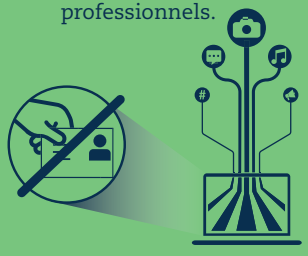
Chapitre 7

RENFORCER LA CONFIANCE

Près de **30 %** **des internautes se méfient** des réseaux sociaux et professionnels.



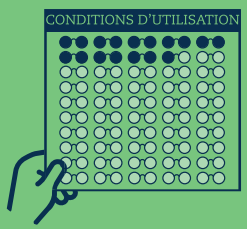
Répondre aux inquiétudes quant à la sécurité numérique et à la protection de la vie privée et des consommateurs afin de renforcer la confiance.

Un Internaute sur quatre au sein de l'Union européenne est **préoccupé par la sécurité des paiements**.

Donner à tous les acteurs les moyens d'évaluer et de mieux gérer le risque de sécurité numérique.

CONFIANCE

Seuls **17 %** des utilisateurs **lisent l'intégralité des conditions générales** des plateformes mettant en relation les particuliers.



Concevoir et mettre en œuvre des mesures plus efficaces pour protéger les cyberconsommateurs.

La majorité des **mesures de protection de la vie privée** visent à renforcer la sensibilisation et **l'autonomie des individus**.

Définir et mettre en œuvre une stratégie nationale de protection de la vie privée suivant une approche englobant l'ensemble de la société.

RENFORCER LA CONFIANCE : PRINCIPAUX ENJEUX DE L'ACTION PUBLIQUE

Renforcer la confiance en adoptant une approche fondée sur la gestion du risque

- Ériger la gestion du risque en principe pour l'élaboration de politiques destinées à renforcer la confiance, notamment en vue d'évaluer et de prendre en charge les risques liés aux technologies, aux données et aux flux transfrontières.
- Aider les petites et moyennes entreprises (PME) à saisir les opportunités qu'offre le numérique en renforçant la sensibilisation et en promouvant de bonnes pratiques de gestion du risque par des efforts publics et privés.

Développer des cadres de protection de la vie privée qui soient solides, inclusifs et interopérables

- Les cadres de protection de la vie privée favorisent la libre circulation des données à caractère personnel, stimulant la croissance et la prospérité sociale. Des mesures doivent être prises pour renforcer la transparence sur la finalité et l'utilisation des données à caractère personnel collectées et élargir les possibilités offertes aux utilisateurs d'accéder aux données les concernant et de les contrôler. Les solutions technologiques peuvent aider à renforcer la confiance via l'intégration par défaut de processus de protection de la vie privée dès la phase de conception des produits ou services.
- Les politiques nationales de protection de la vie privée devraient être soutenues aux plus hauts niveaux d'administration et suivre une approche englobant l'ensemble de la société. Plus de la moitié des mesures de protection mises en place dans les pays de l'OCDE ont pour objectif d'accroître la sensibilisation et l'autonomie des individus.
- Encourager l'interopérabilité des cadres de protection de la vie privée entre les pays et territoires, notamment par le biais de stratégies nationales et d'autres approches pratiques.

Gérer le risque de sécurité numérique plutôt que de chercher à l'éliminer

- Les menaces qui pèsent sur la sécurité numérique, y compris les actes malveillants, sont en augmentation, à tel point que près de 30 % des internautes s'abstiennent de communiquer des informations personnelles sur les réseaux sociaux et professionnels. Qui plus est, au sein de l'Union européenne, un internaute sur quatre est préoccupé par la sécurité des paiements en ligne.
- La sécurité numérique ne doit pas être appréhendée comme une simple question d'ordre technique, mais doit devenir une priorité stratégique pour les individus, les entreprises et les pouvoirs publics. La gestion du risque de sécurité numérique relève de la responsabilité de l'ensemble des acteurs du cyberespace.

Protéger les consommateurs à l'heure où les mondes physique et virtuel convergent

- Les cyberconsommateurs sont confrontés à des problématiques liées à la divulgation des informations, à des pratiques commerciales trompeuses et déloyales, aux processus de confirmation et de paiement, aux cas de fraude et d'usurpation d'identité, à la sécurité des produits, ou encore aux mécanismes de règlement et de réparation des litiges, y compris lorsqu'ils utilisent des appareils connectés qui contribuent à brouiller les frontières entre les mondes physique et virtuel.
- Les conditions d'utilisation ne constituent pas un moyen efficace pour communiquer des informations importantes aux consommateurs. De fait, seuls 17 % des individus lisent l'intégralité des conditions d'utilisation des plateformes de mise en relation (telles Airbnb et BlaBlaCar). D'où la nécessité de privilégier d'autres approches pour protéger les consommateurs sur l'internet.

Pour entrer de plain-pied dans la transformation numérique et en tirer le meilleur parti, les individus, les entreprises et les pouvoirs publics doivent avoir l'assurance que les activités économiques et sociales qu'ils mènent à bien dans le cyberenvironnement leur procureront plus d'avantages que d'inconvénients. Ces derniers peuvent être le résultat de diverses sources d'incertitudes entourant les technologies numériques, les données et les flux transfrontières, et sont souvent liés à de possibles incidents de sécurité numérique (atteintes à la disponibilité, à l'intégrité ou à la confidentialité des données, systèmes ou réseaux, par exemple). D'autres inconvénients ont trait aux asymétries d'information, aux rapports de force déséquilibrés ou aux problèmes de compétence juridictionnelle exacerbés par le cyberenvironnement. Peuvent s'ensuivre des violations des lois et réglementations relatives au respect de la vie privée, à la protection des consommateurs ou à la sécurité des produits, destinées à réduire ces déséquilibres et surmonter ces défis. Pour garantir la confiance, il est impératif de limiter autant que faire se peut ces incertitudes.

Renforcer la confiance en adoptant une approche fondée sur la gestion du risque

Les événements indésirables – qu'il s'agisse du vol d'actifs d'entreprises, de l'usurpation de l'identité d'individus, ou de l'utilisation abusive de données à caractère personnel – peuvent nuire à la réputation, aux finances, à la liberté, à l'autonomie, à la santé, au bien-être, à la sécurité, à la compétitivité ou à l'efficience de l'ensemble des acteurs, et finir par les dissuader de s'engager pleinement dans l'environnement numérique. Ils ont également des incidences sur le fonctionnement même de la société, puisque des incidents de sécurité numérique sont à même de perturber les infrastructures critiques et les services essentiels comme la fourniture d'énergie, les services financiers et les transports.

Dans la pratique, la solution la plus efficace face à ces incertitudes est de gérer les risques numériques. Compte tenu de l'impossibilité de les éliminer entièrement, un certain niveau de risque doit être accepté. En d'autres termes, les risques numériques doivent être réduits à un niveau acceptable au regard des objectifs et des avantages visés. Cela implique d'apprendre à les évaluer et les gérer et, en définitive, de décider de les accepter, les réduire, les transférer ou les éviter (soit, dans ce dernier cas, s'abstenir de mener des activités dans l'environnement numérique).

Encadré 7.1. Qu'est-ce que la confiance ?

