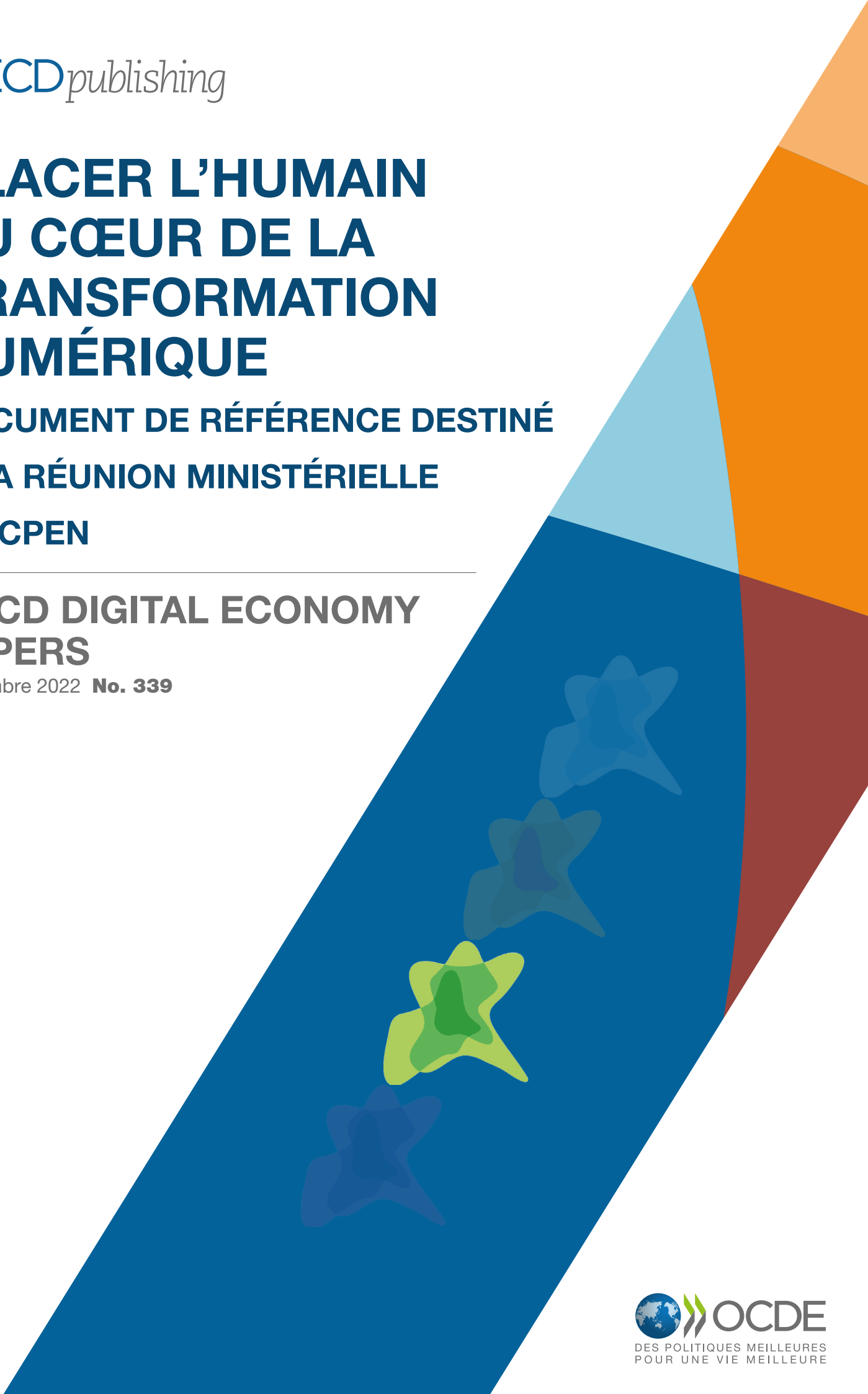
OECD publishing

PLACER L'HUMAIN AU CŒUR DE LA TRANSFORMATION NUMÉRIQUE

DOCUMENT DE RÉFÉRENCE DESTINÉ À LA RÉUNION MINISTÉRIELLE DU CPEN

OECD DIGITAL ECONOMY PAPERS
Novembre 2022 **No. 339**



OCDE
DES POLITIQUES MEILLEURES POUR UNE VIE MEILLEURE

Avant-propos

Le présent document donne à voir comment la transformation numérique nous touche individuellement, que ce soit en tant que citoyens, consommateurs ou travailleurs. Nous y trouverons une présentation sommaire de l'environnement réglementaire ainsi qu'une description des efforts internationaux, multipartites et nuancés nécessaires pour parvenir à concilier des droits, intérêts et valeurs différents.

Ce document apporte des éléments d'information destinés à nourrir les débats qui seront menés au titre du thème 3, « Placer l'humain au cœur de la transformation numérique », lors de la Réunion ministérielle du Comité de la politique de l'économie numérique qui se tiendra les 14 et 15 décembre 2022 à la Grande Canarie, en Espagne. Il vise à étayer les sessions de la Réunion ministérielle consacrées aux thèmes : « Les droits à l'ère numérique – bâtir une base factuelle solide (atelier) », « Créer un environnement numérique plus sûr (atelier) » et « Autonomiser les consommateurs dans un monde numérique ».

Le présent document a été rédigé par Nora Beauvais, Giuseppe Bianco, Kosuke Kizawa, Nicholas McSpedden-Brown et Lisa Robinson, sous la supervision d'Audrey Plonk, Cheffe de la Division de la politique de l'économie numérique de l'OCDE. Il a bénéficié de la contribution de Brigitte Acoca, Gallia Daor, Clarisse Girot, Molly Lesher, Adam Mollerup, Vincenzo Spiezia, Verena Weber et Jeremy West ; Angela Gosmann, Sebastian Ordelheide et Misha Pinkhasov ont apporté un appui rédactionnel. La Réunion ministérielle et les travaux connexes bénéficient du généreux soutien du gouvernement espagnol.

Le présent document a été approuvé et déclassifié selon la procédure écrite par le Comité de la politique de l'économie numérique le 26 octobre 2022 et le Secrétariat de l'OCDE en a établi le texte à publier.

Note à l'intention des délégations :

Ce document est également disponible sur O.N.E sous la cote :

DSTI/CDEP(2022)13/FINAL

Table des matières

Graphiques

Encadrés

Résumé

La transformation numérique offre aux individus une multitude de possibilités, dans le champ économique et social, à exploiter en tant que citoyens, consommateurs et travailleurs. Les technologies numériques transforment la vie de milliards de personnes en mettant à leur disposition de nouveaux espaces et de nouveaux outils pour communiquer, travailler, consommer, participer à la vie économique et aux débats publics, exercer leurs droits et jouir de leurs libertés. Placer l'humain au cœur de la transformation numérique implique nécessairement la création d'un environnement en ligne qui soit à la fois émancipateur et sûr.

Aux consommateurs, les technologies numériques offrent des produits et des services sur mesure, un accès aisé aux places de marchés en ligne, un plus large choix et des prix compétitifs, ainsi que des logements connectés. Pour autant, le risque existe de tomber victime d'escroqueries et de fraudes en ligne, d'acheter des produits dangereux, d'être dupé, exploité ou discriminé.

Les travailleurs ont accès à de nouvelles perspectives d'emploi, promettant davantage de flexibilité, au travail par l'intermédiaire de plateformes et à des outils pratiques. Ils peuvent toutefois pâtir de conditions de travail difficiles, d'une gestion décentralisée ou de biais algorithmiques.

Grâce aux technologies numériques, les individus ont désormais accès à de nombreuses possibilités pour nouer des relations, se détendre, apprendre ou participer à la vie publique. Mais ils peuvent aussi se trouver face à des contenus illicites et préjudiciables, voir leur vie privée attaquée ou être victimes de discrimination, d'inégalités ou d'atteintes à la sécurité.

Le cadre d'action dans lequel s'inscrit l'environnement numérique exige des efforts internationaux, multipartites et nuancés pour concilier droits, intérêts et valeurs. Les responsables de la formulation des politiques et les autorités chargées de leur application prêtent une attention de plus en plus grande à la protection, à l'autonomisation, à la sécurité et aux droits, mais ils ont besoin d'outils pour mener ces efforts à bien. Des mesures non contraignantes doivent impérativement être mises en œuvre en complément de la réglementation et de son application, et peuvent prendre la forme, par exemple, d'engagements volontaires, de normes éthiques, d'une prise en compte de certaines exigences dès le stade de la conception, de dispositions techniques et de campagnes d'information et de sensibilisation. Il conviendrait que les lois et politiques tiennent compte des interdépendances qui existent dans l'environnement numérique et reposent sur des éléments factuels pour permettre de combler les lacunes de l'action publique et apporter des réponses appropriées.

Placer l'humain au cœur de la transformation numérique est plus qu'un slogan ou un vœu pieux – c'est l'énoncé des objectifs fondamentaux de l'ère numérique.

Placer l'humain au cœur de la transformation numérique : document de référence destiné à la Réunion ministérielle du CPEN

Les technologies numériques sont intrinsèquement liées à la vie quotidienne...

La transformation numérique offre aux individus des bienfaits d'ordre sociologique, à exploiter en tant que citoyens, consommateurs et travailleurs. Les avancées technologiques et les nouveaux modèles économiques ont remodelé le quotidien de milliards de personnes, ouvrant de nouvelles sphères publiques et de nouveaux marchés de biens et de services. La messagerie instantanée, le partage de contenus, les courses en ligne, les objets connectés et les paiements au moyen de dispositifs intelligents ouvrent de nouvelles possibilités aux individus pour communiquer, travailler, consommer, apprendre et créer, participer à la vie démocratique et économique et exercer et jouir de leurs droits à l'ère numérique.

