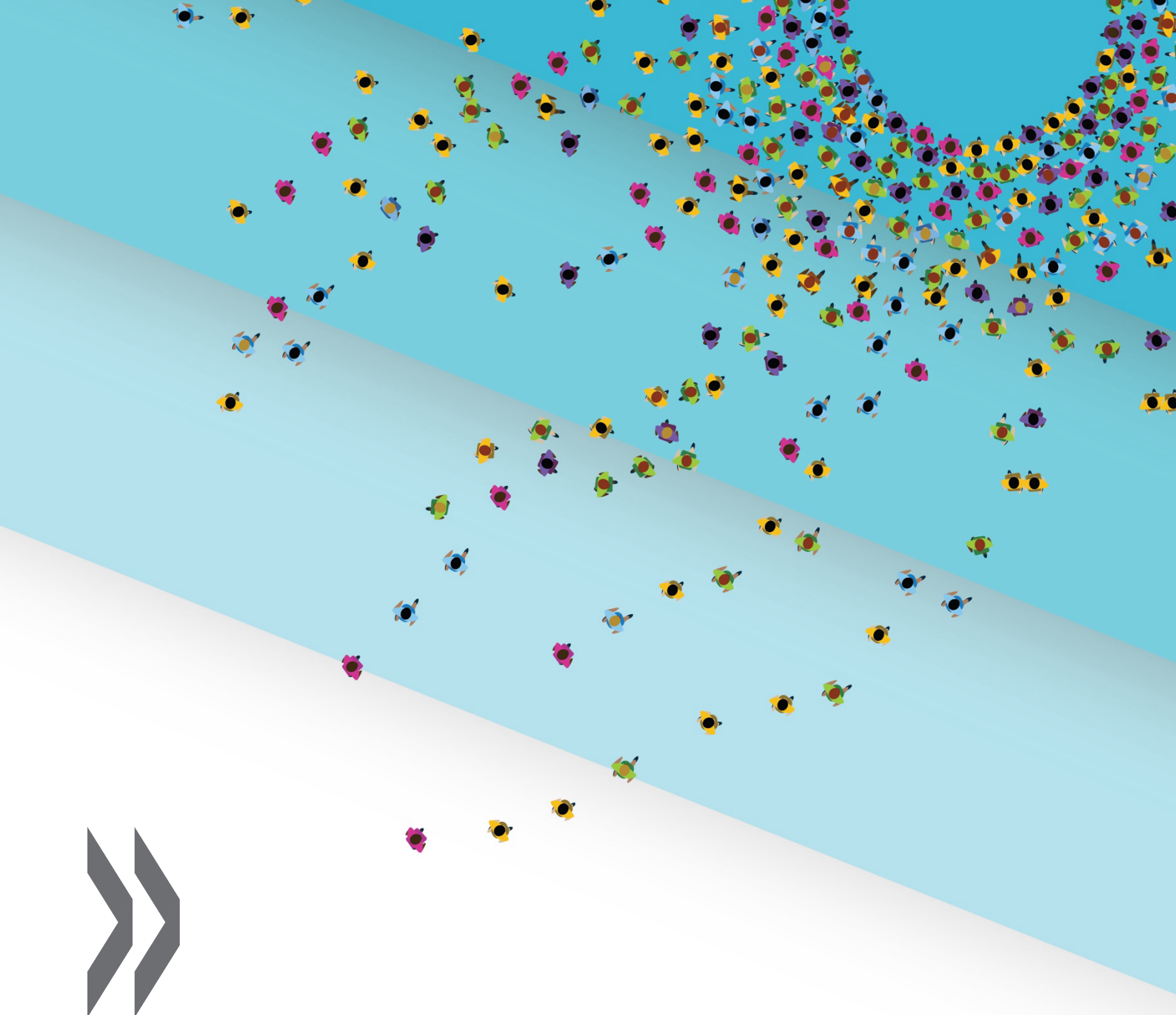




Protéger et autonomiser les consommateurs dans la transition numérique

NOTE THÉMATIQUE

La présente Note thématique fournit des éléments de référence destinés à étayer les discussions de la Réunion ministérielle de l'OCDE sur la politique à l'égard des consommateurs.

Cet ouvrage est publié sous la responsabilité du Secrétaire général de l'OCDE. Les opinions exprimées et les arguments employés ici ne reflètent pas nécessairement les vues officielles des pays Membres de l'OCDE.

Ce document, ainsi que les données et cartes qu'il peut comprendre, sont sans préjudice du statut de tout territoire, de la souveraineté s'exerçant sur ce dernier, du tracé des frontières et limites internationales, et du nom de tout territoire, ville ou région.

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.

Crédits photo : Shutterstock et Adobe Stock

POINTS CLÉS

En permettant d'accéder facilement aux biens, aux services et à l'information, les marchés numériques promettent d'améliorer la vie des consommateurs. Mais beaucoup de ces marchés ne fonctionnent pas de sorte que les consommateurs puissent en tirer le meilleur parti. Les modèles économiques et les technologies numériques peuvent créer et exacerber des asymétries d'information et des asymétries de pouvoir structurelles, et ainsi favoriser l'émergence de pratiques susceptibles de tromper les consommateurs et de les exploiter et, ce faisant, réduire leurs choix, saper leur confiance et placer les entreprises honnêtes dans des conditions de concurrence inégales.