La confiance touche de nombreux aspects de la vie des individus – confiance dans les institutions politiques, les pouvoirs publics, les statistiques, l'état de droit (confiance institutionnelle) ou dans autrui (confiance interpersonnelle) (voir chapitre 6). S'il n'existe pas de définition universellement admise de la confiance, l'OCDE l'entend comme « la croyance d'une personne qu'une autre personne ou institution agira conformément à ses attentes en termes de comportement positif », et a contribué à en améliorer la mesure en énonçant des lignes directrices à l'intention des offices statistiques nationaux (OCDE, 2017[1]) et en menant à bien des travaux expérimentaux (Murtin et al., 2018[2]).

La transformation numérique ajoute une nouvelle dimension à la notion de confiance pour les individus, les sociétés et l'économie. Le présent chapitre aborde la confiance par le prisme des incertitudes et des interdépendances (Mayer, Davis et Schoorman, 1995[3]), ces facteurs faisant partie intégrante des environnements numériques. La confiance dans ces environnements dépend du contexte et varie selon les enjeux, y compris les opportunités et les défis qui se présentent.

Pour les individus, la confiance dans le monde numérique revient à accepter de mobiliser des ressources (temps, moyens financiers et données à caractère personnel) pour mener des activités commerciales et sociales, et de devenir vulnérables si un achat ne se passe pas comme prévu ou si leurs données sont dérobées, utilisées pour surveiller leur comportement, les discriminer ou porter atteinte à leur vie privée. Pour les organisations, la confiance équivaut à accepter un certain niveau de risque inhérent à d'éventuels incidents compromettant la sécurité numérique, le respect de la vie privée, la protection des consommateurs, etc., afin de tirer parti de la transformation numérique. La confiance représente par conséquent une condition essentielle pour exploiter le plein potentiel de croissance et de progrès social à l'ère du numérique.

La gestion du risque numérique vaut pour les individus comme les organisations, des petites entreprises aux grandes structures, en passant par les entités publiques. Tous les acteurs partagent une certaine part de responsabilité dans la gestion des risques numériques inhérents à leurs activités, selon leurs rôles respectifs, leur capacité à agir et le contexte, et doivent pour ce faire disposer de compétences adaptées. Compte tenu du caractère transfrontière, intersectoriel et multipartite du risque numérique, sa gestion fournit aux différents secteurs de l'action des pouvoirs publics un cadre de référence commun pour aborder les politiques ayant trait à la confiance selon une approche intégrée et globale, faisant fond sur les composantes fondamentales d'un cycle de gestion du risque. Ces composantes sont les suivantes :

- définir les objectifs et le contexte d'une activité et déterminer un niveau de risque acceptable au regard des avantages attendus
- mesurer le risque en identifiant les facteurs connexes et évaluer la probabilité et la gravité de la réalisation du risque
- traiter le risque, notamment en acceptant une part de risque, en le réduisant à un niveau acceptable grâce à la mise en place de mesures adaptées, en en partageant ou transférant une partie, et/ou en en évitant une partie
- surveiller et réexaminer en permanence le cycle de gestion du risque afin de l'adapter à un environnement en constante évolution.

Il est essentiel de miser sur des politiques encourageant la gestion du risque numérique pour renforcer la confiance et permettre aux individus et aux organisations de donner corps à leurs objectifs économiques et sociaux. Si les pratiques de gestion du risque sont susceptibles de différer selon l'objectif visé (sécurité numérique, protection de la vie privée, protection des consommateurs ou sécurité des produits), les politiques doivent tenir compte des corrélations entre les diverses catégories de risque. Toute mesure de gestion du risque numérique doit être adaptée et proportionnée au risque et aux objectifs en jeu pour les acteurs concernés. En effet, des mesures appropriées pour un individu peuvent ne pas l'être pour une grande entreprise privée, bien que les deux acteurs poursuivent le même objectif.

Parmi les entreprises du secteur privé, les startups et les PME méritent une attention particulière de la part des décideurs, du fait non seulement de leur rôle essentiel dans l'économie, mais aussi de leur capacité limitée à faire face à des incidents majeurs et à gérer efficacement le risque numérique. Les PME, et plus particulièrement les startups en phase de démarrage, jouent un rôle essentiel dans la croissance économique et contribuent à la concurrence, à l'innovation et à la création d'emplois. En revanche, la gestion du risque numérique leur pose des difficultés spécifiques. Par exemple, un incident de sécurité numérique qui entraînerait une perte de confiance des consommateurs, une atteinte à la réputation ou une baisse du chiffre d'affaires pourrait s'avérer plus dommageable pour des PME que pour de grandes entreprises. De fait, elles pourraient avoir plus de mal à surmonter une perte temporaire de revenus.

En outre, les PME ne disposent souvent pas des connaissances, des ressources ni de l'expertise suffisantes pour évaluer et gérer efficacement le risque. Or la sensibilisation au risque numérique et la mise en place de pratiques de gestion solides pourraient leur procurer un avantage concurrentiel utile pour nouer des partenariats avec des organisations de plus grande taille. Pour aider les PME à saisir de telles opportunités et éviter que des risques non gérés ne mettent en péril les PME elles-mêmes, mais aussi leurs partenaires, il est impératif de mettre l'accent sur la sensibilisation et de promouvoir les bonnes pratiques.

Développer des cadres de protection de la vie privée qui soient solides, inclusifs et interopérables

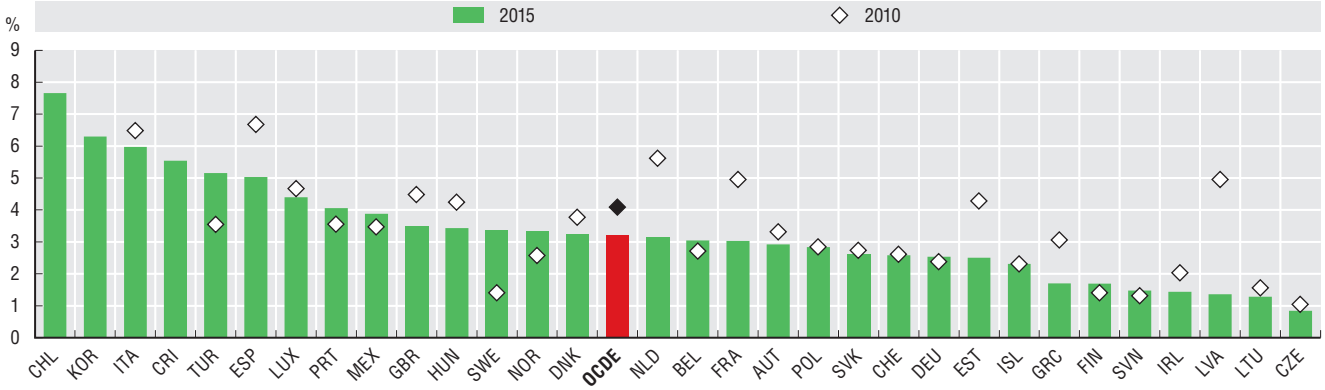
Alors que la transformation numérique gagne du terrain, la protection de la vie privée en général, et des données à caractère personnel en particulier, semble exercer une influence toujours plus critique sur la confiance. Les données à caractère personnel jouent un rôle croissant dans l'économie, la société et la vie quotidienne des individus ; qui plus est, les nouvelles technologies et l'utilisation responsable des données offrent des avantages sociétaux et économiques considérables. Parallèlement, l'abondance de données à caractère personnel recueillies, traitées et échangées fait peser des risques accrus sur la vie privée des individus.