Qu'est-ce que cela signifie concrètement ? Prenons le cas de la famille d'Antonio, 45 ans, enseignant et père de deux enfants. Lui et sa compagne, Yoko, peuvent communiquer à tout moment avec leurs proches et amis partout dans le monde. Dans leurs discussions en ligne avec les membres de leur famille, ils échangent des nouvelles, des mèmes, des vidéos de chats et des photos de leurs enfants et de leurs vacances. Antonio est convaincu que cela permet d'entretenir le lien familial, surtout depuis que ses parents vivent loin. Écologiste militante, Yoko utilise régulièrement l'internet pour s'informer et aime débattre des enjeux environnementaux sur les réseaux sociaux, où elle diffuse articles et idées auprès de communautés virtuelles. Grâce à l'un de ces groupes, elle a repris contact dernièrement avec d'anciens amis du lycée qu'elle avait perdus de vue.

Antonio n'est pas un inconditionnel des réseaux sociaux et ne comprend d'ailleurs pas toujours quel intérêt on peut trouver aux vlogues, tweets ou les flux (« streams »). Les smartphones n'en sont pas moins un outil pratique pour garder un œil sur les enfants, Tom (14 ans) et Ana (11 ans), qui fréquentent les réseaux sociaux, quand bien même Antonio et Yoko avaient quelques craintes à l'idée qu'Ana ait son propre compte à son âge. Ils peuvent apparemment rester rivés à leur écran pendant des heures – ce qui est beaucoup trop au goût d'Antonio. Tom passe le plus clair de son temps à jouer aux jeux vidéo avec des amis rencontrés en ligne – dont certains qu'il n'a jamais rencontrés en personne. Il aime aussi beaucoup créer des bandes dessinées sur sa tablette. Quant à Ana, elle regarde des dessins animés ou communique avec des amis sur les réseaux sociaux – quand elle ne fait pas les deux en même temps. Antonio dit que ses enfants ont considérablement progressé en français grâce à une nouvelle application interactive. Ils ont accès à une telle quantité de ressources éducatives, de connaissances et d'informations ! Pendant les

périodes de confinement, Antonio, à l'instar de nombreux enseignants, a utilisé des plateformes d'enseignement en ligne, grâce auxquelles il a pu mieux cerner les besoins de ses élèves. L'un d'entre eux n'ayant pas d'accès à l'internet chez lui, Antonio, ses collègues et d'autres élèves se sont cotisés pour qu'il puisse avoir une tablette disposant d'une connexion mobile.

La transformation numérique a apporté de la souplesse dans la vie professionnelle des membres de la famille. Pour arrondir ses fins de mois, Ken, le frère de Yoko, a été chauffeur pour un service de covoiturage lorsqu'il était à l'université. Ce père célibataire pouvait ainsi décider où et quand travailler en fonction de son emploi du temps d'étudiant. Après avoir quitté l'université, il a continué de transporter des passagers de temps à autre pour compléter ses revenus. Ken a ainsi travaillé pour de multiples plateformes et, même s'il ignorait tout des moyens technologiques mis en œuvre, pouvait demander le transfert des évaluations le concernant entre ces plateformes (« portabilité des données de réputation »). De ce fait, il ne se sentait pas lié exclusivement à une seule plateforme pour conserver les bonnes appréciations reçues.

Ken fait partie de ceux, ils sont nombreux, qui auraient peut-être eu du mal à joindre les deux bouts s'ils n'avaient trouvé à gagner de l'argent en accomplissant un travail par l'intermédiaire des plateformes numériques, ce qui comprend « toute activité de production de biens ou de prestation de services que les individus exercent à travers une plateforme numérique ou directement sur celle-ci » (OCDE, 2022[1]). Il peut s'agir de l'activité professionnelle principale d'un individu ou d'une activité annexe, à caractère occasionnel, apportant un revenu d'appoint (dans le cas par exemple d'étudiants, de personnes venant de perdre leur emploi ou de jeunes retraités).

... mais gare à leurs inconvénients.

La situation n'était pas idéale pour autant. C'est à Ken qu'incombait la responsabilité d'entretenir sa voiture et de s'assurer qu'il avait la formation nécessaire pour être autorisé à exercer son activité. Lorsque le COVID-19 a fait son apparition, il s'est inquiété pour sa santé, lui qui côtoyait beaucoup de monde, sachant d'autre part qu'il ne pourrait plus travailler ni être payé s'il venait à tomber malade. Le manque de visibilité financière lui était pénible aussi. Il ne savait jamais combien il allait gagner, et il lui arrivait parfois de perdre de l'argent parce qu'un passager refusait de le payer ou contestait la somme due. Une plateforme a un jour désactivé son compte sans préavis ni explication. En l'absence de mécanismes simples de règlement des différends, Ken s'est senti démuni, sans réelle possibilité de faire état de tels problèmes.

Ken s'est aperçu qu'il perdait peu à peu des places au classement après avoir pris plusieurs jours de congé maladie lorsqu'il a contracté le COVID-19. Les systèmes d'algorithmes qui sous-tendent le travail par l'intermédiaire des plateformes peuvent être enclins à la discrimination et présenter certains biais. D'autres exemples similaires ont été signalés : en 2020, un algorithme de classement fondé sur la réputation utilisé par une plateforme de livraison de repas à la demande en Italie pénalisait les travailleurs absents, que le motif de leur absence soit futile ou légitime (grève ou congé maladie, par exemple). Cette pratique a été jugée contraire à la législation en vigueur (Tribunal of Bologna, 2020[2]).

Les technologies numériques permettent de donner davantage d'autonomie aux citoyens...

Les technologies et données numériques transforment les relations entre les citoyens et les pouvoirs publics, en leur fournissant de nouveaux moyens de participer à la vie démocratique et de s'impliquer dans la société civile. L'administration numérique crée les conditions d'ouverture et de participation du public nécessaires pour que les citoyens puissent prendre part à la conception, à la formulation, à la mise en place et au suivi des politiques et services

publics. Dans cette logique, certains pays adoptent une approche de l'administration numérique privilégiant la téléphonie mobile. Les technologies numériques sont aussi en train de transformer les modes de fonctionnement des processus et institutions démocratiques, ouvrant de nouvelles perspectives (comme le vote électronique ou le comptage électronique des voix par exemple), mais faisant aussi naître de nouveaux enjeux en termes de protection de la vie privée, d'égalité et de sécurité. Face à ces évolutions, les pouvoirs publics collaborent souvent avec des partenaires du secteur privé pour mettre en place des mesures destinées à favoriser la confiance.

L'arrivée des signatures et systèmes d'identification électroniques fait gagner beaucoup de temps à Antonio et Yoko. Tom, leur fils, utilise les technologies numériques pour s'affirmer en tant que citoyen et s'engager sur des questions politiques. En compagnie de plusieurs de ses amis, il fait partie d'un groupe de jeunes mobilisés en ligne en faveur de l'écologie. Ce n'est là qu'une des nombreuses façons dont la transformation numérique facilite l'engagement citoyen des enfants, leur permettant de se faire entendre et de défendre leurs droits et intérêts, individuellement et collectivement. En même temps, la concentration d'informations sur les activités des citoyens au sein d'un système centralisé n'est pas dénuée de risque, comme celui d'intrusions injustifiées par exemple (ICO, 2021[3]).

… et de proposer des services commerciaux sur mesure...

Antonio, exploitant au maximum les possibilités offertes par le commerce électronique, propose sur une place de marché en ligne des tables en bois rénovées par ses soins. Il effectue également la plupart de ses achats en ligne, suivant en cela la tendance (amplifiée par la pandémie de COVID-19) des consommateurs des pays de l'OCDE : de 36 % en 2010, la proportion des clients du commerce électronique est passée à 64 % en 2020. À l'aide de son smartphone, il saisit des mots-clés dans des moteurs de recherche utilisant des algorithmes et peut ainsi comparer des douzaines d'offres portant sur un large éventail de produits, souvent sur des places de marché en ligne où il peut lire des avis détaillés rédigés par d'autres consommateurs. Les outils de comparaison numériques, les annonces personnalisées et les recommandations l'aident à repérer ce dont il a besoin. Quelquefois, il échange avec sa jeune sœur Maria, qui est en fauteuil roulant et qui peut, d'un seul doigt, commander et recevoir des produits de manière totalement indépendante. Ils effectuent ces transactions facilement, en utilisant des services bancaires et moyens de paiement numériques. Avec la pandémie de COVID-19, Antonio a eu conscience de la chance qu'il avait de pouvoir accéder facilement au marché mondial pendant les confinements, durant lesquels il a intensifié ses achats en ligne, car il savait que certaines personnes n'avaient pas cette possibilité faute d'accès à l'internet.

