Perspectives de l'économie numérique de l'OCDE 2020

VERSION ABRÉGÉE

OCDE

Perspectives de l'économie numérique de l'OCDE 2020 (Version abrégée)

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.

Note de la Turquie
Les informations figurant dans ce document qui font référence à « Chypre » concernent la partie méridionale de l'Ile. Il n'y a pas d'autorité unique représentant à la fois les Chypriotes turcs et grecs sur l'Ile. La Turquie reconnaît la République Turque de Chypre Nord (RTCN). Jusqu'à ce qu'une solution durable et équitable soit trouvée dans le cadre des Nations Unies, la Turquie maintiendra sa position sur la « question chypriote ».

Note de tous les États de l'Union européenne membres de l'OCDE et de l'Union européenne
La République de Chypre est reconnue par tous les membres des Nations Unies sauf la Turquie. Les informations figurant dans ce document concernent la zone sous le contrôle effectif du gouvernement de la République de Chypre.

Merci de citer cet ouvrage comme suit :
OCDE (2021), *Perspectives de l'économie numérique de l'OCDE 2020 (Version abrégée)*, Éditions OCDE, Paris, *https://doi.org/10.1787/3b257711-fr*.

ISBN 978-92-64-93148-0 (pdf)

Crédits photo : Couverture © iStockphoto.com/metamorworks.

Les corrigenda des publications sont disponibles sur : *www.oecd.org/about/publishing/corrigenda.htm*.

Résumé

La pandémie de COVID-19 a amplifié tous les aspects de la transformation numérique

Les mesures prises pour endiguer la pandémie de COVID-19 ont modifié en profondeur la relation aux technologies numériques des pays de l'OCDE. Jamais auparavant la dépendance mondiale à l'égard des technologies numériques n'avait à ce point concerné tous les aspects de la société – de l'éducation jusqu'à la santé. Le télétravail, l'apprentissage à distance et le commerce électronique ont explosé dans l'ensemble de la zone OCDE, tout comme l'adoption des outils numériques au sein des entreprises. Pouvoirs publics, entreprises et milieux universitaires ont été prompts à mettre à profit le potentiel de l'intelligence artificielle (IA) pour lutter contre la crise et répondre aux besoins d'accès rapide, sûr et fiable aux données, à l'échelle nationale et par-delà les frontières. Le partage des données de la recherche et la collaboration au plan international ont atteint des niveaux sans précédent.

Pour autant, ces activités fondées sur l'Internet et gourmandes en bande passante requièrent une connexion de qualité et exposent au grand jour les fractures numériques existantes, renforçant la nécessité d'aborder la transformation numérique selon une approche plus inclusive. Avec l'accélération du recours au télétravail et au commerce électronique, la pandémie de COVID-19 a également créé des conditions propices aux cybercriminels. Les agences de sécurité numérique de la zone OCDE ont réagi sans délai en tirant la sonnette d'alarme et en apportant leur appui aux opérateurs d'activités critiques, en particulier dans le secteur de la santé. Elles ont été nombreuses à formuler des orientations pour la collecte, le traitement et le partage des données à caractère personnel dans le cadre du traçage des cas contacts et autres mesures mises en place.

Il est encore trop tôt pour prendre la pleine mesure des effets à plus long terme de la pandémie sur la transformation numérique. Cette étude offre un aperçu de la situation de l'économie numérique et du contexte dans lequel s'inscrit l'action des pouvoirs publics, afin de jeter des bases sur lesquelles les décideurs pourront s'appuyer pour façonner un avenir numérique plus solide et plus inclusif.