Les risques d'atteinte à la vie privée augmentent à mesure que les entreprises, les fournisseurs d'accès à l'internet et les pouvoirs publics collectent et stockent de plus en plus de données à caractère personnel. Environ 3 % en moyenne des internautes des pays de l'OCDE ont déclaré avoir été victimes d'une violation de leur vie privée au cours des trois derniers mois (graphique 7.1), bien que les chiffres varient sensiblement d'un pays à l'autre. Au Chili, par exemple, quelque 7.5 % des internautes ont fait état d'une violation de leur vie privée, tandis qu'en République tchèque, ils étaient moins de 1 %. Les violations de données à caractère personnel représentent le type d'atteinte à la vie privée le plus courant, et les technologies numériques sont de plus en plus fréquemment utilisées pour obtenir des données personnelles par le rapprochement et l'« exploration » d'ensembles de données (OCDE, 2018[4]).

Les données à caractère personnel sont de plus en plus utilisées à des fins autres que celles prévues au moment de la collecte, avec parfois le recours à des moyens impliquant la divulgation d'informations sensibles ou permettant de relier des données en principe anonymes à des individus particuliers. Avec la croissance des usages et de la valeur des données, les cas de violations se multiplient (OCDE, 2018[4]). Les incidents n'impliquent pas seulement les individus concernés : ils portent également atteinte aux valeurs et principes fondamentaux que la protection de la vie privée et des données à caractère personnel entend promouvoir, à savoir l'autonomie des individus, l'égalité et la liberté d'expression, avec à la clé des conséquences potentielles plus larges sur l'ensemble de la société. D'où la nécessité de mieux gérer les risques de violation de la vie privée et des données à caractère personnel, afin de garantir une protection efficace.

Graphique 7.1. Les atteintes à la vie privée varient considérablement d'un pays à l'autre

Individus ayant subi une violation de leur vie privée, en pourcentage de la population d'internautes, 2015



Note : Voir notes de chapitre[1].

Source : OCDE (2019[5]), *Measuring the Digital Transformation*, *https://dx.doi.org/10.1787/9789264311992-en*, d'après OCDE[6], « Accès et utilisation des TIC par les ménages et les individus » (base de données), *http://oe.cd/hhind* (consultée en septembre 2018).

StatLink https://doi.org/10.1787/888933915411

Le respect de la vie privée est non seulement une valeur fondamentale reconnue qu'il convient de protéger, mais aussi une condition nécessaire à la libre circulation des données à caractère personnel entre les organisations et entre les pays, et, partant, à l'innovation fondée sur les données, la croissance économique et la prospérité sociale (OCDE, 2016[7]). Dans la sphère privée comme professionnelle, les individus partagent plus de données à caractère personnel que jamais – que ce soit délibérément, sur les réseaux sociaux ou ailleurs, ou sans qu'ils le sachent, par le biais du suivi de la navigation sur l'internet ou des smartphones. Par conséquent, plus de la moitié des mesures de protection de la vie privée prises dans les pays de l'OCDE visent à sensibiliser et autonomiser les individus (OCDE, à paraître[8]). Dans le même temps, ils cherchent à obtenir plus de garanties et à exercer un contrôle accru sur la gestion qui est faite de leurs données : ils veulent savoir si des données les concernant sont collectées et stockées – et, le cas échéant, lesquelles –, comment elles sont utilisées et s'ils peuvent les supprimer, les corriger, ou contrôler les éventuels usages secondaires.

En d'autres termes, les individus veulent savoir à qui ils peuvent confier leurs données à moindre risque. Les mesures visant à renforcer la transparence sur la finalité des collectes de données à caractère personnel et les utilisations qui en sont faites, ainsi qu'à élargir les possibilités pour les utilisateurs

d'accéder à leurs données et de les contrôler présentent donc un intérêt tout particulier dans le contexte de la confiance à l'ère du numérique. Les avancées technologiques peuvent aider à renforcer la confiance par l'intégration « par défaut » de processus de protection de la vie privée, avec une prise en compte des considérations de vie privée dès la phase initiale de conception d'un produit ou service, plutôt qu'a posteriori. Cela peut permettre d'intégrer ou de coder dans les technologies des garde-fous, ou de minimiser dès le départ la collecte de données à caractère personnel. La cryptographie, par exemple, peut jouer un rôle important dans la protection de la vie privée, compte tenu du développement des appareils mobiles et de l'internet des objets (IdO) (OCDE, 2018[4]). Les fonctions de re-décentralisation du web offrent une autre solution face aux problématiques de respect de la vie privée : cet ensemble d'innovations technologiques permet de répartir le stockage des données à caractère personnel entre les internautes eux-mêmes, plutôt que de les centraliser aux mains d'un groupe restreint d'entreprises.

Si les technologies peuvent aider à protéger la vie privée et les données à caractère personnel, il est nécessaire que les pays se dotent de stratégies nationales en matière de données, soutenues aux plus hauts niveaux de l'administration et adoptant une perspective à l'échelle de l'ensemble de la société, afin de trouver un juste équilibre entre les divers intérêts individuels et collectifs. De telles stratégies énonceraient clairement la voie à suivre pour tirer parti des avantages économiques et sociaux d'une réutilisation et d'un partage accrus des données, tout en répondant aux préoccupations des individus et des organisations en termes de protection de la vie privée, des données à caractère personnel et des droits de propriété intellectuelle. Elles faciliteraient en outre l'interopérabilité des cadres nationaux et, ce faisant, favoriseraient la libre circulation des données.

Vers une interopérabilité des cadres de protection de la vie privée et des données

Bien que les pays disposent de cadres de protection de la vie privée différents, ils tendent à rechercher les mêmes résultats et utilisent souvent des approches similaires, comme en témoignent les accords sur des principes directeurs de haut niveau et sur la mise en œuvre de bonnes pratiques, ou les législations. La nécessité de mettre au point des mécanismes favorisant l'interopérabilité des cadres de protection des données et de la vie privée est également largement reconnue (OCDE, 2016[7] ; OCDE, 2013[9]). Si les stratégies nationales de protection de la vie privée devraient systématiquement intégrer des dispositions en faveur de l'interopérabilité, rares sont les pays de l'OCDE qui ont mis en œuvre de telles stratégies (OCDE, 2018[4]) et d'autres mécanismes peuvent être identifiés pour assurer l'interopérabilité.

Convergence régionale et harmonisation des cadres de protection de la vie privée

Au nombre des instruments ayant un effet d'harmonisation figure la Convention 108 du Conseil de l'Europe. Mise à jour récemment, elle a un caractère contraignant pour les 47 États membres du Conseil de l'Europe et est ouverte à l'adhésion des États non membres. Autre exemple, le Règlement général sur la protection des données (RGPD) de l'Union européenne a pour objet d'harmoniser les législations en matière de protection des données de l'ensemble des pays de l'Espace économique européen. Des dispositifs non contraignants peuvent également favoriser la convergence des législations de protection de la vie privée et faciliter les flux de données qui en respectent les principes. L'Organisation de coopération économique Asie-Pacifique (APEC) a mis en œuvre un système volontaire mais exécutoire de règles transfrontières de protection de la vie privée, dénommé *Cross-Border Privacy Rules* (CBPR), au titre duquel les économies de l'APEC signataires s'efforcent d'élever le niveau global de protection de la vie privée à l'échelle de la région. Toutefois, les approches diffèrent : tandis que le système CBPR de l'APEC établit des normes de référence pour la protection de la vie privée sans modification des législations nationales, le RGPD de l'UE impose une harmonisation des législations par le biais d'un règlement directement applicable dans les États membres.