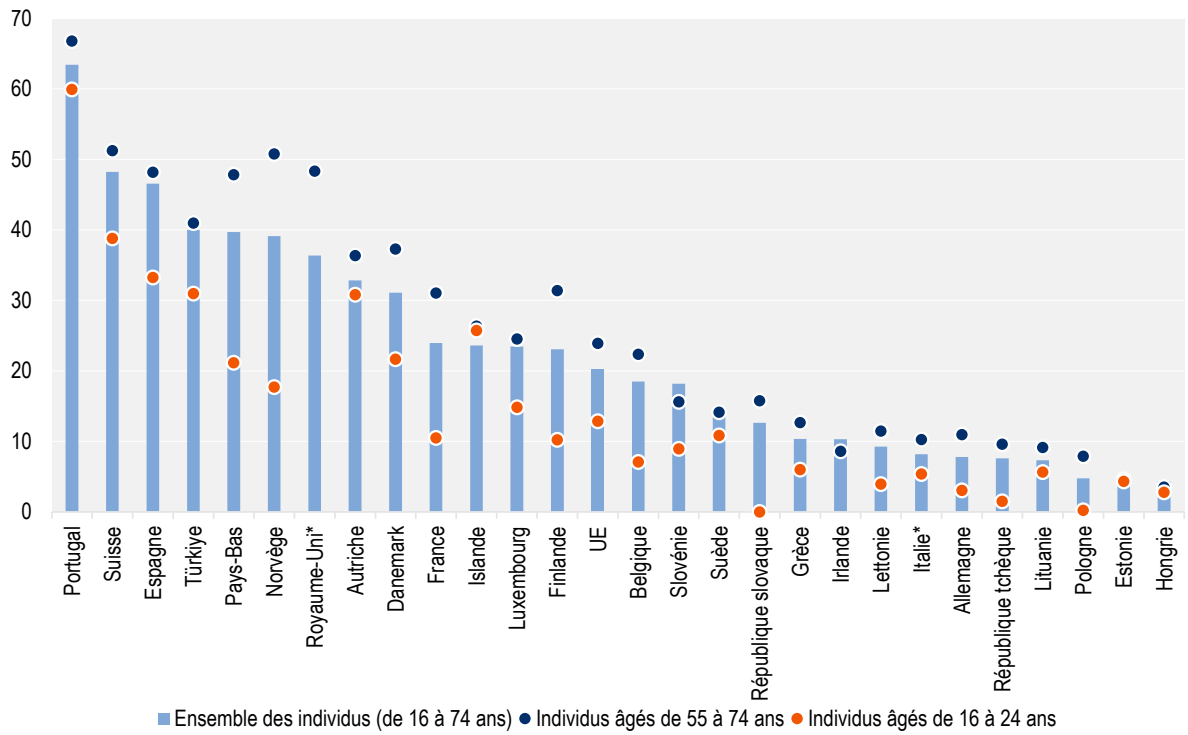
Lorsque Yoko rentre chez elle après le travail, elle s'adresse à son assistant numérique basé sur l'intelligence artificielle (IA) qui se charge d'allumer le chauffage et la lumière, eux-mêmes connectés à l'internet, diffuse de la musique dans toute la maison, l'informe de la météo du lendemain et peut lui réserver un restaurant pour dîner. Grâce aux données qu'il recueille et aux mises à jour à distance en continu, cet assistant a appris à adapter la consommation énergétique du foyer aux besoins de la famille. Il lui propose également des offres plus personnalisées, comme le fait une autre application basée sur les données de transaction de la famille.

… mais les préoccupations relatives aux pratiques commerciales en ligne sont nombreuses.

Cependant, le commerce électronique et les produits de consommation numériques ne sont pas toujours utiles, et la famille a eu certaines expériences négatives en ligne. Pendant la crise liée au COVID-19, Antonio a passé auprès d'un détaillant en ligne apparemment fiable une commande de gel hydroalcoolique qui n'est jamais arrivée : il s'est avéré qu'il s'agissait d'un faux site web utilisant des avis générés par IA et des logos volés pour se donner une apparence de légitimité. Yoko, elle, a commandé des masques qui se sont révélés défectueux et qui auraient pu blesser les enfants. De plus, elle a reçu des appels à venir en aide à des victimes du virus, mais il s'agissait en fait de faux messages et elle a ainsi pris conscience des risques liés à l'hameçonnage et à l'escroquerie financière en ligne. Ces expériences ont conduit Antonio et Yoko à se montrer plus prudents lorsqu'ils effectuent des achats en ligne ou partagent des informations financières ou personnelles. Ils ne sont pas les seuls concernés, puisque les statistiques de l'OCDE montrent que 22.5 % des utilisateurs de l'internet s'abstiennent de faire des achats en ligne par crainte de problèmes liés à la sécurité des paiements ou au respect de la vie privée (graphique 1) (OCDE, s.d.[4]).

Graphique 1. Part des internautes n'effectuant pas d'achats en ligne par crainte de problèmes de sécurité des paiements

% des internautes n'ayant pas effectué d'achats en ligne au cours des trois derniers mois



Note : Sont inclus dans les internautes n'ayant pas commandé de biens ou de services sur l'Internet au cours des trois derniers mois ceux qui n'ont jamais effectué d'achats en ligne. Les dernières données se rapportent à une période de référence de 3 mois précédant l'enquête ; toutefois, certains pays utilisent des périodes différentes et les périodes de référence peuvent varier dans le temps. En 2021, Eurostat a modifié la durée de la période de référence, qui est passée de 12 mois précédant l'enquête à 3 mois. Pour plus d'informations sur les définitions, la qualité des données, les ruptures de séries, etc., veuillez consulter les sources de données sous-jacentes.
Source : Boîte à outils de l'OCDE sur la transformation numérique, d'après Eurostat, base de données Économie et société numériques.

Le commerce électronique soulève un certain nombre de préoccupations. Une étude menée en 2021 par l'OCDE dans 13 pays a montré que 50 % des consommateurs avaient rencontré au moins un problème avec leurs achats en ligne au cours des 12 mois précédant l'enquête. Si l'on considère uniquement les problèmes les plus graves, environ 25 % étaient liés à la crise du COVID-19 (et impliquaient fréquemment des escroqueries), avec un coût total pour les consommateurs des pays de l'OCDE estimé à plus de 22 milliards USD en 2020 (OCDE, 2022[5]). Selon des données préliminaires issues d'une investigation surprise sur la sécurité des produits vendus en ligne menée en 2021 par l'OCDE dans 21 pays, les taux moyens de non-respect des interdictions/rappels de produits, des exigences d'étiquetage et des normes de sécurité n'ont pas progressé depuis l'investigation surprise de 2015 réalisée par l'OCDE sur la sécurité des produits de consommation dans sept catégories (jouets/jeux, appareils électroménagers, appareils ménagers non électriques, articles de sport/loisirs, vêtements/accessoires, articles pour enfants/bébés et technologie mobile) (OCDE, à paraître[6] ; OCDE, 2016[7]).

Certaines pratiques commerciales peuvent affaiblir davantage la confiance...

Yoko s'est récemment inscrite à un service en ligne qui apprend aux enfants à jouer d'un instrument de musique. N'étant pas entièrement satisfaite, elle a décidé d'annuler son inscription, mais elle s'est heurtée à plusieurs difficultés: informations cachées, questions-pièges, nombreuses étapes dans la procédure de résiliation et registre de langage émotionnel visant à la persuader de continuer à utiliser le service. Une période d'essai très courte a débouché sur un abonnement pour une année entière, qui lui a été facturé par défaut. Yoko a été victime de plusieurs « interfaces commerciales truquées » (ci-après « interfaces truquées ») : ce sont des pratiques commerciales faisant intervenir, en particulier dans les interfaces utilisateur en ligne, des éléments d'architecture de choix qui perturbent ou réduisent l'autonomie, le pouvoir décisionnel ou les choix des consommateurs. Comme de nombreux autres consommateurs, Yoko ignorait à quel point ces pratiques sont courantes, mais elle avait entendu parler de mesures prises par la Commission fédérale du commerce (FTC) des États-Unis à l'encontre d'une entreprise en ligne ayant renouvelé automatiquement les abonnements des consommateurs sans leur consentement, suite à quoi l'entreprise avait dû rembourser 9.7 millions USD aux utilisateurs concernés en 2021 (Federal Trade Commission des États-Unis, 2021[8]).

En 2022, l'OCDE a constaté que les interfaces truquées étaient fréquemment utilisées sur les sites web de commerce électronique, les applications (y compris celles des principales plateformes et places de marché en ligne), ainsi que dans les bannières de consentement aux témoins de connexion (cookies), les moteurs de recherche et les jeux (OCDE, 2022[9]). Une étude a identifié au moins une interface truquée dans 95 % de 240 applications populaires (Di Geronimo et al., 2020[10]). Les interfaces truquées sont souvent de nature à tromper les consommateurs, à les forcer à effectuer une action ou à les manipuler, et sont susceptibles de leur causer des préjudices directs ou indirects, quoique cela puisse être difficile ou impossible à mesurer. Il est prouvé qu'elles influent efficacement sur la prise de

décision des consommateurs et qu'elles peuvent causer des préjudices, notamment en ce qui concerne les pertes financières, les atteintes à la vie privée, la pression psychologique, l'affaiblissement ou la perturbation de la concurrence et la perte de confiance des consommateurs. Certaines catégories d'individus, comme les personnes les moins instruites, les consommateurs à faible revenu ou les enfants, pourraient être touchées de manière disproportionnée.

Gardant à l'esprit l'expérience de Yoko, Antonio craint que ses enfants puissent être vulnérables aux interfaces truquées. Dans les jeux vidéo, Tom dépense de plus en plus d'argent de poche pour acheter des éléments aléatoires (*« loot boxes »* ou « coffres-surprises »), qui semblent faire appel à un design trompeur et à des techniques de marketing agressives comparables à celles dont Yoko a été victime. Environ 60 % des jeux les plus populaires sur les magasins d'applications que sont Google Play et l'App Store contiendraient des coffres-surprises (Zendle et al., 2020[11]), et 44 % des jeunes de 11 à 16 ans au Royaume-Uni qui connaissaient l'existence de ces coffres-surprises avaient dépensé de l'argent pour les acheter (Gambling Commission, 2019[12]). Fait troublant, les enfants semblent aussi rarement identifier les publicités et les témoignages promotionnels dans les jeux et sur les médias sociaux (OCDE, 2021[13]).

...ce qui pousse les consommateurs à se méfier des interactions en ligne en général.