Les travaux empiriques de l'OCDE mettent en lumière la façon dont de nombreux consommateurs rencontrent des problèmes en ligne et comment leurs décisions peuvent être fortement influencées à leurs dépens par des techniques de manipulation et de conception en ligne. Les faux avis, les pratiques de personnalisation à des fins d'exploitation, la collecte, le traçage et le partage des données intrusifs et étendus, l'exploitation de biais comportementaux, la discrimination algorithmique, la fraude et les escroqueries sont d'autres risques auxquels les consommateurs sont exposés. Tous les consommateurs sont potentiellement vulnérables à ces pratiques, et certains groupes, définis par exemple par âge ou genre, le sont plus spécifiquement. Les conséquences en sont des préjudices substantiels de vaste portée, allant de pertes financières et d'atteintes à la vie privée, à des dommages psychologiques.

La mise en place d'un cadre d'action solide et efficace permet aux consommateurs de faire confiance aux marchés numériques. De nombreuses autorités chargées de la protection des consommateurs ont pris des mesures contre les pratiques numériques préjudiciables. Néanmoins, on peut se demander si les lois et les mécanismes d'application en vigueur sont suffisamment efficaces pour traiter les préjudices résultant du numérique, et certains pays ou territoires ont d'ailleurs introduit de nouvelles législations. Étant donné que les risques auxquels les consommateurs sont exposés à l'ère du numérique existent par-delà les frontières et les domaines d'action, il faut mettre en place une coopération internationale et interdisciplinaire.

LA TRANSITION NUMÉRIQUE : UNE ARME À DOUBLE TRANCHANT POUR LES CONSOMMATEURS

La transition numérique a profondément modifié l'interaction des consommateurs avec le marché. Les marchés numériques qui fonctionnent bien peuvent profiter aux consommateurs en leur offrant une facilité d'accès aux biens, aux services et à des informations plus complètes qui les aident à prendre des décisions éclairées. Les technologies numériques comme l'intelligence artificielle (l'IA), l'Internet des objets (l'IdO) et la réalité virtuelle, peuvent contribuer à améliorer la vie des consommateurs.

Toutefois, elles présentent aussi des inconvénients. Le fait que le commerce électronique soit une activité de

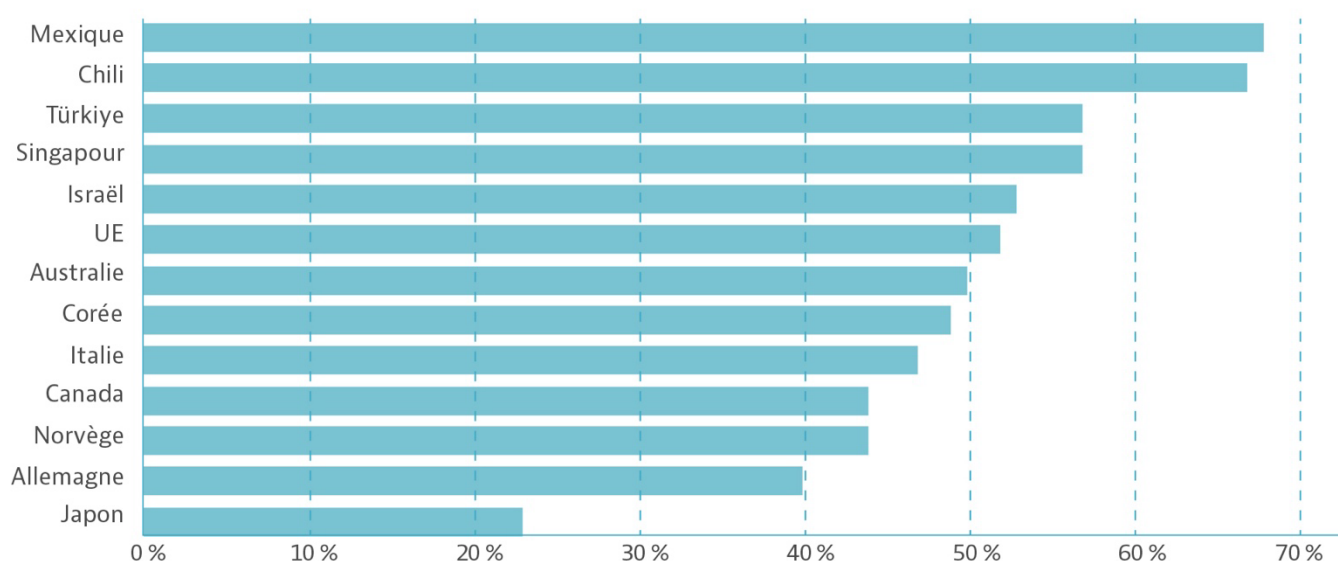
vente à distance expose les consommateurs à des indicateurs de qualité ou de sécurité qui ne sont pas fiables (comme les faux avis), à des types de transactions qui ne leur sont pas familiers et qui sont souvent délibérément complexes (par exemple, les abonnements payants non sollicités, les paiements avec données personnelles ou les microtransactions occultées), et à des difficultés à obtenir réparation en cas de problèmes. Si un grand nombre de ces problèmes surviennent également dans les magasins physiques (des produits qui ne fonctionnent pas comme annoncé, par exemple), leur prévalence et leur

gravité peuvent être sensiblement amplifiées dans leur version en ligne.