Reconnaissance de l'« équivalence » ou de l'« adéquation » des mesures de protection de la vie privée

Les autorités nationales responsables de la protection des données et de la vie privée peuvent certifier que d'autres pays appliquent des principes garantissant une protection équivalente ou compatible. Par exemple, l'article 45 du RGPD de l'UE stipule qu'un transfert de données à caractère personnel peut avoir lieu entre l'Union européenne et un pays tiers dès lors qu'il a été établi que ce dernier assure un niveau de protection adéquat. Israël et la Nouvelle-Zélande sont dans ce cas. D'autres types de mesures peuvent être prises, telles que des clauses contractuelles types, des règles d'entreprise contraignantes pour les multinationales, ou encore des mécanismes de certification, afin d'assortir des

flux transfrontières de données de dispositions exécutoires protégeant les individus dont les données sont transférées. Le Bouclier de protection des données UE-États-Unis est un exemple de mécanisme de certification permettant aux entreprises adhérentes de transférer des données entre les deux espaces économiques sous réserve qu'elles se soient engagées au préalable à respecter un ensemble de principes conformes aux exigences de protection des données en vigueur dans l'UE.

Coopération transfrontière entre les autorités chargées de l'application des mesures de protection de la vie privée

Des principes de haut niveau adoptés d'un commun accord, tels que ceux énoncés dans la *Recommandation du Conseil de l'OCDE sur la coopération transfrontière dans l'application des législations protégeant la vie privée* (OCDE, 2007[23]), peuvent aider à faire en sorte que les autorités compétentes assurent une protection harmonisée des informations personnelles des individus et ce, où qu'elles se trouvent. La participation à des forums, à l'instar du *Global Privacy Enforcement Network*, qui favorise le partage d'informations et la coopération et a conduit à la mise en place d'initiatives conjointes, ou la coopération bilatérale entre les autorités chargées de l'application des mesures de protection de la vie privée, contribuent également à renforcer la coopération transfrontière. L'efficacité des mécanismes d'interopérabilité passe en outre par la coopération et le contrôle de l'application des mesures à l'échelle internationale. Par exemple, une économie souhaitant participer au système CBPR de l'APEC doit également s'engager à respecter le cadre de l'APEC régissant la coopération en matière d'application des règles. À cela s'ajoutent d'autres formes de coopération, comme les mémorandums d'entente et les accords de partage d'informations (OCDE, à paraître[8]).

Accords commerciaux régionaux

Les pays commencent à s'atteler aux questions relatives aux flux de données en intégrant dans des accords commerciaux bilatéraux ou régionaux des dispositions relatives à la protection de la vie privée, en général pour faciliter les flux transfrontières de données. Par exemple, l'Accord Canada–États-Unis–Mexique – qui n'a pas encore été ratifié par les Parlements – prévoit (dans son article 19.8) l'adoption ou le maintien d'un cadre juridique assurant la protection des renseignements personnels, tout en précisant qu'aucune partie ne doit limiter le transfert transfrontière de renseignements, sauf conditions particulières servant des objectifs légitimes de politique publique (article 19.11) (Casalini et López González, 2019[10]).

Mesures pour les entreprises et entités de pays qui ne reconnaissant pas leurs systèmes respectifs de protection des données

Le RGPD, qui prévoit des mécanismes régissant l'application par les entreprises multinationales de « règles d'entreprise contraignantes » à l'ensemble des entreprises affiliées afin de permettre les flux de données entre ces entités, même si les entreprises affiliées sont implantées dans des pays ne disposant pas d'un mécanisme spécifique ou n'ayant pas conclu d'accord en ce sens, offre un exemple concret de recours à des règles de protection de la vie privée en cas de non-reconnaissance réciproque des législations de protection des données de différents pays. De même, certaines autorités de contrôle de l'application des mesures de protection de la vie privée ont défini des clauses contractuelles types pouvant être utilisées dans n'importe quel contrat ou accord régissant le transfert de données entre des entités implantées dans des pays ne reconnaissant pas les dispositifs respectifs de protection des données ou de la vie privée. Toutefois, certaines entreprises considèrent que de telles clauses imposent de lourdes obligations et peuvent donner lieu à des coûts administratifs élevés (Casalini et López González, 2019[10]).

Gérer le risque de sécurité numérique plutôt que de chercher à l'éliminer

Un aspect important de la transformation numérique tient à la nécessité de renforcer la résilience et la sécurité afin de limiter les éventuelles perturbations des activités économiques et sociales consécutives à des incidents de sécurité numérique. La dimension mondiale de l'internet facilite la propagation de tels incidents par-delà les frontières juridictionnelles, organisationnelles et sectorielles, comme en témoignent les récentes attaques Wannacry, NotPetya et Dyn. Les incidents de sécurité numérique peuvent perturber les activités de tous types d'entreprises – PME ou grandes sociétés –, des administrations et des particuliers, et causer des préjudices financiers et des atteintes à la réputation. Ainsi, l'attaque NotPetya a temporairement mis à l'arrêt les sites de production de plusieurs entreprises

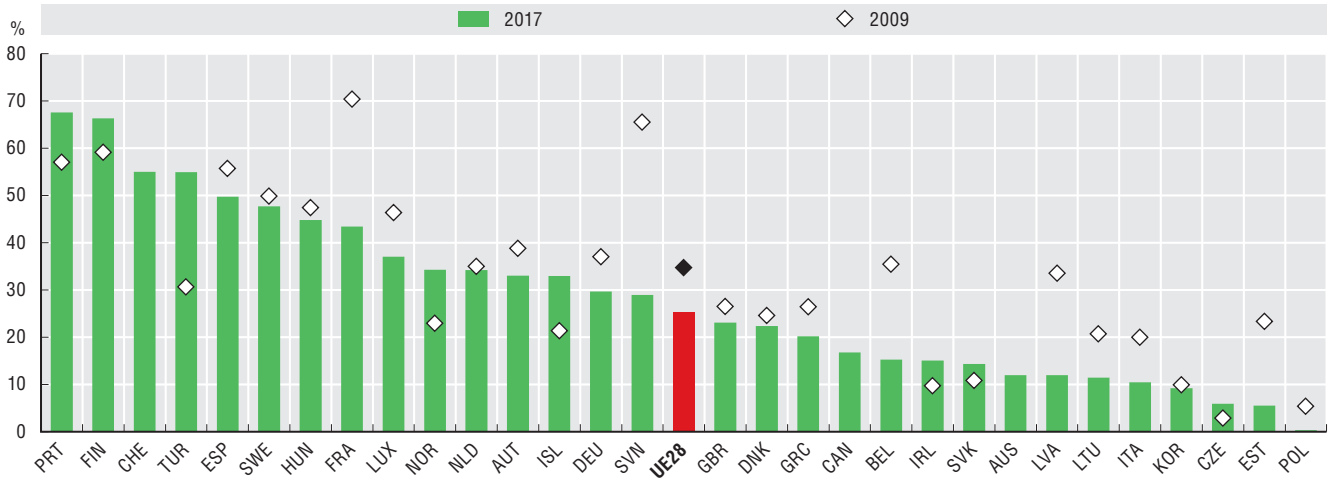
internationales, à l'instar par exemple de Merck, qui a dû puiser dans les réserves de vaccins de l'*US Center for Disease Control and Prevention* pour satisfaire ses commandes, ce qui lui a coûté un manque à gagner de 240 millions USD au troisième trimestre de 2017 (Merck, 2017[11] ; Hufford et Loftus, 2017[12]).