Les pays de l'OCDE renforcent leur approche stratégique de l'action publique en faveur de la transformation numérique

La transformation numérique a des effets complexes et interdépendants sur les économies et les sociétés et appelle par conséquent des approches plus stratégiques. Trente-quatre pays de l'OCDE se sont dotés d'une stratégie numérique nationale afin de renforcer la coordination de l'action publique aux plus hauts niveaux de l'État, le plus souvent au niveau du premier ministre ou de la chancellerie, ou disposent d'un ministère ou d'un organisme dédié. Cette approche stratégique est particulièrement manifeste dans le domaine des technologies émergentes : mi-2020, 24 pays de l'OCDE avaient défini une stratégie nationale en matière d'IA, l'accent étant mis sur l'adoption de l'IA et le développement des compétences connexes. Depuis 2017, de nombreux pays de l'OCDE ont mis au point des stratégies nationales en matière de 5G. De plus, la plupart disposent de stratégies de sécurité numérique complètes, bien qu'elles soient souvent séparées des plans numériques nationaux et rarement assorties d'un budget indépendant et d'outils d'évaluation.

La connectivité continue de s'améliorer dans les pays de l'OCDE

La transformation numérique ne saurait se faire sans un accès fiable à l'Internet, qui facilite les interactions entre les individus, les organisations et les machines. Les abonnements aux services de télécommunications continuent de progresser à un rythme soutenu : au cours des huit dernières années, la part de la fibre dans les abonnements au haut débit fixe a plus

que doublé dans la zone OCDE, et représentait pas moins de 50 % dans neuf pays membres. Au niveau des entreprises, les écarts en termes d'accès entre petites et grandes entreprises se sont resserrés partout dans la zone l'OCDE – 93 % des entreprises disposaient d'un accès haut débit en 2019. L'utilisation moyenne de données mobiles par abonnement a quant à elle quadruplé en quatre ans. Elle a atteint 4.6 Go par mois en 2018, tandis que les prix des forfaits haut débit mobile assortis d'un niveau d'utilisation élevé ont chuté d'environ 60 % entre 2013 et 2019. Enfin, en juin 2020, des services commerciaux 5G étaient disponibles dans certaines zones, dans 22 pays de l'OCDE. Pour continuer d'élargir l'accès au très haut débit à un prix abordable, les pays de l'OCDE prennent des mesures politiques et réglementaires destinées à garantir une gestion efficiente du spectre, faciliter le déploiement et l'accessibilité des réseaux de collecte et des réseaux dorsaux, et encourager les nouvelles formes de partage d'infrastructures.

L'utilisation de l'Internet a progressé, mais le fossé numérique demeure

L'adoption de l'Internet, par les individus comme les entreprises, continue de gagner du terrain, bien que des écarts subsistent en termes de capacités et d'utilisation efficace. En 2019, dans les pays de l'OCDE, 70 % à 95 % des adultes utilisaient l'Internet ; pour ce faire, le smartphone est devenu l'appareil de prédilection. Par ailleurs, les individus passent plus de temps dans le cyberespace, l'utilisation quotidienne dans la zone OCDE ayant progressé en moyenne de 30 minutes au cours de la période 2014-19. En revanche, les différences d'utilisation selon les classes d'âge ou le niveau d'instruction subsistent. Par exemple, seuls 58 % des personnes âgées de 55 à 74 ans utilisaient l'Internet fréquemment en 2019 – contre 30 % en 2010 –, soit un taux très inférieur à celui des 16-24 ans, qui étaient près de 95 % à accéder quotidiennement à l'Internet.

En 2018, seuls 40 % des adultes des pays de l'OCDE présentant un niveau d'instruction faible ou n'ayant pas bénéficié d'un enseignement structuré utilisaient l'Internet pour interagir avec les administrations publiques, contre 80 % de ceux qui ont suivi des études supérieures.

Des écarts demeurent également entre les petites et les grandes entreprises. Par exemple, en 2019, le commerce électronique représentait 24 % du chiffre d'affaires des grandes entreprises, mais seulement 10 % de celui des structures de petite taille.

