle couvre à la fois les avantages et les risques, en exploitant les données existantes pour décrire les attitudes des consommateurs à l'égard du partage de données de caractère personnel.

Sur la base de cette analyse, les responsables des politiques en matière d'éducation financière sont encouragés à tenir compte des questions liées aux données de caractère personnel lorsqu'elles rassemblent des éléments probants pour étayer leurs politiques et leurs programmes. Il s'agit idéalement de couvrir à la fois l'offre, c'est-à-dire l'utilisation des données de caractère personnel par les prestataires et le cadre réglementaire applicable, et la demande, c'est-à-dire l'attitude des consommateurs à l'égard du partage de données et leur compréhension de la valeur et des implications de leurs données de caractère personnel.

Les autorités chargées de l'éducation financière dans chaque juridiction sont invitées à se coordonner avec les autorités chargées de la protection des données de caractère personnel et de la protection financière des consommateurs, ou à consulter ces dernières, afin de veiller à ce que les politiques et initiatives en matière d'éducation financière bénéficient de leur expertise et soient cohérentes avec les cadres nationaux existants régissant la protection des données de caractère personnel. De même, elles devraient assurer une coordination avec les entreprises de technologie financière, ou une consultation de ces dernières, afin de comprendre pleinement les nouvelles évolutions en matière de partage de données de caractère personnel.

Enfin, le rapport met en évidence des compétences spécifiques en matière de culture financière qui bénéficieraient aux particuliers et aux entrepreneurs dans ce domaine, en proposant de nouveaux éléments relatifs aux données de caractère personnel à l'appui de la mise en œuvre de la note d'orientation du G20/OCDE-INFE sur la culture financière numérique. Ces nouveaux éléments, qui sont soumis à l'examen des décideurs publics,

devraient être lus dans le contexte du cadre régissant la protection financière des consommateurs et la protection des données de caractère personnel dans chaque juridiction.

L'OCDE, par l'intermédiaire de son Réseau international sur l'éducation financière (OCDE/INFE), et dans le cadre son projet horizontal sur la numérisation, continuera de suivre les politiques mises en œuvre au niveau national, et de mener un dialogue fructueux au niveau international pour recenser les bonnes pratiques. Grâce à son caractère mondial, l'OCDE/INFE favorisera également les approches transfrontières nécessaires concernant les politiques en matière de données de caractère personnel.

Références

Accenture (2017), *Accenture Financial Services 2017 Global Distribution & Marketing Consumer study: financial services report*, www.accenture.com/t20170111T041601__w__/us-en/_acnmedia/Accenture/next-gen-3/DandM-Global-Research-Study/Accenture-Financial-Services-Global-Distribution-Marketing-Consumer-Study.pdf.

Accenture (2019), *Accenture Global Financial Services Consumer Study*, https://www.accenture.com/_acnmedia/PDF-95/Accenture-2019-Global-Financial-Services-Consumer-Study.pdf.

Berg T. et al. (2018), « On the Rise of FinTechs – Credit Scoring using Digital Footprints », *Working Paper Series*, https://www.fdic.gov/bank/analytical/cfr/2018/wp2018/cfr-wp2018-04.pdf.

CE (2015), *Special Eurobarometer 423 Cyber Security - Report*, http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf.

Comité mixte des Autorités européennes de surveillance (2016), *Discussion Paper on the Use of Big Data by Financial Institutions*, https://esas-joint-committee.europa.eu/Publications/Discussion%20Paper/jc-2016-86_discussion_paper_big_data.pdf.

Cormen T. et al. (2009), *Introduction to Algorithms* : *Third Edition*, MIT Press.

Forbes (2017), « Equifax and SAS leverage AI and deep learning to improve consumer access to credit », *Forbes*, 20 février, https://www.forbes.com/sites/gilpress/2017/02/20/equifaxand-sas-leverage-ai-and-deep-learning-to-improve-consumer-access-tocredit/2/#2ea15ddd7f69.

Groupe des utilisateurs des services financiers de l'UE (2016), *Assessment of current and future impact of Big Data on Financial Services*, https://ec.europa.eu/info/sites/info/files/file_import/1606-big-data-on-financial-services_en_0.pdf.