Une étude de l'OCDE menée en 2021 dans 13 pays a montré qu'en moyenne, 50 % des consommateurs en ligne ont été confrontés à au moins un problème dans l'année qui a précédé, notamment à des pratiques commerciales trompeuses ou frauduleuses, à des escroqueries et à de la fraude.¹

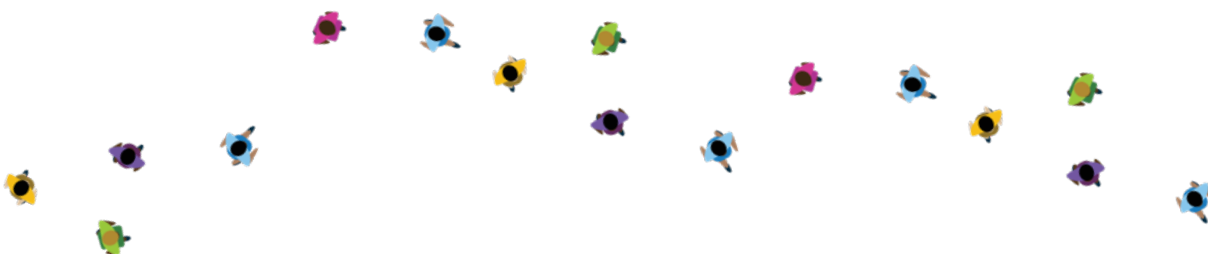
En n'englobant que les problèmes les plus graves et en tenant compte des réparations obtenues, on estime à 22 milliards USD en 2020 les pertes subies par les consommateurs dans les pays de l'OCDE, les pertes de certains pays totalisant 3 % du total des ventes de l'année en commerce électronique.¹ En prenant en compte le stress émotionnel, mais aussi le temps passé à résoudre le problème (cinq heures en moyenne), on atteint 15 milliards USD de pertes supplémentaires en termes monétaires.

Graphique 1. **Fréquence des problèmes liés aux transactions en ligne (2020)**



Note : Résultats basés sur une étude menée en février et juin 2021 dans 13 pays : Allemagne, Australie, Canada, Chili, Corée, États-Unis, Israël, Italie, Japon, Mexique, Norvège, Singapour et République de Türkiye.

Source : OCDE (2022), « Measuring financial consumer detriment in e-commerce », Documents de travail de l'OCDE sur l'économie numérique, n° 326, Éditions OCDE, Paris, <https://doi.org/10.1787/4055c40e-en>.



¹ OCDE (2022), « Measuring financial consumer detriment in e-commerce », Documents de travail de l'OCDE sur l'économie numérique, n° 326, Éditions OCDE, Paris, <https://doi.org/10.1787/4055c40e-en>.

Les modèles économiques numériques peuvent également accentuer les asymétries d'information et de pouvoir, ce qui favorise l'émergence de pratiques susceptibles de tromper et d'exploiter les consommateurs et, ce faisant, de réduire leurs choix et de saper leur confiance dans les marchés. Plus spécifiquement, les entreprises peuvent plus aisément se fonder sur les schémas comportementaux des consommateurs en ligne pour concevoir des interfaces numériques susceptibles de nuire à ces derniers.² La collecte intrusive de données à partir de l'interaction des consommateurs avec des services et des produits numériques, notamment par le biais d'expériences répétées (connues sous le nom de « test A/B »), permet aux entreprises non seulement de suivre et de profiler les consommateurs de manière invasive, avec les risques d'atteinte à la vie privée qui en résultent, mais aussi d'exploiter avec plus de précision leurs biais. Il est alarmant de constater à quel point les techniques de manipulation, de coercition, de tromperie ou de conception addictive bien rodées, connues sous le nom « dark commercial patterns » ou interfaces commerciales truquées, sont répandues.³ Une étude de l'OCDE de 2024 portant sur 20 pays a montré que 9 consommateurs sur 10 ont déjà rencontré une interface truquée sur un site web ou une application.⁴



² OCDE (2023), « Consumer vulnerability in the digital age », Documents de travail de l'OCDE sur l'économie numérique, n° 355, Éditions OCDE, Paris, <https://doi.org/10.1787/4d013cc5-en>.

³ OCDE (2022), « Dark commercial patterns », Documents de travail de l'OCDE sur l'économie numérique, n° 336, Éditions OCDE, Paris, <https://doi.org/10.1787/44f5e846-en>. Le Comité de la politique à l'égard des consommateurs (CPC) de l'OCDE a proposé une définition pratique « dark patterns » ou interfaces truquées, qui vise à faciliter les discussions à court terme à ce sujet entre les pays ou territoires : « Les interfaces commerciales truquées sont des pratiques commerciales faisant intervenir, en particulier dans les interfaces utilisateur en ligne, des éléments d'architecture de choix numérique qui perturbent ou réduisent l'autonomie, le pouvoir décisionnel ou les choix des consommateurs. Elles sont souvent de nature à tromper les consommateurs, à les forcer à faire une action ou à les manipuler et sont susceptibles de leur causer des préjudices directs ou indirects de diverses façons, quoique ces préjudices soient dans bien des cas difficiles ou impossibles à mesurer. »

⁴ OCDE (à paraître), *Etude empirique des interfaces truquées*, Éditions OCDE, Paris.