Les données massives créent certes de nouvelles opportunités pour les entreprises et les consommateurs, mais posent également de nouveaux défis en termes de sécurité et de protection de la vie privée

L'utilisation des données, qu'elles soient vendues à des tierces parties ou utilisées par les entreprises pour promouvoir ou adapter leurs propres produits, fait désormais partie intégrante des modèles économiques. En moyenne 12 % des entreprises de la zone OCDE avaient recours à l'analytique des données massives en 2017 – ce taux grimpe à 33 % dans les grandes entreprises. Les médias sociaux étaient la principale source des données utilisées par la moitié des entreprises concernées.

Les technologies à forte intensité de données, telles l'IA et l'Internet des objets (IdO), permettent d'offrir un plus large choix aux consommateurs et des possibilités de personnalisation. Dans le même temps, elles créent de nouveaux risques en termes de sûreté, de sécurité et de protection de la vie privée, et pourraient pénaliser les groupes défavorisés (notamment les femmes et les minorités ethniques). En 2019 déjà, plus de 80 % des pays de l'OCDE considéraient l'IA et l'analytique des données massives comme les principales sources de difficultés liées à la protection de la vie privée et des données à caractère personnel, suivies de près par l'IdO et la biométrie.

Dans ce contexte, les pouvoirs publics prennent des mesures pour mieux faire connaître les cadres de protection de la vie privée et des données et renforcer le contrôle de leur mise en œuvre, tout en promouvant la transparence des responsables du traitement des données. Les pays de l'OCDE cherchent par ailleurs des solutions pour gérer les questions de sécurité numérique et favoriser l'adoption de bonnes pratiques dans ce domaine. Ces efforts revêtent une importance d'autant plus cruciale que les économies et les sociétés se tournent massivement vers l'environnement numérique.

Chapitre 2

ÉVOLUTION DE L'ACTION DES POUVOIRS PUBLICS

PRINCIPAUX CONSTATS

- Les pays de l'OCDE renforcent leur approche stratégique de l'action publique liée à la transformation numérique.
- Les stratégies numériques nationales sont de plus en plus souvent coordonnées aux plus hauts niveaux de l'État. Par rapport à 2016, en 2019, cinq pays supplémentaires ont fait état d'une coordination au niveau du premier ministre ou de la chancellerie, et ils étaient légèrement plus nombreux à disposer d'un ministère dédié aux questions numériques.
- Au cours des trois dernières années, de nombreux pays, dont l'Allemagne, l'Australie, l'Autriche, la Colombie, la Corée, l'Espagne, les États-Unis, la France et le Royaume-Uni, ont adopté des stratégies nationales en matière de 5G.
- Tous les pays de l'OCDE et plusieurs économies partenaires ont amélioré l'accès aux données du secteur public et leur partage. Seule une poignée de pays (l'Allemagne, l'Australie, les États-Unis, le Japon et Singapour) ont également lancé des initiatives en vue de faciliter le partage des données au sein du secteur privé.
- L'innovation en matière de sécurité numérique apparaît comme une tendance émergente dans la zone OCDE. Plusieurs pays membres, dont l'Allemagne, l'Australie, la France, Israël et le Royaume-Uni, ont créé des centres d'innovation ouverte afin d'en promouvoir le développement.
- Mi-2020, plus de 60 pays disposaient d'une stratégie nationale en matière d'intelligence artificielle (IA). Ces stratégies ciblent différents domaines prioritaires : la recherche et le développement (R-D) liés à l'IA (Canada, États-Unis, Commission européenne), l'adoption de l'IA (Allemagne, Corée, Finlande) et les compétences en matière d'IA (Australie, États-Unis, Finlande, Royaume-Uni).
- Partout dans le monde, la technologie du « *blockchain* » et l'informatique quantique suscitent un intérêt croissant de la part des pouvoirs publics. Plusieurs pays ont adopté une stratégie en matière de technologie du « *blockchain* » (l'Allemagne, l'Australie, la République populaire de Chine [ci-après dénommée « la Chine »], l'Inde et la Suisse). D'autres (la France, l'Italie) leur emboîtent le pas. Les États-Unis, la Chine et l'Union européenne arrivent en tête pour ce qui est des dépenses de R-D consacrées à l'informatique quantique.
- La gestion des effets socio-économiques de la pandémie de COVID-19 est devenue une priorité d'action dans le domaine du numérique. Pouvoirs publics, universités et entreprises des pays de l'OCDE (États-Unis, Royaume-Uni) ont rapidement mis en place des systèmes d'IA afin de prévoir et de suivre la propagation de l'épidémie et d'impulser la recherche médicale.
- Les autorités nationales chargées de la protection de la vie privée dans les pays de l'OCDE, ainsi que le Comité européen de la protection des données et le Conseil de l'Europe, ont formulé des orientations sur la collecte, le traitement et le partage des données à caractère personnel dans le cadre de la crise du COVID-19.
- Les agences de sécurité numérique dans des pays comme le Canada, les États-Unis et la République tchèque ont pris, face à la crise du COVID-19, des mesures de sensibilisation, de suivi des menaces et d'assistance.
- Tous les pays de l'OCDE disposent de politiques destinées à favoriser l'adoption du numérique par les entreprises, en particulier les start-ups, et la création de nouvelles entreprises.
- Certains pays ont étendu les droits établis par les conventions collectives (ainsi du Canada, du Danemark et de la France). D'autres envisagent d'introduire un salaire minimum (Pays-Bas, Royaume-Uni) pour les travailleurs des plateformes numériques, qui ont été les plus durement touchés par la crise économique.