Financial Services Consumer Panel (2018), *Consenting adults? - consumers sharing their financial data*, https://www.fs-cp.org.uk/sites/default/files/final_position_paper_-_consenting_adults_-_20180419_0.pdf.

G20 (2011), *Principes de haut niveau G20/OCDE sur la protection financière des consommateurs*, http://www.oecd.org/daf/fin/financial-markets/48892010.pdf.

GfK (2017), *Willingness to share personal data in exchange for benefits or rewards - Global GfK survey*, https://www.gfk.com/fileadmin/user_upload/country_one_pager/NL/images/Global-GfK_onderzoek_-_delen_van_persoonlijke_data.pdf.

GSMA (2018), *The Mobile Economy 2018*, https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf.

Hurley, M. et J. Adebayo (2017), « Credit Scoring in the Era of Big Data », *Yale Journal of Law and Technology*, vol. 18, n° 1, https://digitalcommons.law.yale.edu/yjolt/vol18/iss1/5.

Ipsos MORI (2019), *UK Cyber Survey Key findings – General public*, enquête réalisée pour le compte du National Cyber Security Centre and Department for Digital, Culture, Media and Sport (DCMS), https://www.ipsos.com/ipsos-mori/en-uk/uk-cyber-security-survey-2019.

OCDE (2019a), *Recommandation du Conseil sur l'intelligence artificielle*, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0449.

OCDE (2019b), *L'intelligence artificielle dans la société*, Éditions OCDE, Paris, https://doi.org/10.1787/eedfee77-en.

OCDE (2019c), « Good practice guide on consumer data », *Documents de travail de l'OCDE sur l'économie numérique*, n° 290, Éditions OCDE, Paris, https://doi.org/10.1787/b7f8cd16-fr.

OCDE (2018a), *Note d'orientation du G20/OCDE-INFE sur la numérisation et la culture financière*, http://www.oecd.org/finance/G20-OECD-INFE-Policy-Guidance-Digitalisation-Financial-Literacy-2018.pdf.

OCDE (2018b), *G20/OECD Policy Guidance on Financial Consumer Protection Approaches in the Digital Age*, https://www.oecd.org/finance/G20-OECD-Policy-Guidance-Financial-Consumer-Protection-Digital-Age-2018.pdf.

OCDE (2018c), « IoT measurement and applications », *Documents de travail de l'OCDE sur l'économie numérique*, n° 271, Éditions OCDE, Paris, https://doi.org/10.1787/35209dbf-en.

OCDE (2018d), « Consumer policy and the smart home », *Documents de travail de l'OCDE sur l'économie numérique*, n° 268, Éditions OCDE, Paris, https://doi.org/10.1787/e124c34a-en.

OCDE (2018e), *G20 Toolkit for Protecting Digital Consumers*, https://www.oecd.org/internet/consumer/toolkit-for-protecting-digital-consumers.pdf.

OCDE (2017a), *Perspectives de l'économie numérique de l'OCDE 2017*, Éditions OCDE, Paris, https://doi.org/10.1787/9789264282483-fr.

OCDE (2017b), *Technology and innovation in the insurance sector*, https://www.oecd.org/finance/Technology-and-innovation-in-the-insurance-sector.pdf.

OCDE (2017c), *Robo-Advice for Pensions*, https://www.oecd.org/finance/Robo-Advice-for-Pensions-2017.pdf.

OCDE (2016a), *G20/OECD INFE Core competencies framework on financial literacy for adults*, http://www.oecd.org/daf/fin/financial-education/Core-Competencies-Framework-Adults.pdf.

OCDE (2016b), *Recommandation du Conseil sur la protection du consommateur dans le commerce électronique*, Éditions OCDE, Paris, https://doi.org/10.1787/9789264255272-fr.

OCDE (2015a), *OCDE/INFE Core competencies framework on financial literacy for youth*, http://www.oecd.org/daf/fin/financial-education/Core-Competencies-Framework-Youth.pdf.

OCDE (2015b), *Data-Driven Innovation: Big Data for Growth and Well-Being*, Éditions OCDE, Paris, http://dx.doi.org/10.1787/9789264229358-en.