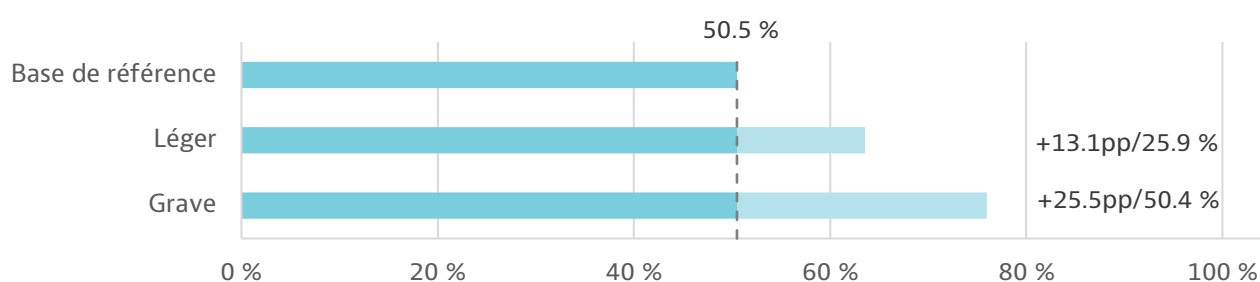


En 2024, une investigation surprise (étude coordonnée de sites web) menée par le Réseau international de contrôle et de protection des consommateurs (RICPC) auprès de 642 entreprises dans 26 pays a révélé que 75 % d'entre elles ont utilisé au moins une interface truquée dans la commercialisation de leurs services d'abonnement.⁵

De même, selon une autre investigation surprise menée en 2024 sur 1 010 sites web et applications par 26 autorités chargées de protéger la vie privée et rassemblées au sein du Global Privacy Enforcement Network (GPEN), la majorité de ces sites web et applications a utilisé des interfaces truquées

intrusives.⁶ Les preuves à l'appui de l'efficacité et des préjudices de vaste portée de ces pratiques sont nombreuses. Par exemple, les expériences en ligne menées dans le cadre de la même enquête de l'OCDE indiquent que les interfaces truquées pourraient influencer la prise de décision des consommateurs de façon significative, et par effet de cumul, produire des conséquences financières importantes, entraîner la divulgation de données personnelles, générer du stress émotionnel et induire des pertes de temps. Tous les consommateurs, quel que soit leur milieu sociodémographique, ont été identifiés comme potentiellement vulnérables et certains, comme les plus âgés ou ceux qui n'utilisent internet que rarement, sont plus à même d'être influencés par certaines interfaces truquées.⁷

Graphique 2. Impact d'interfaces truquées faisant intervenir des techniques d'obstruction pour entraver l'annulation d'abonnements dans les expériences de l'OCDE



Note : dans les expériences de l'OCDE, les participants ont été informés qu'il avaient été abonnés à un service de streaming avec période d'essai gratuite. Ceux qui ont tenté d'annuler l'abonnement ont été confrontés à deux invites truquées (étiquetées en tant que « obstruction faible ») : une question piège pour confirmer l'annulation et une offre de remise. Lorsqu'ils ont choisi de poursuivre, ils ont dû alors faire face à deux autres invites truquées (quatre au total, étiquetées en tant que « obstruction forte ») : une proposant un rappel à l'issue de la période d'essai, et une autre exigeant l'envoi d'un formulaire d'annulation. L'augmentation de l'acceptation de l'abonnement par rapport à un groupe témoin résultant de l'obstruction est indiquée, en termes de points de pourcentage (« pp ») et de différences relatives en pourcentage. Les résultats présentés étaient statistiquement significatifs à l'ordre de 0,1 %.

Source : OCDE (à paraître), *Etude empirique des interfaces truquées*, Éditions OCDE, Paris.

⁵ RICPC (Réseau international de contrôle et de protection des consommateurs), Dark Patterns in Subscription Services Sweep Public Report, 2024, <https://icpen.org/news/1360>

⁶ GPEN (Global Privacy Enforcement Network), GPEN Sweep 2024: Deceptive Design Patterns, 2024, <https://www.privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns>.

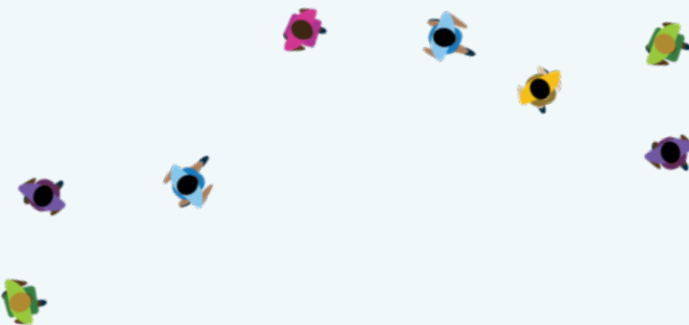
⁷ OCDE (à paraître), *Etude empirique des interfaces truquées*, Éditions OCDE, Paris.