Les incidents de sécurité numérique peuvent également causer des dommages matériels, comme le montre celui à l'origine des pannes d'électricité survenues en Ukraine qui ont privé de courant quelque 225 000 clients en 2015 (NCCIC, 2016[13] ; Popescu et Secrieru, 2018[14]). Il peut aussi en résulter une crise de grande envergure dès lors que des infrastructures indispensables au bon fonctionnement de l'économie et de la société sont touchées, notamment dans les secteurs de la finance, de l'énergie et des transports, ainsi que dans les services essentiels des administrations publiques. Outre ces scénarios catastrophes, les incidents de sécurité numérique peuvent avoir des effets subtils, mais dommageables sur le long terme : ils peuvent saper la confiance dans l'environnement numérique, brider l'innovation, freiner l'adoption des nouvelles technologies et entraver la transformation numérique et la concrétisation des avantages qui en découlent.

Le risque lié aux incidents de sécurité va croissant à mesure que la transformation numérique gagne du terrain. D'ailleurs, près de 30 % des internautes s'abstiennent de fournir des informations personnelles sur les réseaux sociaux et professionnels du fait des menaces qui pèsent sur la sécurité numérique (OCDE, 2018[4]). La sécurité des paiements en ligne et les inquiétudes quant au respect de la vie privée restent prégnantes dans de nombreux pays – plus de la moitié des internautes au Portugal (68 %), en Finlande (66 %), en Suisse (55 %) et en Turquie (55 %) faisaient état de telles préoccupations en 2017 (graphique 7.2). Les pays affichant au cours de la même période les taux les plus faibles d'individus préoccupés par la sécurité des paiements et les atteintes à la vie privée étaient la Pologne (moins de 1 %), l'Estonie (6 %), la République tchèque (6 %) et la Corée (9 %).

Graphique 7.2. Les inquiétudes quant à la sécurité des paiements et la protection de la vie privée restent d'actualité dans de nombreux pays

Individus n'ayant pas réalisé d'achats en ligne pour des raisons liées à la sécurité des paiements ou au respect de la vie privée, en pourcentage du nombre d'internautes n'ayant pas acheté de biens ou de services sur l'internet depuis plus d'un an ou n'ayant jamais réalisé de tels achats, 2017



Note : Voir notes de chapitre[2].

Source : Calculs de l'OCDE, d'après (Eurostat[15]), *Économie et société numériques* (base de données), *https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/comprehensive-database* ; sources nationales (consultées en décembre 2018).

StatLink https://doi.org/10.1787/888933914917

Compte tenu de l'impossibilité de créer un environnement numérique totalement sûr et sécurisé, les entreprises, les autres organisations et les individus prennent toujours un certain risque en se tournant vers le numérique. Il importe donc de les encourager à comprendre comment gérer ce risque de manière à ne pas restreindre les opportunités économiques et sociales offertes par l'utilisation des cybertechnologies. Ils peuvent pour ce faire mettre en œuvre des normes de sécurité (à l'instar de celles de la famille ISO 27000, par exemple) afin de renforcer la résilience et d'assurer la continuité opérationnelle en limitant les conséquences d'éventuels incidents de sécurité. Dans la mesure où

toutes les parties prenantes sont interdépendantes dans l'environnement numérique et à l'échelle internationale, il est essentiel de les inciter à nouer des partenariats en vue de réduire les risques et de promouvoir les bonnes pratiques de gestion, en particulier grâce au partage d'informations sur les menaces, les vulnérabilités, les incidents et les pratiques de gestion du risque, y compris avec les PME.

Les politiques visant à favoriser la sécurité numérique peuvent aider à instaurer des conditions propices pour que les organisations adoptent des cadres de gestion du risque de sécurité numérique, que les entreprises mettent au point des technologies moins vulnérables et plus sûres, et que les individus aient une meilleure compréhension des risques et utilisent les appareils numériques de manière plus responsable. L'action des pouvoirs publics peut également contribuer à remédier à la pénurie croissante de compétences en matière de sécurité numérique qui concerne à la fois les experts techniques et les responsables opérationnels, et à encourager l'innovation dans le domaine de la sécurité numérique et le développement d'un secteur spécialisé dynamique. La cyberassurance peut représenter un élément important de la gestion du risque puisqu'elle permet le transfert d'une partie du risque de sécurité numérique et incite les parties prenantes à adopter de meilleures pratiques de gestion.

La sécurité numérique et la résilience des infrastructures et des services critiques essentiels au fonctionnement des économies et des sociétés représentent un volet particulièrement important de la politique de sécurité numérique, au croisement de la prospérité économique et de la sécurité nationale. La transformation numérique accroît sensiblement les interdépendances et la complexité de ces systèmes vitaux, ainsi que le risque de défaillance systémique susceptible d'engendrer des effets en cascade sur différents secteurs et par-delà les frontières. C'est pourquoi les pouvoirs publics doivent prendre des mesures qui aident et encouragent les opérateurs d'infrastructures et de services critiques à renforcer leur sécurité numérique. Ce faisant, ils doivent les aider à tirer le meilleur parti de la transformation numérique, notamment via l'adoption de technologies comme l'IdO, l'intelligence artificielle, l'analytique des données massives et la technologie blockchain, tout en tenant compte des spécificités commerciales, réglementaires et culturelles des différents secteurs. Alors que les infrastructures critiques et les services essentiels sont souvent aux mains de grands opérateurs du secteur privé, la transformation numérique permet également aux PME de prendre part aux chaînes de valeur des services essentiels (OCDE, 2019[16]).

Dans les secteurs de la finance, de l'énergie et des transports, la transformation numérique pose un défi de taille lié au rôle grandissant des petites structures comme les PME, qui fait sortir les risques de sécurité numérique du périmètre des grands acteurs centraux que sont les banques ou les compagnies d'électricité. Ces PME sont notamment des startups qui proposent des systèmes de paiement innovants, des technologies basées sur la blockchain pour le négoce de l'énergie, ou encore des services de mobilité dans le domaine des transports. À cela s'ajoutent des PME solidement implantées, spécialisées dans la prestation de services essentiels, qui jouent un rôle croissant dans la gestion du risque de sécurité numérique afin d'atténuer le risque pour les grandes entreprises au sein de leurs chaînes de valeur.

La sécurité numérique est un domaine d'action pluridimensionnel qui touche à la fois aux questions liées à la prospérité économique et sociale, aux technologies, au droit pénal, ou encore à la sécurité nationale et internationale. Du point de vue économique et social, le risque de sécurité numérique a généralement été abordé comme un problème purement technique appelant des solutions techniques, mais l'évolution de la nature et de l'échelle du risque conduit les pouvoirs publics à réévaluer leurs stratégies afin de faire évoluer les mentalités dans ce domaine.