OCDE (2015c), *La gestion du risque de sécurité numérique pour la prospérité économique et sociale : Recommandation de l'OCDE et document d'accompagnement*, Éditions OCDE, Paris, https://doi.org/10.1787/9789264246089-fr.

OCDE (2014), « Consumer Policy Guidance on Mobile and Online Payments », *Documents de travail de l'OCDE sur l'économie numérique*, n° 236, Éditions OCDE, Paris, https://doi.org/10.1787/5jz432cl1ns7-en.

OCDE (2013), *The OECD Privacy Framework*, www.oecd.org/internet/ieconomy/oecd_privacy_framework.pdf.

Pingitore G. et al. (2017), « To share or not to share : What consumers really think about sharing their personal information », *Deloitte University Press*,

https://www2.deloitte.com/content/dam/insights/us/articles/4020_To-share-or-not-to-share/DUP_To-share-or-not-to-share.pdf.

Reserve Bank of India (2016), *Master Direction- Non-Banking Financial Company - Account Aggregator*, https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598.

Rosner G. et E. Kenneally (2018), *Clearly Opaque: Privacy Risks of the Internet of Things*, https://www.iotprivacyforum.org/wp-content/uploads/2018/06/Clearly-Opaque-Privacy-Risks-of-the-Internet-of-Things.pdf?d8bd54&d8bd54.

UE (2016), *Règlement (UE) 2016/679 du Parlement européen et du Conseil (Règlement général sur la protection des données)*, https://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504.

UE (2015), *Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur*, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32015L2366.

Annexe A. Liste des membres du groupe de travail de l'OCDE-INFE sur la culture financière numérique

Autriche	Martin Taborsky, Banque centrale d'Autriche (codirigeant)
Pays-Bas	Olaf Simonse, Ministère des finances (codirigeant)
Australie	Laura Higgins, Australian Securities and Investments Commission
Autriche	Elisabeth Ulbrich, Banque centrale d'Autriche
Brésil	João Evangelista de Sousa Filho, Banco do Brasil
Brésil	José Alexandre Cavalcanti Vasco, CVM
Brunei Darussalam	Rina Hayane Sumardi, Autoriti Monetari Brunei Darussalam
Canada	Chris Poole, Agence de la consommation en matière financière du Canada
Chili	Carolina del Río, Commission des marchés financiers (anciennement SBIF)
République tchèque	Alex Ivanco, ministère des finances
France	Astrid Delacour, Banque de France
Inde	Gautam Prasad Borah, Reserve Bank of India
Inde	Girraj Prasad Garg, NISM
Indonésie	Rela Ginting, OJK
Italie	Roberta Nanula, Banca d'Italia
Italie	Nadia Linciano, CONSOB
Corée	Jin Yong Kim, Banque de Corée
Lettonie	Dace Jansone, Commission des marchés financiers et des capitaux
Luxembourg	Danièle Berna-Ost, Commission de Surveillance du Secteur Financier
Malaisie	Jeremy Lee Eng Huat, Bank Negara Malaysia
Mexique	Pedro Garza López, Banco de México
Mongolie	Myendu Nurgul, Banque centrale de Mongolie
Maroc	Imane Benzarouel, Fondation Marocaine pour l'Éducation Financière
Nouvelle-Zélande	Celestyna Galicki, Commission for Financial Capability
Pakistan	Syed Samir Hasnain, Banque nationale du Pakistan
Pérou	Juan-Carlos Chong, Direction de la banque, de l'assurance et des fonds de pension privés
Portugal	Lucía Leitão, Banque centrale
Portugal	Lucélia Fernandes, Autorité portugaise de surveillance des assurances et des fonds de pension
République de Macédoine du Nord	Kristina Pavleska, Organe de coordination des Autorités de réglementation pour l'éducation financière en Macédoine du Nord
Roumanie	Anton Comanescu, Banque nationale de Roumanie
Singapour	Abigail Ng, Autorité monétaire de Singapour
Afrique du Sud	Lyndwill Clarke, Financial Sector Conduct Authority
Espagne	Emilio Ruiz, Banco d'España
Suède	Thèrese Wieselqvist Ekman, Financinspektionen
Turquie	Nihal Değirmenci, Banque centrale de la République de Turquie

www.oecd.org/finance