DONNÉES PROBANTES EMPIRIQUES DE L'OCDE SUR LES INTERFACES COMMERCIALES TRUQUÉES

En 2024, l'OCDE a mené une enquête en ligne comprenant des expériences comportementales, auprès de plus de 35 000 personnes, dans 20 pays différents (18 membres de l'OCDE et deux membres de l'ASEAN)⁸, afin d'examiner les impacts des **interfaces truquées**. Il est difficile d'évaluer de façon certaine dans quelle mesure les résultats reflètent la réalité, mais les expériences ont été **conçues avec soin de sorte à inciter les consommateurs à dévoiler leurs véritables comportements**, dans les limites de l'environnement de l'enquête en ligne⁹. Dans un ensemble d'expériences, les personnes interrogées ont indiqué avoir été abonnées à un nouveau service de streaming vidéo, fictif mais présenté comme réel, avec comme seules possibilités de créer un compte (et donc d'accepter l'abonnement) ou d'annuler l'abonnement. Les premières conclusions relatives à certaines interfaces truquées (soulignées) sont les suivantes :

- Hierarchisation factice : 72.9 % des personnes interrogées ont accepté l'abonnement lorsque cette option était plus visible que celle permettant de l'annuler. Ce chiffre tombe à 47.4 % lorsque les deux options étaient de taille équivalente, ce qui correspond à une **augmentation de 25.5 points de pourcentage (pp), ou de 54 % en valeur relative**.

- Autres pratiques d'obstruction et de harcèlement : 87.9 % des personnes interrogées ont fini par accepter lorsque, de surcroît, une série d'invites truquées a constitué un obstacle à l'annulation et que des fenêtres contextuelles les ont harcelées pour qu'elles acceptent. Cette proportion est de 46.7 % quand il n'a été recouru à aucun de ces trois procédés (hiérarchisation factice, obstruction, harcèlement), ce qui représente une **augmentation de 41.2 pp (88 %)**.
- Rôle des préférences du consommateur : le taux d'acceptation des personnes interrogées ayant indiqué *ne pas être intéressées* par un nouvel abonnement augmente avec l'exposition à trois ces interfaces truquées (passant de 34.4 % à 83.2 %), de **48.8 pp (142 %)**. Il s'agit d'une **augmentation plus forte** que celle enregistrée parmi les personnes qui ont indiqué *être intéressées* (leur taux d'acceptation passant de 53.34 % à 90.08 %, soit une hausse de 36.7 pp (69 %)).
- Rôle de la capacité à reconnaître les interfaces truquées : chez les personnes interrogées qui n'ont identifié aucune de ces interfaces truquées comme cherchant à influencer leur décision, le taux d'acceptation passe de 46.9 % à 94.3 %, soit une hausse de **47.4 pp ou de 101 %**. Il s'agit d'une **augmentation plus forte** que celle enregistrée parmi les personnes qui en ont reconnu une ou plusieurs (leur taux d'acceptation passant de 46.9 % à 73.9 %, soit une hausse de 27.0 pp ou 57 %).



⁸ Allemagne, Australie, Cambodge, Canada, Colombie, Corée, Danemark, États-Unis, Israël, Italie, Japon, Luxembourg, Mexique, Norvège, Pays-Bas, Pologne, Portugal, Royaume-Uni, Suède et Thaïlande.

⁹ Après les premières questions de l'enquête, il a été demandé aux personnes interrogées d'accéder à un faux site web de commerce électronique vendant des téléviseurs, similaire à un vrai site web de leur pays mais dont les noms de marque avaient été modifiés, puis de sélectionner une télévision et de passer en caisse comme à l'accoutumée (mais sans que l'achat soit réellement effectué). Après paiement, on les a informés qu'elles étaient redirigées vers un message émanant des partenaires du site web et soudain, une fenêtre contextuelle s'est affichée, leur indiquant qu'elles avaient été abonnées à un nouveau service de streaming vidéo (fictif, mais présenté comme réel) sur le point d'être lancé dans leur pays, avec une période d'essai gratuite de trois mois. La conception de fenêtre contextuelle la rendait crédible (bien que les personnes interrogées aient été informées par la suite que le service n'était pas réel).

Dans d'autres expériences, les personnes interrogées ont été invitées à naviguer sur un faux site web marchand et à y acheter une télévision comme elles le feraient normalement (mais sans que l'achat soit réellement effectué). Les premières conclusions sont les suivantes :

- Urgence et tarification de référence : 13.1 % des personnes interrogées ont acheté une télévision haut de gamme donnée lorsqu'un faux minuteur affiché à côté indiquait que le prix était remisé par rapport à un prix de référence plus élevé. Ce chiffre passe à 8.7 % lorsque les personnes n'ont pas été exposées à cette technique, ce qui correspond à une **augmentation de 4.4 pp (51 %)**.
- Harcèlement : 24 % des personnes interrogées ont également acheté une fixation murale lorsqu'elles ont été harcelées à cette fin par des fenêtres contextuelles. Ce chiffre passe à 12.8 % lorsque les personnes n'ont pas été exposées aux fenêtres contextuelles, ce qui correspond à une **augmentation de 12.2 pp (95 %)**.

L'IA et d'autres technologies numériques peuvent être à l'origine de risques nouveaux ou amplifier des risques existants pour les consommateurs et leur porter préjudice. Par exemple, les entreprises ont de plus en plus de facilités pour exploiter l'IA et les données des consommateurs afin de cibler par la publicité ou la tarification les vulnérabilités individuelles des consommateurs, et potentiellement générer des achats non souhaités ou du stress psychologique.¹⁰ L'IA risque d'exacerber les biais à l'encontre de certains groupes de consommateurs (définis par exemple par genre ou origine ethnique), qui reçoivent ainsi de la publicité ou des services à des conditions moins favorables ou sont exclus de ces offres.¹¹ Des acteurs frauduleux peuvent exploiter l'IA dans le but de réaliser des escroqueries de plus en plus sophistiquées, y compris au moyen d'hypertrucages.¹² Enfin, les technologies immersives, telles que la réalité virtuelle, leur offrent un moyen de tirer profit de l'immersion des utilisateurs dans des environnements inconnus, tels que les jeux vidéo.¹³