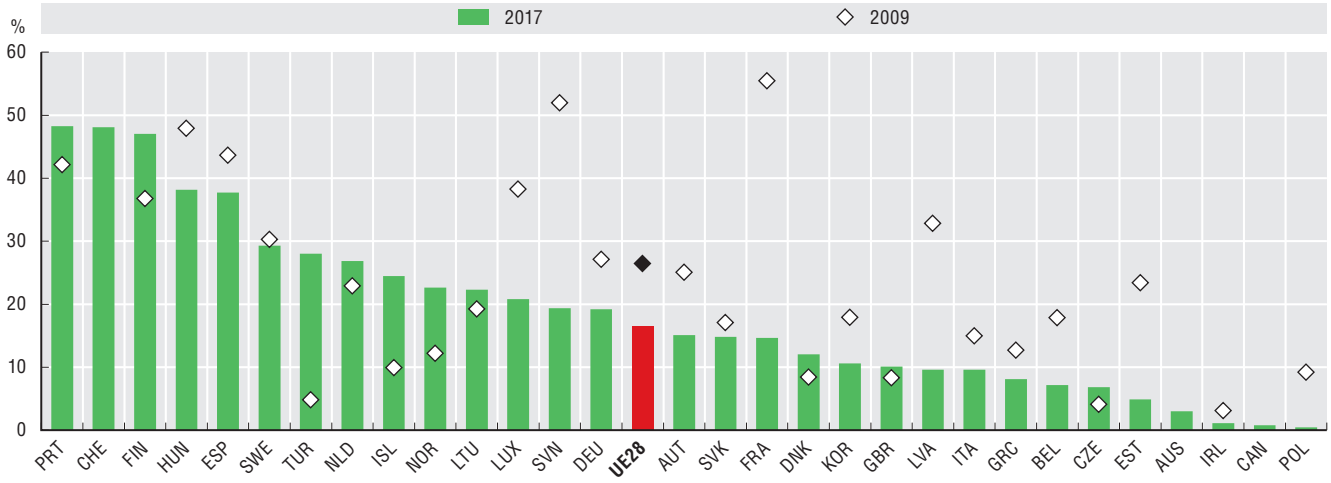
Protéger les consommateurs à l'heure où les mondes physique et virtuel convergent

La protection des consommateurs dans l'environnement numérique est une autre condition essentielle pour bâtir la confiance dans le commerce électronique comme dans l'utilisation de nouvelles technologies telles que l'IdO (voir encadré 7.2). Elle offre la possibilité de conquérir de nouveaux clients et de nouveaux marchés, avec, à la clé, des retombées économiques plus larges. La mise en place de marchés du commerce électronique florissants nécessite plus qu'une infrastructure haut débit, des services d'hébergement et de paiement, et des logiciels spécialisés. Elle exige des consommateurs qu'ils dépassent leurs doutes à l'égard des transactions réalisées à distance, sans pouvoir examiner les biens avant d'acheter, leurs craintes quant aux risques qu'ils encourent en communiquant leurs informations bancaires en ligne, et leurs inquiétudes quant aux possibilités de recours ou de réparation en cas de problème.

Si les préoccupations liées à la réception ou au retour de biens, aux réclamations ou aux dédommagements ont en moyenne diminué au cours des dix dernières années, elles demeurent malgré tout importantes (graphique 7.3). C'est au Portugal (48 %), en Suisse (48 %), en Finlande (47 %) et en Hongrie (38 %) que l'on observe les taux les plus élevés. De l'autre côté du spectre, la protection des consommateurs inquiète moins de 1 % des internautes en Pologne et au Canada ; suivent l'Irlande (1 %) et l'Australie (3 %).

Graphique 7.3. Les achats de biens en ligne continuent de susciter des inquiétudes quant à la protection des consommateurs

Individus n'ayant pas réalisé d'achats en ligne pour des raisons liées à la réception ou au retour des biens, ou aux possibilités de réclamation ou de réparation, en pourcentage du nombre d'internautes n'ayant pas acheté de biens ou de services sur l'internet depuis plus d'un an ou n'ayant jamais réalisé de tels achats, 2017



Note : Voir notes de chapitre[3].

Source : Calculs de l'OCDE, d'après (Eurostat[15]), *Économie et société numériques* (base de données), *https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/comprehensive-database* ; sources nationales (consultées en décembre 2018).

StatLink https://doi.org/10.1787/888933914936

Autre source d'inquiétude, on note une multiplication des produits non conformes et dangereux proposés à la vente sur l'internet, au niveau tant national et qu'international, alors qu'ils ont été interdits à la vente ou ont fait l'objet d'un rappel. Dans le cadre de ses activités annuelles mondiales de sensibilisation à la sécurité des produits de consommation, l'OCDE a mené en 2018 une campagne de sensibilisation à la sécurité des produits vendus sur l'internet[4], afin d'informer les plateformes électroniques, les cybervendeurs et les cyberconsommateurs des moyens de détecter les risques de sécurité et de s'y retrouver dans les réglementations applicables selon les juridictions.

La mise en place d'une protection efficace des consommateurs ayant recours au commerce électronique et menant d'autres activités sur l'internet est une condition essentielle à la prospérité de l'économie numérique. Les transactions portant sur des contenus numériques et les frontières de plus en plus poreuses entre les consommateurs et les entreprises peuvent également venir brouiller les notions traditionnelles de propriété, de responsabilité, de droits et d'obligations. Les principaux problèmes qui se posent ont trait à la divulgation des informations, aux pratiques commerciales trompeuses et déloyales, aux processus de confirmation et de paiement, aux cas de fraude et d'usurpation d'identité, à la sécurité des produits, et aux mécanismes de règlement et de réparation des litiges.

Par exemple, il est de plus en plus fréquent que des consommateurs acquièrent des biens et des services dits « gratuits » en contrepartie de leurs données personnelles, dans le cadre de transactions non monétaires, ce qui peut rendre inopérants les mécanismes traditionnels de règlement des litiges (OCDE, 2016[17]). De même, avec l'émergence de nouvelles formes d'utilisation des actifs et des contenus, notamment par le biais des services de location, de partage d'actifs et d'abonnement, les consommateurs peinent à appréhender leurs droits et obligations (encadré 7.2). Sans compter que, bien souvent, les limitations de fonctionnalités et d'interopérabilité des produits numériques ne sont pas énoncées clairement. Les pratiques de tarification peuvent également poser problème aux

consommateurs, par exemple lorsque les entreprises ne communiquent pas en amont l'ensemble des éléments de tarification (pratiques dites de « frais cachés ») ou utilisent des prix de référence trompeurs pour exploiter les biais comportementaux des consommateurs.

Encadré 7.2. Confiance dans les marchés de plateformes de mise en relation

Si les transactions entre particuliers jouent de longue date un rôle dans le commerce traditionnel, elles prennent aujourd'hui une dimension sans précédent avec les plateformes électroniques. Aux premières plateformes, dédiées à la vente de biens (à l'instar des sites d'enchères en ligne, par exemple), succèdent des modèles nouveaux, fondés sur l'offre de services d'hébergement, de transport et de mobilité. D'autres domaines sont également en pleine transformation, comme les petits boulots, les services de restauration et les services financiers. On parle souvent de l'« économie du partage » ou de la « consommation collaborative » pour désigner les modèles économiques qui sous-tendent ces activités, mais ces expressions ne reflètent que sommairement la réalité des échanges commerciaux qui ont cours sur ces marchés.