De temps à autre, Antonio réfléchit à l'empreinte numérique de la présence en ligne permanente des membres de sa famille. Il admet ne pas vraiment savoir quelle est la finalité de l'utilisation de leurs données, d'autant plus qu'ils ne lisent jamais les bannières de consentement aux cookies, ni les conditions d'utilisation ou les politiques de protection de la vie privée, estimant qu'elles sont trop longues et partant souvent du principe qu'ils doivent de toute façon les accepter. Le fait que les enfants ne soient pas conscients de la valeur que leurs données peuvent avoir pour les entreprises pourrait en effet les exposer à un risque accru de violation de leur droit à la vie privée.

Antonio s'inquiète parfois de savoir si le fait qu'un si grand nombre de données à caractère personnel puissent être utilisées à des fins de profilage algorithmique par les entreprises pourrait rendre sa famille plus vulnérable à l'exploitation ou aux discriminations, même s'il n'est pas sûr du bien-fondé de ces craintes. Et si les entreprises pouvaient déterminer l'état émotionnel, les biais ou les problèmes de santé individuels des membres de sa famille à des moments clés et les manipuler via des publicités ciblées ou leur faire payer des prix plus élevés que d'autres utilisateurs ? Les algorithmes dont l'apprentissage est basé sur des données historiques pourraient-ils reproduire ou exacerber la marginalisation que sa sœur, María, subit en tant que personne handicapée ? Antonio a également entendu que les algorithmes et l'IA pouvaient avoir un impact disproportionné sur les individus en fonction de leur origine ethnique ou raciale et d'autres caractéristiques protégées.

Les interactions sociales en ligne peuvent également présenter des dangers...

La transformation numérique a permis une diffusion plus rapide, moins coûteuse et plus large de contenus préjudiciables. Il y a tout juste quelques semaines, Tom, le fils d'Antonio et de Yoko, a suivi à l'école un cours de prévention au cyberharcèlement. Il a appris que les technologies numériques facilitaient l'expansion et l'amplification du cyberharcèlement, et que ce dernier était souvent associé à des niveaux élevés de stress, de difficultés sociales, de dépression, d'anxiété, d'automutilation et de suicide. D'autres types de contenus préjudiciables, comme la propagande et la désinformation, peuvent constituer des menaces pour la démocratie et avoir des répercussions de grande ampleur. La famille d'Antonio se souvient encore d'un scandale dans lequel un cabinet de conseil politique avait collecté et vendu les données de 50 millions d'utilisateurs d'un réseau social sans leur consentement, pour influencer les

électeurs (ICO, 2018[14]). Les termes « caisses de résonance » et « bulles de filtres » sont utilisés pour décrire des communautés en ligne partageant les mêmes valeurs et qui sont peu exposées à différents points de vue. Ces phénomènes sont parfois renforcés par des algorithmes et peuvent contribuer à la propagation d'informations fausses et trompeuses, à l'isolement intellectuel, à l'exacerbation des préjugés et à la polarisation des positions idéologiques. Cette tendance s'étend aux contenus illicites. Par exemple, Yoko a souvent entendu parler dans des reportages d'auteurs d'attentats terroristes qui s'étaient radicalisés en ligne ou qui avaient diffusé un attentat en direct sur l'internet.

Ana, la fille de 11 ans d'Antonio et Yoko, a installé sur son téléphone une application de médias sociaux que tous les autres élèves de sa classe utilisaient, alors qu'elle savait qu'elle n'était pas autorisée à le faire. L'été dernier, elle a reçu via cette application une invitation provenant d'un inconnu. Voyant qu'ils avaient des amis en commun, elle a accepté l'invitation. Ils ont commencé à discuter, mais il lui a soudain envoyé plusieurs photos à caractère violent et pornographique. Il a aussi commencé à lui demander d'envoyer des photos d'elle. Elle l'a immédiatement bloqué mais, trop effrayée et choquée, elle n'a pas raconté à ses parents ce qui s'était passé. Ils ont tout de même remarqué que quelque chose n'allait pas, voyant qu'elle semblait bouleversée.

L'ampleur de l'exploitation et des abus sexuels en ligne concernant des enfants augmente à un rythme effroyable. Les victimes sont principalement des filles, bien que les garçons soient également touchés, et sont principalement âgées de 3 à 13 ans ; cependant, les images représentent souvent des enfants de 0 à 2 ans. Le phénomène de « sextorsion » prend également de l'ampleur : dans ces situations, un prédateur exige d'un enfant des faveurs sexuelles, de l'argent ou d'autres avantages sous la menace de partager les contenus produits par la victime elle-même (WeProtect Global Alliance, 2021[15]).

...tandis que les mesures de protection comportent leurs propres risques.

Yoko s'est renseignée et a appris que les technologies et algorithmes numériques existants et émergents pouvaient détecter des contenus et pratiques préjudiciables et/ou illicites et prendre des mesures correctives. C'est le cas par exemple des outils permettant de détecter et de supprimer des contenus terroristes et extrémistes violents en ligne à l'aide de bases de données ou d'outils partagés entre entreprises, ou qui identifient automatiquement les pratiques commerciales préjudiciables en ligne. Cependant, les recherches de Yoko lui ont également appris que la détection algorithmique de contenus au moyen de l'IA pouvait présenter ses propres limites et problèmes, étant donné que ces outils peuvent être imprécis, biaisés et discriminatoires dans leur conception, et pourrait faciliter la censure et la surveillance de masse par les entreprises (Federal Trade Commission des États-Unis, 2022[16]), voire par les pouvoirs publics.

Les technologies de surveillance de masse peuvent compromettre la liberté d'expression et la confidentialité, mais aussi la sécurité physique et, en définitive, le droit à la vie. En effet, dans certains pays, il existe un lien avéré entre l'utilisation de technologies de surveillance et les arrestations, intimidations et assassinats de journalistes et de militants des droits humains. Ces technologies peuvent également susciter la peur et conduire des personnes (notamment les journalistes, les défenseurs et les militants) à s'autocensurer, menaçant la liberté d'expression et la capacité des populations à accéder à l'information. Elles peuvent

aggraver les conséquences physiques et psychologiques des violences sexistes et conjugales.

Yoko a lu dans les médias que la Commission fédérale du commerce (FTC) avait pris des mesures à l'encontre d'une entreprise vendant des applications de type « logiciel de traque », qui peuvent être installées subrepticement sur un appareil afin de surveiller les photos, messages textuels, historiques de navigation, localisations GPS et autres informations personnelles du propriétaire de l'appareil à son insu (Federal Trade Commission des États-Unis, 2021[17]).

Il est important que les politiques placent l'humain au cœur de la transformation numérique

Antonio, Yoko, Tom, Ana, Ken et María sont certes fictifs, mais les défis décrits ci-dessus sont une réalité pour des millions de personnes dans le monde. Compte tenu des avantages et des risques multiples induits par l'environnement numérique, il est essentiel que le bien-être économique et social et la sécurité psychologique et physique des individus soient au centre de l'action des pouvoirs publics. Ce qui implique d'adopter une approche, non pas purement protectionniste, mais conforme à la double priorité de protection et d'autonomisation, qui tout à la fois optimise les avantages et limite les risques. Si des efforts restent à déployer, l'OCDE mène de longue date des travaux sur ces questions (Encadré 1).

Encadré 1. Travaux de l'OCDE visant à placer l'humain au cœur de la transformation numérique

Protection de la vie privée

- Lignes directrices de l'OCDE sur la protection de la vie privée
- Recommandation du Conseil sur la coopération transfrontière dans l'application des législations protégeant la vie privée

Protection des enfants dans l'environnement numérique

- Recommandation du Conseil sur les enfants dans l'environnement numérique
- Lignes directrices de l'OCDE à l'intention des prestataires de services numériques

Rapports de transparence

- Rapports d'évaluation comparative 2020 ; 2021 et 2022
- Cadre relatif à l'établissement de rapports de transparence volontaires

Protection des consommateurs

- Lignes directrices régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses
- Protection du consommateur dans le commerce électronique
- Sécurité des produits de consommation

Un effort multilatéral et nuancé de la part des pouvoirs publics

Préserver le bien-être des personnes, qu'elles agissent en qualité de citoyens, de travailleurs ou de consommateurs, et veiller à la protection et au respect de leurs droits exigent des approches de l'action publique coordonnées, fondées sur des données probantes.

Les défis inhérents à la lutte contre les effets préjudiciables des contenus erronés et/ou trompeurs – dont la mésinformation, la désinformation, la propagande, les informations sorties de leur contexte et la satire – qui se diffusent largement et rapidement en ligne, illustrent cette complexité. Il devient dès lors difficile, à l'ère numérique, de trouver un juste équilibre entre, d'un côté, ces problématiques et, de l'autre, la liberté d'expression et l'accès à des informations fiables sur les enjeux mondiaux tels que le changement

climatique. Lorsque les pouvoirs publics ou les entreprises déploient des efforts disproportionnés pour supprimer les contenus préjudiciables ou trompeurs, ils peuvent restreindre indûment la parole. La liberté d'expression et une presse libre et indépendante sont indispensables au bon fonctionnement des sociétés démocratiques (OCDE, 2022[18]). Il convient toutefois de veiller à concilier la liberté d'expression et les autres droits, tels que la santé et la vie privée.

La protection de la vie privée et des données est souvent au centre des débats sur l'équilibre à trouver entre des droits et des intérêts concurrents. Comment les consommateurs peuvent-ils bénéficier des avantages de la publicité et des contenus personnalisés sans transiger sur la protection des données qui les concernent ? Le chiffrement de bout en bout est souvent jugé essentiel pour protéger la vie privée ; or, dans le cadre de la lutte contre l'exploitation et les abus sexuels concernant les enfants, par exemple, on peut considérer qu'il permet aux acteurs malveillants de mener leurs activités en dehors de toute surveillance. Ce dilemme nécessite une collaboration entre les décideurs, la société civile, les experts des technologies et de la vie privée, les services chargés du contrôle de l'application des lois et les spécialistes de la protection des enfants.