- Divulgateur forcé : 58 % des personnes ont effectué leur achat même dans les cas où, pour se faire, elles devaient communiquer leurs données personnelles et en accepter l'utilisation à des fins de marketing. Ce chiffre passe à 62.4 % en l'absence de telles contraintes, ce qui correspond à une **baisse d'à peine 4.4 pp (7 %)**.
- Disparités entre comportement déclaré et constaté dans le cadre de l'expérience : les personnes interrogées qui ont indiqué que normalement, elles cesseraient d'utiliser des sites web qui tenteraient de les influencer de façon négative, **n'ont pas moins** concrétisé leur achat que celles qui n'avaient pas fait de déclaration en ce sens.

Ces résultats s'alignent sur des recherches antérieures et soulignent **la nécessité d'une politique des consommateurs rigoureuse en matière d'interfaces truquées et des actions d'application des lois** contre leur utilisation illégale aux niveaux national et mondial.

Certains groupes de consommateurs sont particulièrement exposés au risque de préjudice en ligne. Les enfants, et notamment les adolescents, qui sont parmi les premiers à adopter les technologies numériques, ne disposent pas des aptitudes de réflexion essentielles pour gérer les risques numériques, tels que l'addiction aux médias sociaux, le brouillage par le marketing de la frontière entre publicité et autres contenus, le ciblage par la publicité et l'exposition à des produits non appropriés pour leur âge. En même temps, les tendances ci-dessus illustrent la façon dont, en ligne, quasiment tous les consommateurs sont, à certains moments, victimes de préjudices ou susceptibles de l'être.¹³ Des chercheurs ont ainsi caractérisé la vulnérabilité des consommateurs dans l'environnement numérique comme étant universelle ou systémique.¹⁴ Une grande partie des travaux, y compris de l'OCDE, a déjà permis de comprendre les dommages subis par les consommateurs en ligne, mais il convient de poursuivre la recherche sur les nouveaux préjudices auxquels ils sont exposés, surtout dans ce contexte

¹⁰ OCDE (2023), « Consumer vulnerability in the digital age », *Documents de travail de l'OCDE sur l'économie numérique*, n° 355, Éditions OCDE, Paris, <https://doi.org/10.1787/4d013cc5-en>.

¹¹ Pour d'autres exemples, voir aussi OCDE (2023), « Consumer vulnerability in the digital age », *Documents de travail de l'OCDE sur l'économie numérique*, n° 355, Éditions OCDE, Paris, <https://doi.org/10.1787/4d013cc5-en>.

¹² Hyde, R. et P. Cartwright (2023), « Exploring Consumer Detriment in Immersive Gaming Technologies », *Journal of Consumer Policy*, Vol. 46/3, pp. 335-361, <https://doi.org/10.1007/s10603-023-09544-9>.

¹³ OCDE (2023), « Consumer vulnerability in the digital age », *Documents de travail de l'OCDE sur l'économie numérique*, n° 355, Éditions OCDE, Paris, <https://doi.org/10.1787/4d013cc5-en>.

¹⁴ Ibid. Voir aussi Helberger, N. et al. (2021), « Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability », *Journal of Consumer Policy* 2021, pp. 1-26, <https://doi.org/10.1007/S10603-021-09500-5> et Riefa, C. (2022), « Protecting Vulnerable Consumers in the Digital Single Market », *European Business Law Review*, Vol. 33/Issue 4, pp. 607-634, <https://doi.org/10.54648/eulr2022028>.

d'évolution rapide des technologies. Cela souligne le rôle important de l'OCDE et d'autres parties prenantes, qui doivent approfondir les recherches

empiriques en intégrant les éclairages comportementaux afin d'élargir la base factuelle à l'appui de l'action publique et de sa mise en œuvre.

PROTÉGER LES CONSOMMATEURS AVEC DES MESURES ET DES OUTILS EXISTANTS ET INÉDITS

La mise en place d'un cadre d'action solide et efficace permet aux consommateurs de faire confiance aux marchés numériques.

De nombreux pays et territoires ont adopté des lois visant à lutter contre les risques rencontrés par les consommateurs dans l'environnement numérique, particulièrement l'interdiction des pratiques trompeuses, frauduleuses et déloyales, conformément à la *Recommandation de l'OCDE sur la protection du consommateur dans le contexte du commerce électronique* (2016).¹⁵ Comme le démontre l'OCDE, plusieurs actions coercitives visant à faire appliquer ces lois ont été engagées contre les interfaces truquées et les pratiques préjudiciables, telles que les techniques de marketing et les pratiques trompeuses et déloyales en matière de données, les faux avis et les fausses évaluations.¹⁶

Les autorités chargées de la protection des consommateurs se sont également perfectionnées en technologies numériques pour tenir le rythme de leur utilisation de plus en plus répandue par les entreprises. Certaines expérimentent des outils numériques susceptibles de les aider à détecter les interfaces truquées, les clauses contractuelles abusives, les faux avis, les produits dangereux et d'autres violations du droit de la consommation.¹⁷ Selon certains universitaires, l'IA pourrait améliorer l'élaboration des politiques publiques en matière de consommation, notamment grâce à l'identification des biais des consommateurs, à des actions

publiques plus ciblées et à une amélioration de l'analyse des données et des travaux de recherche sur les consommateurs.¹⁸