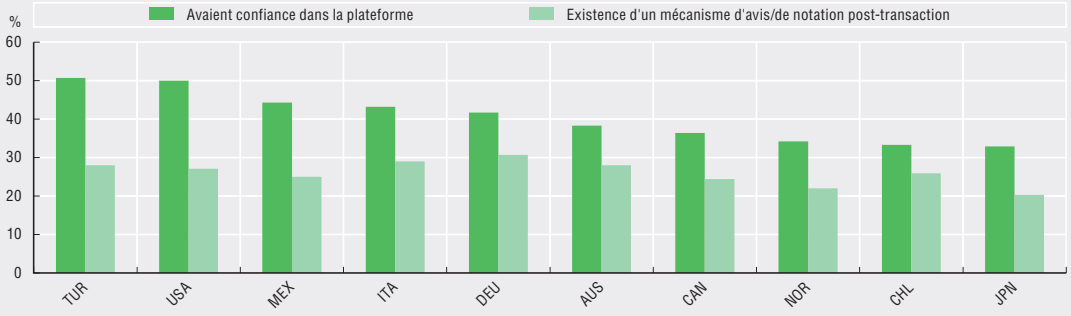
Ces modèles ouvrent la voie à des opportunités économiques pour les personnes qui fournissent les biens ou les services (« particuliers fournisseurs ») et pour les plateformes qui assurent l'interface (« plateformes de mise en relation »). L'utilisation des plateformes peut poser aux consommateurs divers problèmes de confiance selon les situations rencontrées : confiance dans la fiabilité et les qualifications des particuliers fournisseurs ; dans les biens ou les services fournis ; dans les garanties et mesures de protection mises en place par les plateformes. Or, les conditions d'utilisation ne suffisent pas toujours à communiquer les informations importantes aux consommateurs. De fait, seuls 17 % des utilisateurs lisent l'intégralité des conditions générales des plateformes (comme Airbnb et BlaBlaCar).

Pour lever les inquiétudes et les obstacles qui freinent la participation des consommateurs, les plateformes ont mis au point un certain nombre de mécanismes pratiques innovants. Au premier rang des mécanismes de confiance figurent les systèmes de publication d'avis et de réputation. À cela s'ajoutent les garanties ou assurances ; la vérification de l'identité des intervenants ; la présélection des fournisseurs ; les systèmes de paiement sécurisé ; et la sensibilisation, les listes de contrôle et les formulaires (OCDE, 2016[18]).

Pour mieux appréhender les déterminants de la confiance dans les marchés des plateformes de mise en relation, l'OCDE a réalisé une enquête en ligne auprès de 10 000 consommateurs répartis dans dix pays membres de l'Organisation (OCDE, 2017[19]). Il en est ressorti que les consommateurs ont généralement confiance dans les marchés de plateformes de mise en relation, souvent davantage que dans des entreprises traditionnelles opérant sur les mêmes marchés. L'enquête révèle qu'au moins 30 % des consommateurs ayant réalisé un achat sans être assurés de la fiabilité du vendeur l'ont fait parce qu'ils avaient confiance dans la plateforme (graphique 7.4).

Graphique 7.4. Les consommateurs tendent à faire confiance aux plateformes de mise en relation

Raisons de réaliser un achat sur une plateforme sans être assuré de la fiabilité du vendeur ou du fournisseur, en pourcentage du nombre total d'acheteurs ayant effectué un achat sur une plateforme sans être sûrs du vendeur ou du fournisseur, 2017



Source : OCDE (2019[5]), *Measuring the Digital Transformation*, *https://dx.doi.org/10.1787/9789264311992-en*, calculs de l'OCDE d'après OCDE (2017[19]), « Trust in peer platform markets: Consumer survey findings », *https://dx.doi.org/10.1787/1a893b58-en*.

StatLink *https://doi.org/10.1787/888933915430*

Encadré 7.2. Confiance dans les marchés de plateformes de mise en relation *(suite)*

Bien que la confiance ne dépende pas d'un déterminant unique, la sécurisation des paiements, la sécurité des données et la publication de photos des biens et des services en sont les principaux vecteurs. Paradoxalement, les utilisateurs des plateformes de mise en relation ne lisent pas toujours en détail leurs conditions d'utilisation ou leur politique de confidentialité, alors qu'ils déclarent accorder une grande importance au respect de leur vie privée et à la sécurité de leurs données. Cela ne semble pas pour autant nuire à la confiance des consommateurs dans l'utilisation responsable de leurs données à caractère personnel par les plateformes, en particulier en comparaison des autres types d'entreprises opérant sur l'internet.

Source : OCDE (2017[19]), « Trust in peer platform markets: Consumer survey findings », *https://dx.doi.org/10.1787/1a893b58-en*.

Sur les marchés financiers, les individus (notamment ceux présentant une habileté numérique limitée) devront acquérir des compétences et des connaissances nouvelles pour pouvoir utiliser les produits et les services numériques en toute efficacité et comprendre les ramifications potentielles du partage des données avec les établissements. De plus, le recours croissant aux processus automatisés et aux services de soutien non humains (avec les robots conseillers et les agents conversationnels) appelle la mise en place d'une gouvernance et de contrôles pour assurer une protection des consommateurs de services financiers en ligne comparable à celle offerte pour les services traditionnels. Sans compter que les transactions dématérialisées tendent à exacerber des problématiques qui se posent dans l'environnement hors ligne quant au niveau de compréhension, par les consommateurs, des conditions et de la nature des transactions menées à bien, une question d'autant plus cruciale qu'un nombre croissant d'activités numériques sont réalisées à partir de téléphones mobiles.

Encadré 7.3. Consommateurs et internet des objets

Les consommateurs interagissent avec un éventail croissant d'appareils connectés, à domicile et dans leur vie quotidienne, dans le cadre de ce que l'on dénomme l'internet des objets (IdO). Il peut s'agir de technologies prêt-à-porter (moniteurs d'activité physique ou montres et lunettes intelligentes, par exemple), d'équipements domotiques et d'appareils électroménagers intelligents (tels que des verrous et des thermostats capables d'informer les utilisateurs de leur consommation et de leur profil énergétique), ou encore de jouets et de matériel de puériculture connectés.

Parmi les nombreux avantages de l'IdO, les consommateurs plébiscitent la facilité d'utilisation et les possibilités de personnalisation et de contrôle à distance à partir d'un smartphone (OCDE, 2018[20]). Qui plus est, l'IdO devrait révolutionner la manière d'améliorer les processus de conception, de fabrication et de livraison des produits et apporter un certain nombre d'avantages en termes de sécurité des produits. Par exemple, les appareils connectés, à l'instar des thermostats ou des détecteurs de fumée intelligents peuvent être surveillés, mis à jour ou désactivés à distance, ce qui permet une meilleure gestion des risques de sécurité des produits (y compris des rappels) après leur installation (OCDE, 2018[21] ; OCDE, 2018[22]).

Bien que prometteur, l'IdO est également synonyme de risques et de défis susceptibles de mettre à mal la confiance dans ce marché émergent. Les mises à jour logicielles pourraient par exemple nuire au fonctionnement des produits connectés ou poser des problèmes de conformité. Les risques de sécurité numérique et les vulnérabilités peuvent également compromettre la sécurité des produits connectés. La complexité des chaînes d'approvisionnement de l'IdO peut être source d'incertitudes quant aux responsabilités en cas de dommages causés par un produit connecté et soulever des questions plus larges quant à la nécessité éventuelle d'adapter les cadres de protection des consommateurs et de sécurité des produits face à ces nouveaux défis.

D'une manière générale, il est impératif de faire de la gestion du risque un cadre de référence commun pour l'élaboration de politiques cohérentes à l'appui du renforcement de la confiance, en impliquant les différents secteurs de l'action des pouvoirs publics travaillant sur la sécurité numérique, la protection de la vie privée, la protection des consommateurs et la sécurité des produits. Les décideurs doivent notamment tenir compte des interactions entre les risques numériques dans chacun des domaines. De fait, un incident de sécurité numérique au cours duquel les données des consommateurs sont volées dans l'optique d'une utilisation frauduleuse peut relever d'une atteinte à la fois à la vie privée et aux droits des consommateurs. Compte tenu de ces interférences, la coordination des politiques dans ces domaines doit être un préalable à l'adoption d'une approche plus exhaustive de la confiance à l'ère du numérique.