Il conviendrait peut-être également de mener une réflexion plus critique sur la façon dont on fait respecter certains droits. Par exemple, on tend à remettre en question des hypothèses encore répandues selon lesquelles les données anonymisées ou dépersonnalisées n'ont pas d'incidence sur la protection de la vie privée. Certes, la dépersonnalisation peut protéger contre la divulgation de l'identité et la violation de la vie privée des individus, mais elle n'empêche pas l'attribution de traits ou de caractéristiques aux groupes auxquels ils appartiennent. Ce qui soulève des questions quant aux droits collectifs des groupes (tels que les populations autochtones, par exemple), notamment sur leur capacité à s'autodéterminer et à exercer leur souveraineté sur leurs données pour parer au désavantage systémique qu'ils subissent (OCDE, 2022[19]). D'aucuns avancent qu'il importe d'offrir aux individus de la visibilité ou de la transparence sur l'utilisation qui est faite de leurs données à caractère personnel une fois qu'elles ont été dépersonnalisées, et de leur donner des informations pour qu'ils puissent déterminer si cette utilisation est conforme à leurs valeurs (CGIPN[20]). Les solutions en matière de transparence ne suffisent généralement pas à elles seules et les individus n'en tirent que peu d'avantages, le suivi de l'utilisation de leurs informations personnelles dans le cadre des différentes technologies étant à la fois chronophage et complexe.

Il est important que les décideurs s'attachent à éviter que leurs actions aient des conséquences préjudiciables indésirables, par exemple que la résolution de problèmes sociaux existants n'en crée de nouveaux. Les réponses juridiques apportées à la textopornographie en offrent un exemple probant. Les enfants qui la pratiquent peuvent contribuer à produire des contenus apparentés juridiquement à de l'exploitation et des abus sexuels concernant les enfants ; nombreux sont ceux qui ont été visés par des mesures pénales – certains ont fait l'objet de poursuites ou d'une inscription sur un registre des délinquants sexuels sur mineurs obligatoire –, ce qui peut avoir des répercussions négatives qui les suivront toute leur vie. La Recommandation de l'OCDE sur les enfants dans l'environnement numérique aborde ces questions et préconise que les mesures prises pour protéger les enfants dans l'environnement numérique soient proportionnées et ne soient pas indûment punitives, et que, le cas échéant, l'on envisage en premier lieu des méthodes éducatives ou thérapeutiques (OCDE, 2021[21]).

Protection, autonomisation, sécurité et droits des consommateurs au centre des politiques et de leur application

Des lois visant à lutter contre ces risques émergents existent déjà. De nombreux pays et territoires se sont dotés de lois sur la protection de la vie privée et des données tenant compte de normes internationales communes telles que les Lignes directrices de l'OCDE sur la protection de la vie privée, qui énoncent des principes fondamentaux en la matière. Par ailleurs, nombre de législations relatives à la protection des consommateurs, qui reprennent les principes phares de la Recommandation de 2016 de l'OCDE sur la protection du consommateur dans le contexte du commerce électronique (OCDE, 2016[22]) et de la

Recommandation de 2020 de l'OCDE sur la sécurité des produits de consommation (OCDE, 2020[23]), intègrent des dispositions interdisant les pratiques commerciales trompeuses, mensongères, frauduleuses, déloyales et préjudiciables, ainsi que la commercialisation de produits dangereux (OCDE, à paraître[24] ; OCDE, 2022[9]). Beaucoup prévoient des mesures de protection particulières pour les consommateurs vulnérables, dont les enfants (OCDE, à paraître[24]). Les autorités chargées de la protection des consommateurs et des données peuvent dès lors apporter des réponses à de multiples préoccupations. De même, de nombreux pays suivent la Recommandation de l'OCDE relative à des Principes de haut niveau sur la protection financière des consommateurs (OCDE, 2012[25]) pour mettre en place ou renforcer leurs cadres dans ce domaine et gérer les incidences, les opportunités et les risques inhérents à la transformation numérique.

Un consensus se dégage toutefois sur la nécessité d'une mise en œuvre plus exhaustive et sur le fait que, dans bien des cas, la réglementation existante est insuffisante. Cela tient en partie aux caractéristiques propres à l'environnement numérique, par opposition au monde physique, à savoir son ubiquité, une rapidité et une échelle considérables, et l'absence de frontières. De plus, les données et les contenus peuvent être reproduits à un coût nul ou faible, et partagés ou utilisés dans des algorithmes.

Jusqu'à récemment, de nombreux domaines de l'environnement numérique reposaient sur l'autorégulation des entités privées, qui bénéficiaient souvent d'exonérations de responsabilité. Les forums internationaux à haut niveau et les responsables de l'action publique s'intéressent aujourd'hui aux moyens de protéger le bien-être économique et social, la vie privée et la sécurité de tous, dans le cadre de la transformation numérique, en proposant ou en mettant en œuvre de nouvelles réglementations.

Les décideurs insistent sur le rôle des entreprises et des plateformes en ligne dans les solutions face aux préjudices qui y sont causés. Cette tendance est reconnue aux niveaux de l'OCDE, du G7 et du G20[1]. Les appels lancés mettent souvent l'accent sur la responsabilité partagée et la nécessité d'une approche multipartite. La Recommandation de l'OCDE sur la protection du consommateur dans le contexte du commerce électronique insiste par exemple sur le fait qu'il incombe aux entreprises de contribuer à promouvoir le bien-être des consommateurs et de renforcer leur confiance, les appelant à prendre dûment en considération leurs intérêts (OCDE, 2016[22]).

Dans le même temps, les décideurs proposent de contraindre les entreprises présentes sur l'internet – en particulier les plateformes, dont les places de marché – à protéger les consommateurs et interdire les pratiques préjudiciables. Plusieurs lois ou propositions de lois entendent interdire les interfaces truquées, limiter la publicité ciblée, ou obliger les places de marché en ligne à lutter contre la vente de produits dangereux. D'autres propositions de lois portent sur les pratiques préjudiciables ou les produits de consommation fondés sur l'IA (il s'agit par exemple d'interdire le recours aux techniques subliminales ou les pratiques visant à exploiter les vulnérabilités des personnes pour altérer de manière substantielle leur comportement (OCDE, 2022[9])[2]. D'autres mesures encore ont pour but de donner aux consommateurs les moyens de prendre des décisions plus éclairées au sein de l'environnement en ligne, notamment en améliorant l'efficacité de la communication d'informations (OCDE, 2022[26]).

On prête une attention particulière aux pratiques des plateformes électroniques – en particulier les plus importantes – en matière de transparence et de responsabilité. Des pays et territoires de plus en plus nombreux imposent aux plateformes électroniques des exigences de transparence, notamment sur leurs politiques et mesures relatives à la modération de contenu, et prévoient des sanctions en cas de non-respect. Ces exigences portent par exemple sur l'établissement de rapports sur les méthodes de détection (examen humain, technologies automatisées, signaleurs de confiance), les mesures correctrices (retrait ou blocage des contenus, avertissements, suspension ou retrait du compte), et les mécanismes de réclamation, procédures de règlement des litiges et évaluations des risques. La plupart de ces mesures sont inscrites dans des lois traitant plus largement de la sécurité en ligne[3]. Elles aussi sont centrées sur les activités des plateformes en ligne et prévoient des obligations visant à faciliter le signalement de contenus illicites ou préjudiciables, en exiger le retrait, et imposer des sanctions en cas de non-respect de

ces obligations. Il en va de même pour l'utilisation des données à caractère personnel. Une enquête de l'Australian Competition and Consumer Commission a en effet mis en évidence un manque de transparence sur les plateformes numériques, l'absence de choix éclairés de la part des consommateurs sur la collecte et l'utilisation des données, ainsi que la nécessité de renforcer les mesures de protection dans la législation relative à la protection de la vie privée (ACCC, 2019[27]).

La lutte contre les préjudices que subissent les enfants et la violence sexiste est une question importante et de nombreuses propositions énoncent des mesures pour combattre les violences sexistes et conjugales[4], ou l'exploitation des vulnérabilités des enfants. Parmi les mesures axées sur les enfants figure la Proposition de règlement de l'UE établissant des règles en vue de prévenir et de combattre les abus sexuels sur les enfants (CE, 2022[28]) ; certaines imposent par ailleurs d'intégrer, dès la phase de conception, des considérations relatives à la protection de la vie privée adaptées à l'âge, spécifiquement pour les enfants.

On porte en outre une attention croissante aux intérêts des travailleurs dans l'environnement en ligne. Selon l'OCDE, les pouvoirs publics devraient veiller à ce que tous les travailleurs bénéficient de droits et de protections adaptés, indépendamment de leur situation au regard de l'emploi ou de leur type de contrat, et devraient garantir des règles du jeu équitables en empêchant certaines entreprises d'acquérir un avantage concurrentiel indu (OCDE, 2019[29]). La proposition de Directive européenne sur l'amélioration des conditions de travail sur les plateformes prévoit des mesures de protection lorsque celles-ci devraient être considérées comme des employeurs (par opposition à celles où l'on considère que les travailleurs sont indépendants). Les travailleurs pourront dès lors bénéficier d'avantages tels que des congés payés, des droits à retraite et un salaire minimum (CE, 2022[30]). Les décideurs et les autorités de réglementation chargées des questions de protection de la vie privée s'intéressent en outre à la portabilité des données, qui peut permettre aux travailleurs à la demande de conserver les données attestant de leur réputation d'une plateforme à l'autre.