Néanmoins, on peut se demander si les lois et les mécanismes d'application en vigueur sont suffisamment efficaces et en mesure de résoudre les problèmes. Par exemple, il est de plus en plus admis que les informations en ligne seules ne suffisent pas pour informer et donner aux consommateurs les moyens d'agir dans bon nombre de situations.¹⁹ Les expériences menées par l'OCDE en Irlande et au Chili en 2019 et 2020 ont notamment montré la capacité limitée des consommateurs à repérer la communication d'informations sur la tarification personnalisée.²⁰ La complexité et l'opacité des modèles économiques numériques continuent également de poser problème aux autorités chargées de la réglementation qui peuvent avoir des lacunes en technologie numérique ou ne pas avoir accès aux données expérimentales des entreprises et aux résultats de leurs algorithmes, et par conséquent manquer de connaissances sur la portée totale des préjudices.

À cet égard, de nouvelles mesures sont actuellement introduites dans différents pays ou territoires afin de mieux lutter contre les préjudices numériques, nouveaux et existants. Il s'agit entre autres de restrictions légales, imposées notamment aux interfaces truquées (par exemple, la législation de l'UE sur les services numériques et celle sur les marchés numériques, la loi du Royaume-Uni sur les

¹⁵ OCDE (2016), *Recommandation du conseil sur la protection du consommateur dans le commerce électronique*, Éditions OCDE, Paris, <https://doi.org/10.1787/9789264255272-fr>.

¹⁶ OCDE (2019), « Good practice guide on consumer data », *Documents de travail de l'OCDE sur l'économie numérique*, n° 290, Éditions OCDE, Paris, <https://dx.doi.org/10.1787/e0040128-en>; OCDE (2019), « Good practice guide on online advertising: Protecting consumers in e-commerce », *Documents de travail de l'OCDE sur l'économie numérique*, n° 279, Éditions OCDE, Paris, <https://dx.doi.org/10.1787/9678e5b1-en>; OCDE (2019), « Good practice guide on online consumer ratings and reviews », *Documents de travail de l'OCDE sur l'économie numérique*, n° 288, Éditions OCDE, Paris, <https://dx.doi.org/10.1787/0f9362cf-en>.

¹⁷ Riefa, C. et L. Coll (2024), *The transformative potential of Enforcement Technology (EnfTech) in Consumer Law*, <https://www.enftech.org/>.

¹⁸ Mills, S., S. Costa et C. Sunstein (2023), « AI, Behavioural Science, and Consumer Welfare », *Journal of Consumer Policy*, <https://doi.org/10.1007/s10603-023-09547-6>.

¹⁹ OCDE (2022), « Enhancing online disclosure effectiveness », *Documents de travail de l'OCDE sur l'économie numérique*, n° 335, Éditions OCDE, Paris, <https://doi.org/10.1787/6d7ea79c-en>.

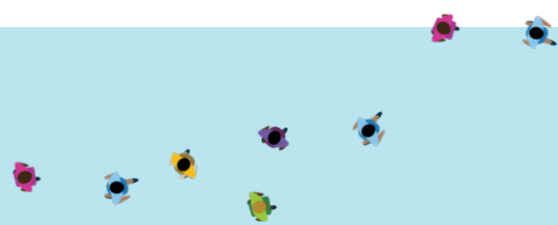
²⁰ OCDE (2021), « The effects of online disclosure about personalised pricing on consumers: Results from a lab experiment in Ireland and Chile », *Documents de travail de l'OCDE sur l'économie numérique*, n° 303, Éditions OCDE, Paris, <https://dx.doi.org/10.1787/1ce1de63-en>.

marchés numériques, la concurrence et les consommateurs, la loi coréenne mise à jour sur la protection du consommateur dans le commerce électronique, ou les lignes directrices indiennes pour la prévention et la réglementation des interfaces truquées) ou à l'IA (par exemple, la loi sur l'intelligence artificielle de l'UE), ainsi que d'engagements, de normes et de principes adoptés volontairement par les entreprises. La société civile joue également un rôle important, comme l'illustrent les campagnes menées par les organisations de consommateurs contre les interfaces truquées, le suivi des consommateurs et les coffres à butin (loot box)²¹.

Enfin, étant donné que les marchés numériques existent par-delà les frontières, la coopération internationale est capitale. De même, les risques

auxquels sont exposés les consommateurs en ligne existant de plus en plus dans tous les domaines d'action, une coopération interdisciplinaire renforcée permettrait de mieux les contrer²². Par exemple, les interfaces truquées, le suivi des consommateurs et la personnalisation subversive portent atteinte à la vie privée en raison de la collecte trompeuse de données personnelles, et affaiblissent la concurrence, en empêchant le passage d'un service à un autre et en compromettant l'égalité des conditions de concurrence. Par conséquent, plusieurs pays ou territoires ont institué des forums visant à renforcer la coopération entre les autorités chargées de la réglementation dans les domaines de la consommation, de la concurrence et de la protection des données et autres autorités de réglementation du monde numérique²³.

QUESTIONS À EXAMINER



1 Quels sont les principaux défis et opportunités auxquels sont confrontés les consommateurs en ligne aujourd'hui ? Comment les avantages se comparent-ils aux inconvénients ?