Introduction

Les pouvoirs publics s'appuient sur des stratégies numériques nationales pour façonner le processus de transformation numérique dans leur pays. Ces stratégies fixent les priorités d'action, les objectifs et les modalités de mise en œuvre. Leur mise au point devrait donc se faire en concertation avec des représentants d'un large éventail de groupes de parties prenantes[1] et de différents services de l'État, y compris au niveau local. À l'heure actuelle, la quasi-totalité des pays de l'OCDE et de nombreuses économies partenaires ont adopté de telles stratégies.

La première section de ce chapitre analyse les évolutions récentes des stratégies numériques nationales à partir des réponses au Questionnaire de 2019 de l'OCDE sur les politiques de l'économie numérique reçues des 37 pays membres de l'OCDE[2] et de quatre économies partenaires[3]. On y recense les principaux objectifs de l'action des pouvoirs publics, les évolutions et les avancées majeures, ainsi que les défis que pose l'élaboration de telles stratégies. On examine ensuite les diverses approches adoptées en matière de gouvernance des stratégies numériques nationales. La deuxième section expose les principales évolutions liées aux politiques propres à certains domaines, décrites plus en détail dans les chapitres thématiques. Ces politiques sont centrées sur la connectivité, l'utilisation du numérique, la gouvernance des données, la sécurité, la protection de la vie privée, l'innovation, le travail et des technologies clés telles que l'intelligence artificielle (IA), la technologie du « *blockchain* » et l'informatique quantique.

Stratégies numériques nationales

Un nombre croissant de pays se dotent de stratégies numériques nationales

La plupart des pays de l'OCDE et des économies partenaires ont défini une stratégie numérique nationale. Sur les 37 pays ayant répondu au Questionnaire de 2019 de l'OCDE sur les politiques de l'économie numérique, 34 disposaient d'une stratégie numérique nationale globale, qu'ils avaient pour la plupart mise en place en 2018. Faisaient exception la Pologne, qui ne dispose pas de stratégie ; le Mexique, dont la stratégie numérique nationale est en cours d'élaboration ; et les États-Unis, qui fondent leur politique numérique globale sur une approche décentralisée, axée sur le marché[4].