Ces questions sont de plus en plus souvent examinées dans le contexte des droits. La transformation numérique modifie-t-elle les attentes quant à la façon dont les pouvoirs publics protègent et font respecter les droits ? Du fait des technologies numériques, devient-il plus difficile de concilier les droits concurrents ? Si certains pays s'intéressent à des droits individuels particuliers, tels que les droits à la protection des données à caractère personnel ou à l'accès à l'internet (Conseil d'État, 2016[31]), d'autres optent pour une approche plus globale de la question et lancent de vastes initiatives visant à assurer la protection des droits à l'ère numérique et à veiller à ce que la transformation numérique soit centrée sur l'humain. En 2021, le gouvernement espagnol a adopté une Charte des droits numériques (Gouvernement de l'Espagne, 2021[32]) ; en 2022, la Commission européenne a proposé une Déclaration sur les droits et principes numériques, afin de les ancrer dans la transformation numérique (CE, 2022[33]) ; et la Corée entend présenter un projet de loi sur les droits numériques en 2023 (Ministry of Science and ICT, Republic of Korea, 2022[34]).

Certains pays et territoires étudient l'instauration de nouveaux droits dans des domaines particuliers, par exemple concernant la transparence algorithmique et la responsabilité dans le cadre de la prise de décision fondée sur l'IA, tandis que d'autres s'attachent en priorité à garantir une protection identique des droits dans l'environnement numérique et dans le monde réel. À l'échelle internationale, la question de la défense des droits en ligne est envisagée pour les enfants. En 2018, le Conseil de l'Europe a élaboré des Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique (CdE, 2018[35]) ; et en 2021, le Comité des droits de l'enfant a adopté une Observation générale sur les droits de l'enfant en relation avec l'environnement numérique (CRC, 2021[36]). Pour ce qui est de la responsabilité des entreprises de respecter les droits dans l'environnement numérique, le projet B-Tech du Haut-Commissariat des Nations unies aux droits de l'homme propose des orientations de référence et des ressources afin d'aider à mettre en œuvre les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits humains dans le domaine des technologies (HCDH, s.d.[37]).

Compatibilité des lois et des politiques entre les frontières et les domaines

Les responsables de l'action publique et les organismes de réglementation devraient garder à l'esprit que l'environnement numérique transcende les frontières traditionnelles et qu'il se caractérise par d'importantes interdépendances. Les exemples de réponses fragmentaires des pouvoirs publics sont légion. La responsabilité de répondre aux besoins des enfants dans le monde numérique est souvent confiée aux ministères responsables de cette même question dans le monde physique (OCDE, 2020[38]), quand bien même de nombreux problèmes comme la textopornographie et le cyberharcèlement nécessitent une action coordonnée de la part des autorités judiciaires, sanitaires et scolaires (tout au moins), ainsi que la prise en compte des incidences sur le droit des enfants à la vie privée. De même, l'hétérogénéité des exigences en matière de transparence, d'établissement de rapports et de responsabilité pour lutter contre les contenus violents et extrémistes pourrait s'avérer coûteuse et inefficace. Les entreprises multinationales pourraient devoir publier plusieurs versions de leurs rapports de transparence, les différents gouvernements risqueraient de supporter des coûts législatifs redondants, et les parties prenantes devraient vraisemblablement rechercher les rapports à différents endroits. Afin de remédier à ces problèmes, l'OCDE a lancé, en mai 2022, le Cadre relatif à l'établissement de rapports de transparence volontaires sur les contenus terroristes et extrémistes violents (OCDE, 2022[39]), une plateforme internationale normalisée que tout service de partage de contenus en ligne peut utiliser, indépendamment de sa taille ou de son modèle économique.

Souvent, la même question relève de plusieurs domaines d'action à la fois, d'où la nécessité d'une coopération réglementaire. Les interfaces truquées, les pratiques de personnalisation à des fins d'exploitation et l'utilisation biaisée des algorithmes peuvent relever de la politique à l'égard des consommateurs, de la politique relative au respect de la vie privée, de la politique de la concurrence, de la politique relative à l'intelligence artificielle, ainsi que de la politique de lutte contre la discrimination. Du fait de l'omniprésence des données dans les secteurs économiques et sociaux, les lois relatives à la protection de la vie privée et des données doivent pouvoir être appliquées dans divers domaines réglementaires, tels que la concurrence et la protection des consommateurs (OCDE, 2022[40]), les autorités compétentes dans ces domaines étant appelées à traiter de questions différentes. Les autorités chargées de la protection de la vie privée pourraient être amenées à évaluer les incidences de la concentration économique sur la protection des données, tandis que les autorités de la concurrence doivent déterminer si la présence d'informations personnelles ou les préoccupations liées à la protection de la vie privée influent sur les analyses de la concurrence. Il est important de comprendre dans quelle mesure les autorités peuvent coopérer et de quelle manière leurs écosystèmes réglementaires peuvent fonctionner les uns avec les autres. Plusieurs pays ont mis en place des forums destinés à renforcer la coopération entre les autorités de réglementation du monde numérique, notamment celles chargées de la protection des consommateurs, du respect de la vie privée, de la concurrence et des communications.

Au lieu d'agir de manière cloisonnée et non coordonnée, les pouvoirs publics et les organismes de réglementation devraient élaborer des approches globales en consultation avec la société civile et les entreprises, favoriser les synergies et la coopération entre différents domaines d'action, éviter les répétitions inutiles d'efforts et déterminer le mécanisme qui serait le plus adapté pour s'attaquer à ces problèmes. La Recommandation de l'OCDE en faveur d'une gouvernance réglementaire agile permettant de mettre l'innovation à profit appelle les pouvoirs publics à jeter des bases institutionnelles permettant une coopération et des approches décloisonnées, tant au sein de chaque territoire qu'entre plusieurs territoires (OCDE, 2021[41]). La cohérence des politiques peut en outre aider les pays de l'OCDE à atteindre les Objectifs de développement durable, qui sont pluridimensionnels et couvrent de nombreux domaines d'action revêtant une importance particulière pour placer l'humain au premier plan de la transformation numérique.

La coopération transfrontière est indispensable dans la mesure où les risques que l'on rencontre dans le cyberespace, tels que les pratiques trompeuses et frauduleuses, les menaces pour la vie privée et les

produits dangereux, constituent des problèmes transnationaux. Toutefois, des difficultés persistent à cet égard. Les organismes chargés de faire respecter l'application de la loi ne disposent souvent pas de l'autorité voulue pour coopérer pleinement avec leurs homologues étrangers ou rencontrent parfois des difficultés pratiques pour travailler avec ceux-ci. En 2021, l'OCDE a publié des orientations sur les mesures législatives pouvant doter les autorités chargées de la protection des consommateurs des pouvoirs et des moyens d'action nécessaires pour faire appliquer les lois sur la protection des consommateurs au niveau national et pour mener à bien une coopération transfrontière (OCDE, 2021[42]). La récente Recommandation de l'OCDE sur la coopération réglementaire internationale face aux défis de portée mondiale vise à aider les responsables publics et les organismes de réglementation à transformer les processus de gouvernance et d'élaboration des règles – qui sont tournés vers l'intérieur – afin de concrétiser les avantages de la coopération internationale (OCDE, 2022[43]).

Mesures réglementaires fondées sur des données probantes

Afin d'établir les priorités de l'action publique pour optimiser les mécanismes de protection et créer de nouvelles possibilités, il faut disposer de données probantes, actualisées et fiables pour comprendre les points forts et les lacunes des politiques. La base factuelle présente encore de grandes lacunes à l'égard de plusieurs problèmes, notamment ceux rencontrés par la famille de Yoko et d'Antonio.

Les interfaces truquées sont un domaine dans lequel la base factuelle doit être améliorée pour soutenir l'action des pouvoirs publics et des autorités de répression. Il est notamment nécessaire de comprendre les effets que certaines interfaces truquées peuvent avoir sur les décisions des consommateurs, ainsi que l'ampleur des préjudices susceptibles d'être subis par ces derniers. Dans bien des cas, il est question de disposer de données factuelles non seulement plus nombreuses ou de meilleure qualité, mais aussi plus diverses. Selon la Recommandation de l'OCDE de 2016 sur la protection du consommateur dans le contexte du commerce électronique, il est essentiel de prendre en compte les enseignements de l'économie comportementale pour étoffer la base factuelle servant à l'élaboration des politiques de consommation, notamment en recourant à des méthodes de recherche empirique comme l'expérimentation.

La base factuelle sur laquelle repose l'élaboration des politiques relatives à la protection de la vie privée manque en outre d'uniformité. Les autorités chargées de la protection de la vie privée recueillent des quantités considérables de données rendues publiques dans les rapports annuels, mais pas nécessairement dans un format adapté aux comparaisons internationales. L'hétérogénéité grandissante des lois relatives à la protection de la vie privée et à la protection des données à l'échelle mondiale constitue une source de préoccupation récurrente, même si celles-ci sont généralement conformes aux principes de protection des données énoncés dans les Lignes directrices de l'OCDE régissant la protection de la vie privée. Ces disparités peuvent tenir à une application divergente des principes dans la pratique ou à l'application de règles semblables mais établies pour des raisons différentes. Cependant, à mesure que la technologie évolue, que les données deviennent plus omniprésentes et que de plus en plus de pays adoptent des lois relatives à la protection de la vie privée, de nouvelles données probantes sont nécessaires pour repérer ces disparités et évaluer si les solutions en place restent pertinentes.