Notes

Israël

Les données statistiques concernant Israël sont fournies par et sous la responsabilité des autorités israéliennes compétentes. L'utilisation de ces données par l'OCDE est sans préjudice du statut des hauteurs du Golan, de Jérusalem Est et des colonies de peuplement israéliennes en Cisjordanie aux termes du droit international.

1. Graphique 7.1 : Sauf mention contraire, les « internautes » désignent les individus ayant accédé à l'internet au cours des 12 derniers mois. Pour le Chili, les données se rapportent à 2014. Pour le Costa Rica, les données portent sur les individus âgés de 18 à 74 ans et non de 16 à 74 ans. Pour la Corée, les données se rapportent à 2017 et couvrent les activités à visée à la fois personnelle et professionnelle. Pour le Mexique, les données se rapportent à 2017 et non pas 2015. À partir de 2015, les informations ont été collectées par le biais d'une enquête thématique indépendante, tandis que pour les années précédentes, elles sont issues d'un module administré dans le cadre de plusieurs enquêtes. Il convient de tenir compte de ce changement méthodologique si l'on compare des données antérieures à 2015. Pour 2017, les données se rapportent à l'élément de réponse suivant : « Fraude exploitant des informations (financières, personnelles, etc.) ». Pour la Suisse, les données se rapportent à 2014 et non pas 2015. Les données relatives à 2014 concernent les individus ayant connu un problème de sécurité au cours des 12 derniers mois.
2. Graphique 7.2 : Pour l'Australie, les données se rapportent à l'exercice budgétaire 2012/13 clos au 30 juin 2013. Pour le Canada, elles concernent 2012. Pour les pays couverts par le Système statistique européen, en 2017, la catégorie « Inquiétudes quant à la sécurité des paiements et au respect de la vie privée » n'intègrent pas les « inquiétudes quant au respect de la vie privée ».
3. Graphique 7.3 : Pour l'Australie, les données se rapportent à l'exercice budgétaire 2012/13 clos au 30 juin 2013. Pour le Canada, elles se rapportent à 2012.
4. *http://oe.cd/safe-products-online*.

Références

Casalini, F. et J. López González (2019), « Trade and Cross-Border Data Flows », *OECD Trade Policy Papers*, n° 220, Éditions OCDE, Paris, *https://doi.org/10.1787/b2023a47-en*. [10]

Eurostat (2018), *Digital Economy and Society Statistics* (base de données), *https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/comprehensive-database* (consultée en décembre 2018). [15]

Hufford, A. et P. Loftus (2017), *Merck Swings to Loss as Cyberattack Hurts Sales*, *https://www.wsj.com/articles/merck-swings-to-loss-as-cyberattack-hurts-sales-1509107269*, (consulté le 21 février 2019). [12]

Mayer, R., J. Davis et D. Schoorman (1995), « An integrative model of organizational trust », *The Academy of Management Review*, vol. 20, n° 3, pp. 709-734, *http://www.jstor.org/stable/258792*. [3]

Merck (2017), *Merck Announces Second-quarter 2017 Financial Results*, communiqué de presse, 28 juillet, *https://www.mrknewsroom.com/news-release/corporate-news/merck-announces-second-quarter-2017-financial-results* (consulté le 21 février 2019). [11]

Murtin, F. et al. (2018), « Trust and its determinants: Evidence from the Trustlab experiment », *OECD Statistics Working Papers*, n° 2018/2, Éditions OCDE, Paris, *https://dx.doi.org/10.1787/869ef2ec-en*. [2]

NCCIC (2016), *Cyber-attack against Ukrainian Critical Infrastructure*, *https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01*, (consulté le 21 février 2019). [13]

OCDE (2019), « Accès et utilisation des TIC par les ménages et les individus », *Statistiques de l'OCDE sur les télécommunications et l'internet* (base de données), *https://doi.org/10.1787/6bca1fd3-fr* (consultée le 28 janvier 2019). [6]

OCDE (2019), « Digital security and resilience in critical infrastructure and essential services », *Documents de travail de l'OCDE sur l'économie numérique*, n° 281, Éditions OCDE, Paris, *https://doi.org/10.1787/a7097901-en*. [16]

OCDE (2019), *Measuring the Digital Transformation: A Roadmap for the Future*, Éditions OCDE, Paris, *https://dx.doi.org/10.1787/9789264311992-en*. [5]

OCDE (2018), « 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*. [20]

OCDE (2018), « Consumer product safety in the Internet of Things », *Documents de travail de l'OCDE sur l'économie numérique*, n° 267, Éditions OCDE, Paris, *https://doi.org/10.1787/c7fa-en*. [21]

OCDE (2018), « Enhancing product recall effectiveness globally: OECD background report », *OECD Science, Technology and Industry Policy Papers*, n° 50, Éditions OCDE, Paris, *https://dx.doi.org/10.1787/74ef71935c8-en*. [22]

OCDE (2018), *Perspectives de l'économie numérique de l'OCDE 2017*, Éditions OCDE, Paris, *https://doi.org/10.1787/9789264282483-fr*. [4]

OCDE (2017), *OECD Guidelines on Measuring Trust*, Éditions OCDE, Paris, *https://dx.doi.org/10.1787/9789264278219-en*. [1]

OCDE (2017), « Trust in peer platform markets: Consumer survey findings », *Documents de travail de l'OCDE sur l'économie numérique*, n° 263, Éditions OCDE, Paris, *https://dx.doi.org/10.1787/1a893b58-en*. [19]

OCDE (2016), *Déclaration ministérielle sur l'économie numérique : Innovation, croissance et prospérité sociale,* OCDE, Paris, *http://www.oecd.org/fr/sti/ieconomie/Declaration-ministerielle-de-Cancun.pdf*. [7]

OCDE (2016), « Protecting Consumers In Peer Platform Markets: Exploring the Issues », n° 253, Éditions OCDE, Paris, *https://dx.doi.org/10.1787/5jlwvz39m1zw-en*. [18]

OCDE (2016), *Recommandation du Conseil sur la protection du consommateur dans le commerce électronique*, Éditions OCDE, Paris, *https://doi.org/10.1787/9789264255272-fr*. [17]

OCDE (2013), *Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, OCDE, Paris, *https://legalinstruments.oecd.org/public/doc/115/115.fr.pdf*. [9]

OCDE (2007), *Recommandation du Conseil sur la coopération transfrontière dans l'application des législations protégeant la vie privée*, OCDE, Paris, *https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0352*. [23]

OCDE (à paraître), « Towards national privacy strategies », *Documents de travail de l'OCDE sur l'économie numérique*, Éditions OCDE, Paris. [8]

Popescu, N. et S. Secrieru (2018), « Hacks, leaks and disruptions: Russian cyber strategies », *Chaillot Paper,* n° 148, *https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf*. [14]

Extrait de :

Going Digital: Shaping Policies, Improving Lives

Accéder à cette publication :
https://doi.org/10.1787/9789264312012-en

Merci de citer ce chapitre comme suit :

OCDE (2019), « Renforcer la confiance », dans *Going Digital: Shaping Policies, Improving Lives*, Éditions OCDE, Paris.

DOI: https://doi.org/10.1787/0cfd8503-fr