Au total, 27 pays se sont appuyés sur une stratégie préexistante pour bâtir leur stratégie numérique actuelle. Ceux dont la stratégie est délimitée dans le temps ont opté pour des périodes de quatre à six ans.

La plupart des pays pour lesquels on dispose de données ont indiqué avoir adossé leur stratégie numérique nationale à un budget. Certains ont inscrit leur stratégie dans un cadre plus large (Royaume-Uni), tandis que d'autres ont opté pour une approche décentralisée (Autriche, Costa Rica).

La moitié des pays a défini une stratégie dédiée au numérique, l'autre moitié l'a intégrée dans une stratégie nationale plus large (une stratégie nationale d'innovation, par exemple). En outre, 19 pays ont aligné leur stratégie numérique nationale sur un programme supranational. Tel est le cas de la plupart des pays européens membres de l'OCDE, qui ont fondé leur stratégie sur les principes et objectifs de la Stratégie numérique pour l'Europe (Commission européenne, 2010[1]), de la Stratégie pour un marché unique numérique en Europe (Commission européenne, 2015[2]), de la stratégie Europe 2020 (Commission européenne, 2010[3]), du plan d'action européen pour l'administration en ligne (Commission européenne, 2016[4]), ou sur une combinaison de ces différents programmes.

Les pays affichent les mêmes priorités pour ce qui est des politiques de l'économie numérique

Comme en 2016, les pays ont été invités, dans le cadre du Questionnaire de 2019 de l'OCDE sur les politiques de l'économie numérique, à classer leurs objectifs d'action par ordre de priorité. En 2019, ils devaient toutefois attribuer une valeur unique à chaque priorité. Des pays comme le Japon, le Royaume-Uni ou la Suède ont indiqué que leur stratégie numérique nationale ne leur permettait pas d'opérer une telle distinction.

Les résultats ci-dessous concernent les pays qui ont été en mesure d'établir un classement. Si ce dernier a quelque peu évolué au cours des dernières années, certains objectifs demeurent hautement prioritaires dans la plupart des pays (Tableau 2.1.). C'est le cas de l'objectif « Renforcer l'administration numérique », classé en tête des priorités en 2016 comme en 2019. L'objectif « Développer les infrastructures de télécommunications » figure en deuxième position également dans les deux cas. De même, de nombreux pays continuent d'accorder une grande importance au développement des compétences nécessaires à la transformation numérique. En revanche, l'objectif « Stimuler l'innovation dans les technologies numériques » est devenu une priorité d'action en 2019.

Tableau 2.1. Évolution des objectifs des politiques en matière de numérique, 2016 et 2019

Objectif	Priorité en 2016 (position dans le classement)	Priorité en 2019 (position dans le classement)	Nombre de stratégies numériques nationales mentionnant cet objectif
Renforcer l'administration numérique	1	**1**	26
Développer les infrastructures de télécommunications	2	**2**	26
Stimuler l'innovation dans les technologies numériques	-	**3**	25
Développer les compétences nécessaires à la transformation numérique	3	**4**	25
Renforcer la sécurité numérique	4	**5**	21
Améliorer la gouvernance des données	5	**6**	10
Promouvoir l'adoption du numérique par les entreprises	6	**7**	19
Promouvoir l'adoption du numérique par les individus	-	**8**	22
Améliorer la protection des consommateurs dans l'environnement numérique	8	**9**	2
Améliorer la gouvernance de l'Internet	7	**10**	3

Note : Les classements sont établis d'après les priorités déclarées par 35 pays en 2016 et 31 pays en 2019. Le questionnaire de 2016 mentionnait huit objectifs ; les objectifs « Stimuler l'innovation dans les technologies numériques » et « Promouvoir l'adoption du numérique par les individus » n'y figuraient pas.

Source : OCDE, questionnaires de 2017 et 2019 de l'OCDE sur les politiques de l'économie numérique.