On constate également des lacunes importantes dans les données nécessaires pour protéger les enfants et favoriser leur autonomisation dans l'environnement numérique. Dans bien des cas, les politiques relatives à la protection des enfants dans l'environnement numérique sont élaborées en réponse à des événements (incidents ayant un grand retentissement, par exemple) ou reposent sur des éléments incomplets plutôt que sur des données fiables et représentatives. Ainsi, on entend fréquemment que passer trop de temps devant un écran nuit à la santé et au bien-être des enfants, mais les éléments factuels à l'appui de telles préoccupations font défaut. Les préoccupations relatives au temps passé devant l'écran ne tiennent en outre pas compte du fait que les enfants ne constituent pas un groupe homogène et que les vulnérabilités des enfants dans le monde numérique sont influencées par celles qu'ils les

caractérisent dans le monde réel (le sexe, le milieu socioéconomique, etc.). Qui plus est, le temps passé devant un écran ne présente pas toujours le même risque et n'est pas toujours préjudiciable ; cela dépend des activités pratiquées par les enfants sur l'internet. Il convient de faire une distinction entre un adolescent sujet à des troubles de l'alimentation qui voit des images irréalistes du corps et un adolescent qui trouve une communauté de soutien dédiée à un sujet lui tenant à cœur. Il est nécessaire de mener des études exhaustives, de qualité et à grande échelle concernant les effets de l'environnement numérique sur la santé et le bien-être des enfants, en tenant compte de la multitude d'activités que les enfants pratiquent dans cet environnement, ainsi que de l'évolution de leurs capacités et de leurs vulnérabilités (OCDE, 2022[44]).

La version révisée de la Feuille de route de l'OCDE sur la mesure de la transformation numérique, qui souligne que les systèmes statistiques nationaux doivent s'adapter et se développer pour tenir compte de la transformation numérique des économies et des sociétés, peut aider les responsables de l'action publique à constituer leur base factuelle et à définir des priorités cohérentes en vue de mesurer la transformation numérique à l'aide de méthodologies et d'approches communes (OCDE, 2022[45]).

Mesures non contraignantes visant à renforcer la réglementation et son application

Les dispositions législatives et réglementaires et leur application doivent être étayées par des mesures complémentaires pour renforcer la sécurité numérique, protéger les internautes et leur donner des moyens d'agir. Il pourrait s'agir, pour les entreprises, de prendre des engagements en matière de prévention de la vente de produits dangereux sur les places de marché en ligne (OCDE, 2021[46]) ou de définir des normes éthiques destinées à promouvoir une conception conviviale de l'interface utilisateur. De telles actions pourraient aider les entreprises à améliorer leur réputation et à renforcer la confiance des utilisateurs. Les mesures librement consenties par une entreprise jouent aussi un rôle important dans l'atténuation des risques, notamment sur le plan de la sécurité de l'information. Il peut s'agir de mesures ou de mécanismes visant à empêcher tout dommage, toute interférence ou tout accès non autorisé, de politiques de sécurité de l'information ou encore d'une évaluation des risques.

Les initiatives qui adoptent une approche « dès la conception » sont des stratégies prometteuses. Certaines sont bien connues, notamment le respect de la vie privée dès la conception et la sécurité dès la conception, qui définissent les principes et les facteurs de base à prendre en compte dès la phase de conception d'un service ou d'un produit et à intégrer dans son fonctionnement (OCDE, 2020[47]). La sécurité numérique dès la conception est une approche plus récente mais qui s'impose de plus en plus comme un objectif d'action, et plusieurs définitions ont vu le jour ces dernières années. D'après certains gouvernements et des organisations internationales de la société civile, la sécurité dès la conception consiste à placer les considérations de sécurité des utilisateurs au centre du développement des services et des produits et permet de réduire autant que possible les menaces en les anticipant, en les détectant et en les éliminant avant qu'elles ne se concrétisent, plutôt que de devoir réagir en mettant en œuvre des mesures correctives (eSafety, s.d.[48]).

Des mesures techniques peuvent également contribuer à remédier aux risques. On peut citer à titre d'exemple des outils tels que les robots d'indexation fondés sur l'IA qui permettent aux autorités chargées de la protection des consommateurs de détecter et de limiter les interfaces truquées ou les produits dangereux vendus en ligne. En 2022, la Commission européenne a lancé un outil de surveillance en ligne destiné à aider les autorités nationales à repérer les offres en ligne de produits dangereux signalés dans « Safety Gate », le système d'alerte de l'UE pour les produits non alimentaires dangereux (CE, 2022[49]). D'autres outils permettent aux entreprises d'examiner leur architecture de choix en ligne, et aux consommateurs de se protéger contre les interfaces truquées, comme les extensions de navigateur qui communiquent automatiquement à l'entreprise les décisions des consommateurs en matière de protection de la vie privée sans que ces derniers n'aient besoin de répondre à une bannière de consentement aux cookies.

Des mesures d'éducation et de sensibilisation peuvent orienter les citoyens et les consommateurs vers l'information, et les aider à éviter de subir des préjudices sur l'internet ou à faire des réclamations. Les orientations peuvent être adaptées à certains groupes de consommateurs, à l'image des campagnes axées sur les enfants ou les consommateurs ayant des compétences numériques moins développées (OCDE, à paraître[24]). De manière plus générale, l'éducation numérique est essentielle pour protéger et autonomiser les internautes. De nombreux pays de l'OCDE disposent d'une stratégie d'éducation numérique ou inscrivent cette question dans une stratégie d'innovation numérique. Les initiatives en faveur de la maîtrise du numérique s'adressent souvent aux enfants – chose essentielle – mais elles devraient aussi cibler un plus large public, en vue notamment d'améliorer les choix financiers des consommateurs (OCDE, 2020[50]), de renforcer les compétences des travailleurs ou leur reconversion, de transmettre des compétences numériques aux seniors ou d'aider les parents, les aidants et les enseignants (ainsi que les administrations locales et les autorités scolaires) à comprendre les technologies de façon à pouvoir guider les enfants. Il est important d'assurer un accès équitable aux programmes de maîtrise du numérique, en particulier pour les enfants. On observe que les disparités sociales et culturelles peuvent créer des disparités en matière de compétences numériques, ce qui peut exacerber certains risques. Ainsi, une plus grande maîtrise du numérique par un cyberharceleur peut créer le rapport de pouvoir déséquilibré qui caractérise de nombreuses formes de harcèlement.

Ces initiatives et ces outils jouent un rôle important, mais ils ne peuvent suffire à eux seuls : c'est pourquoi ils doivent être complémentaires de mesures réglementaires et d'application robustes.

Conclusion : garder une longueur d'avance

D'un côté, les membres de la famille de Yoko et Antonio tirent profit de la transformation numérique, comme citoyens, comme consommateurs et comme travailleurs. L'expérience consommateur s'est améliorée, les interactions sociales et l'inclusion se sont développées, les relations entre les citoyens et leurs administrations se sont transformées, et le potentiel des travailleurs a été amplifié. D'un autre côté, on voit apparaître d'importants risques qui tiennent à l'émergence en ligne de nouvelles formes de pratiques commerciales dommageables, de contenus préjudiciables et illégaux, d'atteintes à la vie privée, à la protection des données personnelles et à la liberté d'expression, sans parler des discriminations et des biais que peut entraîner l'utilisation des algorithmes.

Les avancées rapides et l'adoption généralisée des nouvelles technologies donnent à penser que l'échelle et la nature des vulnérabilités liées à l'avènement du numérique sont en train d'évoluer rapidement. Certains d'entre nous restent disproportionnellement vulnérables, en particulier les catégories défavorisées, marginalisées, minoritaires ou sous-représentées. Cela étant, dans l'environnement numérique actuel, la plupart, si ce n'est la totalité, d'entre nous peut se retrouver en situation de vulnérabilité, selon le moment et selon le contexte. Dans la sphère de la consommation, plusieurs universitaires ont appelé à revoir notre conception d'une vulnérabilité des consommateurs qui serait universelle ou systémique (OCDE, à paraître[24]).

Les tendances technologiques telles que l'omniprésence de plus en plus marquée de l'IA et de l'internet des objets vont perdurer. Elles seront accompagnées de l'émergence d'autres tendances comme les technologies immersives (réalité augmentée et réalité virtuelle par exemple). Ces évolutions vont nécessiter des approches rapides et innovantes pour garantir la sécurité des générations à venir et le respect de leurs droits.

La Réunion ministérielle du CPEN offre à des responsables de haut niveau l'occasion d'examiner s'il est nécessaire d'adapter les mesures et les concepts actuellement utilisés, et selon quelques modalités, de voir comment il est possible de faire en sorte que la transformation numérique reste centrée sur l'humain et ciblée sur les populations, et d'étudier de quelle manière des objectifs mutuels peuvent être atteints. C'est en ce sens que les droits à l'ère numérique trouvent toute leur pertinence : autrement dit, comment

nos droits dans le monde « physique » sont-ils applicables au monde numérique ? Cette réalité nouvelle rend-elle nécessaire la définition de droits spécifiques au monde numérique ? Pour adapter leur action, les responsables de l'action publique devront aller plus loin, et conférer une plus grande autonomie à tous les membres de la société, y compris à ceux qui sont le plus susceptibles de subir des préjudices. L'OCDE, en sa qualité de forum de discussion, met à la disposition de tous les acteurs les résultats de ses études ainsi que ses conseils stratégiques sur toutes les questions concernées.

Notes

[1] Voir par exemple : les Principes de haut niveau du G20 pour la protection des enfants et leur autonomisation dans l'environnement numérique, en 2021 ; les Principes du G7 relatifs à la sécurité sur l'internet, en 2021 ; les Principes du G7 relatifs à la lutte contre la violence en ligne à l'égard des femmes et des filles et Plan d'action pour la lutte contre l'exploitation et les abus sexuels concernant des enfants, en 2021 ; l'Appel de Christchurch, en 2019 ; et la Déclaration d'Osaka des dirigeants du G20 sur la prévention de l'utilisation d'internet à des fins de terrorisme et d'extrémisme violent pouvant mener au terrorisme, en 2019.

[2] Voir par exemple la Proposition de législation de la Commission européenne sur l'intelligence artificielle.