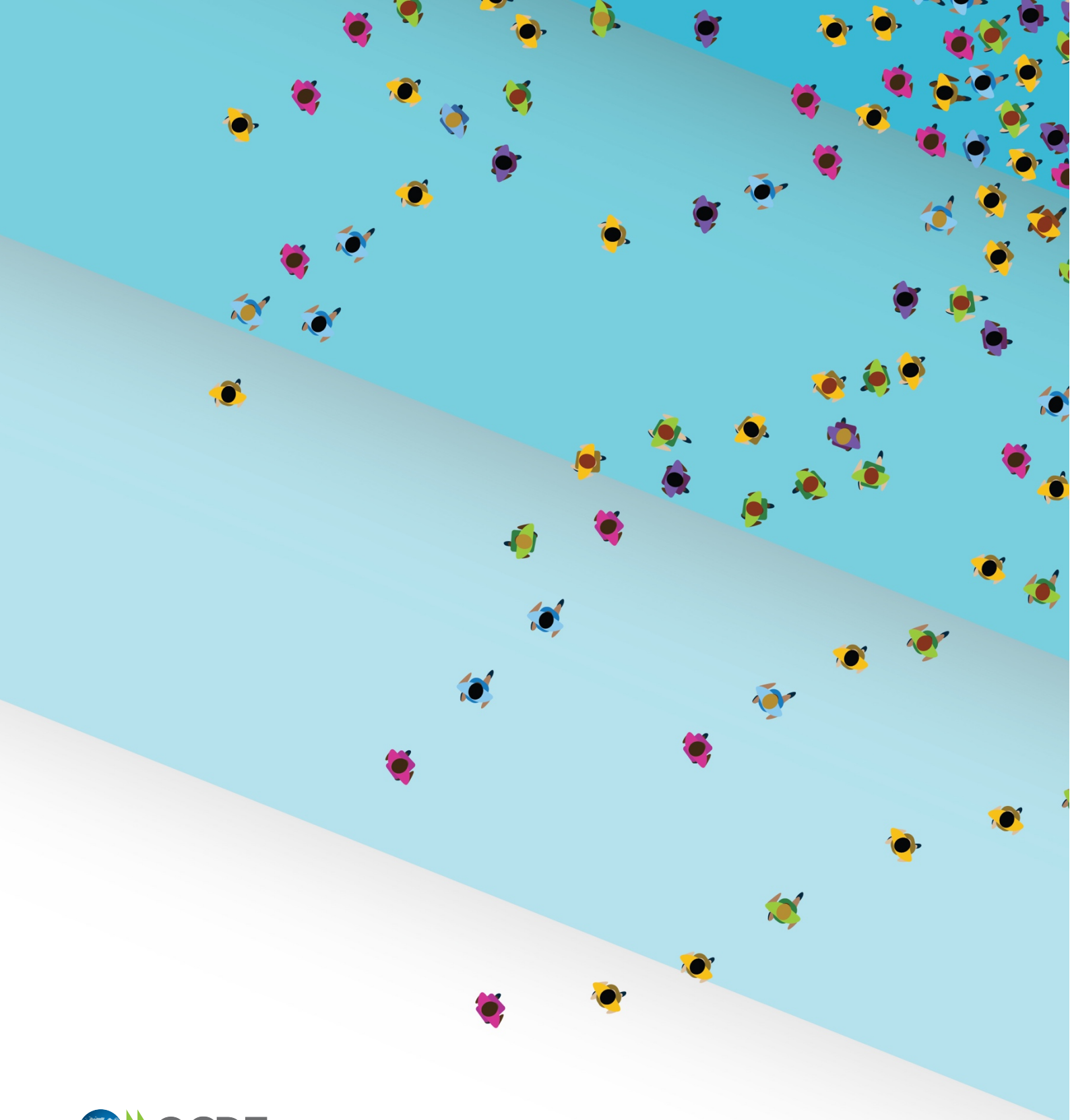
2 Que font les responsables de l'élaboration des politiques en matière de consommation et les acteurs chargés de leur mise en œuvre pour résoudre les problèmes ? Que peuvent-ils accomplir de plus ? Comment peuvent-ils collaborer avec leurs homologues dans d'autres domaines d'action publique et les parties prenantes pour résoudre les problèmes ?

3 Quelles autres recherches, y compris menées par l'OCDE, pourraient aider à mieux appréhender les problématiques liées aux consommateurs du numérique ?

²¹ Voir par exemple les campagnes menées par le Conseil norvégien des consommateurs concernant les interfaces truquées, le suivi et le ciblage par la publicité, et les coffres à butin (définis comme des « paquets mystères » de contenu numérique dans les jeux vidéo que les consommateurs achètent avec de l'argent réel).

²² OCDE (2023), *Applying Behavioural Insights to Consumer and Competition Policy and Enforcement - Workshop issues paper*, [DSTI/CP(2023)6].

²³ Par exemple, le Digital Platform Regulators Forum en Australie, le Forum canadien des organismes de réglementation numérique, la Digital Regulation Cooperation Platform néerlandaise et le Digital Regulation Cooperation Forum (DRCF) au Royaume-Uni. Le DRCF a également lancé l'INDRC (International Network for Digital Regulation Cooperation, réseau international pour la coopération en matière de réglementation numérique) en juin 2023 afin d'établir des relations entre les organismes de réglementation du monde entier afin d'accroître la coopération nationale sur leur territoire.



 <https://oe.cd/consommateur24>

 ccpministerial2024@oecd.org

 OECD - OECD

 @OECD

 @OECD_STI