[3] Voir par exemple : Allemagne (*Netzwerkdurchsetzungsgesetz*, loi visant à améliorer l'application de la législation sur les réseaux sociaux), Australie (Online Safety Act), Canada (projet de loi et de règlement visant à contrer le contenu préjudiciable en ligne), États-Unis (Platform Accountability and Consumer Transparency Act, « PACT ACT »), Irlande (Online Safety and Media Regulation Bill), Nouvelle-Zélande (Films, Videos and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Bill), Royaume-Uni (Online Safety Bill), ou Union européenne (Règlement sur les services numériques).

[4] Par exemple, la Proposition de directive de l'UE sur la lutte contre la violence à l'égard des femmes et la violence domestique traite spécifiquement de la violence en ligne ; en Australie, l'Online Safety Act contient des dispositions particulières sur l'utilisation malveillante d'images.

Références

ACCC (2019), *Digital Platforms Inquiry: Final Report*, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf (consulté le 24 octobre 2022). [27]

CdE (2018), *Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique*, https://rm.coe.int/lignes-directrices-relatives-au-respect-a-la-protection-et-a-la-realis/16808d881b (consulté le 24 octobre 2022). [35]

CE (2022), *Déclaration sur les droits et principes numériques européens*, https://digital-strategy.ec.europa.eu/fr/library/declaration-european-digital-rights-and-principles (consulté le 24 octobre 2022). [33]

CE (2022), *L'UE propose une directive visant à protéger les droits des travailleurs de plateformes*, https://eures.ec.europa.eu/eu-proposes-directive-protect-rights-platform-workers-2022-03-17_fr (consulté le 24 octobre 2022). [30]

CE (2022), *Proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants*, https://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1652451192472&uri=COM%3A2022%3A209%3AFIN (consulté le 24 octobre 2022). [28]

CE (2022), *Système d'alerte rapide: les véhicules à moteur et les jouets figurent en tête de la liste des produits non alimentaires dangereux notifiés cette année*, https://ec.europa.eu/commission/presscorner/detail/fr/IP_22_1343 (consulté le 24 octobre 2022). [49]

CGIPN (s.d.), *Les principes de PCAP des Premières Nations*, https://fnigc.ca/fr/les-principes-de-pcap-des-premieres-nations/ (consulté le 24 octobre 2022). [20]

Conseil d'État (2016), *Fundamental rights in the Digital Age*, https://www.conseil-etat.fr/en/Media/actualites/documents/reprise-_contenus/rapports-et-etudes/fundamental-rights-in-the-digital-age.pdf (consulté le 24 octobre 2022). [31]

CRC (2021), *Observation générale n° 25 (2021) sur les droits de l'enfant en relation avec l'environnement numérique*, https://www.ohchr.org/fr/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation (consulté le 24 octobre 2022). [36]

Di Geronimo, L. et al. (2020), *UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception*, Association for Computing Machinery, New York, NY, USA, https://doi.org/10.1145/3313831.3376600. [10]

eSafety (s.d.), *Safety by Design*, https://www.esafety.gov.au/about-us/safety-by-design (consulté le 24 octobre 2022). [48]

Federal Trade Commission des États-Unis (2022), *FTC Report Warns About Using Artificial Intelligence to Combat Online Problems*, https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems (consulté le 24 octobre 2022). [16]

Federal Trade Commission des États-Unis (2021), *Age of Learning, Inc. (ABCmouse)*, https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3186-age-learning-inc-abcmouse (consulté le 24 octobre 2022). [8]

Federal Trade Commission des États-Unis (2021), *FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data*, https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-bans-spyfone-ceo-surveillance-business-orders-company-delete-all-secretly-stolen-data (consulté le 24 octobre 2022). [17]

Gambling Commission (2019), *Young People and Gambling 2019*, https://www.gamblingcommission.gov.uk/statistics-and-research/publication/young-people-and-gambling-2019 (consulté le 24 octobre 2022). [12]

Gouvernement de l'Espagne (2021), *Charter of Digital Rights*, https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/participacion_publica/audiencia/ficheros/Charter%20of%20Digital%20Rights.pdf (consulté le 24 octobre 2022). [32]

HCDH (s.d.), *Projet B-Tech : Le HCDH et la question des entreprises et des droits de l'homme*, https://www.ohchr.org/fr/business/b-tech-project (consulté le 24 octobre 2022). [37]

ICO (2021), *The Information Commissioner's position paper on the UK Government's proposal for a trusted digital identity system*, https://ico.org.uk/media/about-the-ico/documents/2619686/ico-digital-identity-position-paper-20210422.pdf (consulté le 24 octobre 2022). [3]

ICO (2018), *Investigation into the use of data analytics in political campaigns*, https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf (consulté le 24 octobre 2022). [14]

Ministry of Science and ICT, Republic of Korea (2022), *대한민국 디지털 전략 발표, [Korea Digital Strategy Announcement]*, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=112&pageIndex=3&bbsSeqNo=94&nttSeqNo=3182193&searchOpt=ALL&searchTxt= (consulté le 24 October 2022). [34]

OCDE (2022), *Companion Document to the OECD Recommendation on Children in the Digital Environment*, Éditions OCDE, Paris, https://doi.org/10.1787/a2ebec7c-en. [44]

OCDE (2022), *Dark commercial patterns*, Éditions OCDE, Paris, https://doi.org/10.1787/44f5e846-en. [9]

OCDE (2022), *Enhancing online disclosure effectiveness*, Éditions OCDE, Paris, https://doi.org/10.1787/6d7ea79c-en. [26]

OCDE (2022), *Expert Workshop on Data Ethics: Balancing Ethical and Innovative Uses of Data*, OCDE, https://one.oecd.org/document/DSTI/CDEP/DGP(2022)1/fr/pdf. [19]

OCDE (2022), *Measuring Digital Platform Employment and Work*, https://one.oecd.org/document/WISE/CSSP(2022)4/fr/pdf. [1]

OCDE (2022), *Measuring Financial Consumer Detriment in E-commerce*, Éditions OCDE, Paris, https://doi.org/10.1787/4055c40e-en. [5]

OCDE (2022), *Mésinformation et désinformation : comment les pouvoirs publics peuvent agir pour renforcer la démocratie*, https://one.oecd.org/document/GOV/PGC(2022)8/REV1/fr/pdf. [18]

OCDE (2022), *Recommandation du Conseil sur la coopération réglementaire internationale face aux défis de portée mondiale*, OCDE, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0475. [43]

OCDE (2022), *Review of the 2007 OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy*, https://one.oecd.org/document/DSTI/CDEP/DGP(2022)2/fr/pdf. [40]

OCDE (2022), *The OECD Going Digital Measurement Roadmap*, Éditions OCDE, Paris, https://doi.org/10.1787/bd10100f-en. [45]

OCDE (2022), *VTRF web portal*, https://www.oecd-vtrf-pilot.org/. [39]

OCDE (2021), *Children in the digital environment: Revised typology of risks*, Éditions OCDE, Paris, https://doi.org/10.1787/9b8f222e-en. [13]

OCDE (2021), *Communiqué on product safety pledges*, OCDE, https://www.oecd.org/digital/consumer/communique-product-safety-pledges.pdf. [46]

OCDE (2021), *Implementation toolkit on legislative actions for consumer protection enforcement co-operation*, Éditions OCDE, Paris, https://doi.org/10.1787/eddcdc57-en. [42]

OCDE (2021), *Recommandation du Conseil en faveur d'une gouvernance réglementaire agile permettant de mettre l'innovation à profit*, OCDE, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0464. [41]

OCDE (2021), *Recommandation du Conseil sur les enfants dans l'environnement numérique*, OCDE, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0389. [21]

OCDE (2020), *Perspectives de l'économie numérique de l'OCDE 2020*, Éditions OCDE, Paris, https://doi.org/10.1787/bb167041-en. [47]

OCDE (2020), *Protecting children online: An overview of recent developments in legal frameworks and policies*, Éditions OCDE, Paris, https://doi.org/10.1787/9e0e49a9-en. [38]

OCDE (2020), *Recommandation du Conseil sur la culture financière*, OCDE, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0461. [50]

OCDE (2020), *Recommandation du Conseil sur la sécurité des produits de consommation*, OCDE, http://Https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0459. [23]

OCDE (2019), *Perspectives de l'emploi de l'OCDE 2019 : L'avenir du travail*, Éditions OCDE, Paris, https://doi.org/10.1787/b7e9e205-fr. [29]

OCDE (2016), *Recommandation du Conseil sur la protection du consommateur dans le contexte du commerce électronique*, OCDE, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0422. [22]

OCDE (2016), *Résultats de l'investigation surprise de l'OCDE sur la sécurité des produits vendus en ligne : Commission australienne de la concurrence et de la consommation*, Éditions OCDE, Paris, https://doi.org/10.1787/60bd3ae7-fr. [7]

OCDE (2012), *Recommandation du Conseil relative à des Principes de haut niveau sur la protection financière des consommateurs*, OCDE, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0394. [25]

OCDE (à paraître), *Consumer Vulnerability in the Digital Age*, Éditions OCDE, Paris. [24]

OCDE (à paraître), *OECD Online Product Safety Sweep: Summary Report*, Éditions OCDE, Paris. [6]

OCDE (s.d.), *The OECD Going Digital Toolkit*, https://goingdigital.oecd.org/. [4]

Tribunal of Bologna (2020), *Labour Section, decision of 31 December 2020*, https://www.ansa.it/emiliaromagna/notizie/2021/01/02/rider-cgilalgoritmo-discrimina-sentenza-tribunale-bologna_cc14c299-2c6b-411b-b677-496549ee3af1.html (consulté le 24 octobre 2022). [2]

WeProtect Global Alliance (2021), *Global Threat Assessment*, https://www.weprotect.org/global-threat-assessment-21/ (consulté le 24 octobre 2022). [15]

Zendle, D. et al. (2020), *The prevalence of loot boxes in mobile and desktop games*, Addiction, https://doi.org/10.1111/add.14973. [11]