Le renforcement de la sécurité numérique, l'amélioration de la gouvernance des données et la promotion de l'adoption du numérique par les entreprises figurent en milieu de classement, en 2016 comme en 2019. Les priorités les moins élevées ont été attribuées à la promotion de l'adoption du numérique par les individus, l'amélioration de la protection des consommateurs dans l'environnement numérique et l'amélioration de la gouvernance de l'Internet, ce dernier objectif affichant la plus forte chute dans le classement. Les répondants considèrent que, pour la plupart des objectifs indiqués en 2019, les priorités devraient rester les mêmes au cours des trois à cinq prochaines années, à deux exceptions près : le développement des compétences nécessaires à la transformation numérique et l'amélioration de la gouvernance des données devraient en effet gagner en importance.

Le classement de 2019 des priorités par ordre décroissant reflète peu ou prou le nombre de mentions de ces objectifs dans les stratégies numériques nationales des différents pays (Tableau 2.1, colonne 3). Par exemple, les trois objectifs arrivant en tête du classement des priorités – à savoir « Renforcer l'administration numérique », « Développer les infrastructures de télécommunications » et « Stimuler l'innovation dans les technologies numériques » – sont ceux qui sont le plus souvent mentionnés dans les stratégies nationales – à 26, 26 et 25 reprises, respectivement. Même constat pour les deux derniers du classement des priorités – « Améliorer la protection des consommateurs dans l'environnement numérique » et « Améliorer la gouvernance de l'Internet » –, qui sont également les objectifs qui reviennent le moins dans les stratégies nationales (cités respectivement à deux et trois reprises).

Outre les objectifs énumérés dans le questionnaire de l'OCDE, certaines stratégies numériques nationales accordent de l'importance à d'autres priorités. Par exemple, la problématique de l'égalité femmes-hommes est un objectif mentionné explicitement dans la Stratégie numérique du Brésil (MCTIC, 2018[5]), qui souligne la nécessité de favoriser l'inclusion et la promotion des femmes et des filles dans les domaines liés aux TIC. En Turquie, la Stratégie et le Plan d'action nationaux en faveur de l'administration électronique (Informatics and Information Security Research Center, 2016[6]) lient la transition vers une société de l'information aux Objectifs de développement durable de l'ONU.

Défis liés à la mise en œuvre des objectifs énoncés dans les stratégies numériques nationales

Les pays de l'OCDE et les économies partenaires ont indiqué être confrontés à diverses difficultés dans le cadre de la réalisation des objectifs énoncés dans leurs politiques en matière de numérique. La liste ci-dessous énumère les principaux défis signalés par 22 pays en 2019 :

- Dispersion géographique de la population, notamment dans les zones reculées et rurales ;
- Contraintes budgétaires et financières ;
- Coordination et interactions des acteurs à l'échelle des différents secteurs, ministères et organismes ;

- Élaboration d'instruments et de cadres réglementaires efficaces ;
- Adaptation au rythme rapide de développement et d'évolution des technologies numériques ;
- Équilibre entre la nécessité de stimuler l'innovation et celle de gérer les préoccupations des consommateurs en matière de sécurité et de protection de la vie privée, liées à l'utilisation des données et à l'adoption des nouvelles technologies numériques.

Certains de ces défis, tels que la quête d'un équilibre entre l'innovation et les préoccupations des consommateurs en termes de sécurité et de protection de la vie privée, peuvent être réduits au minimum en mettant l'accent sur la cohérence et la coordination des politiques à l'échelle des différents domaines et secteurs qui façonnent la transformation numérique (OCDE, 2020[7]). D'autres, tels que l'adaptation au rythme rapide de développement et d'évolution des technologies numériques, peuvent être gérés en utilisant les technologies numériques dans le processus inhérent aux politiques (pour la conception, la mise en œuvre et le suivi, par exemple) (OCDE, 2019[8]).

Approches en matière de gouvernance des stratégies numériques nationales

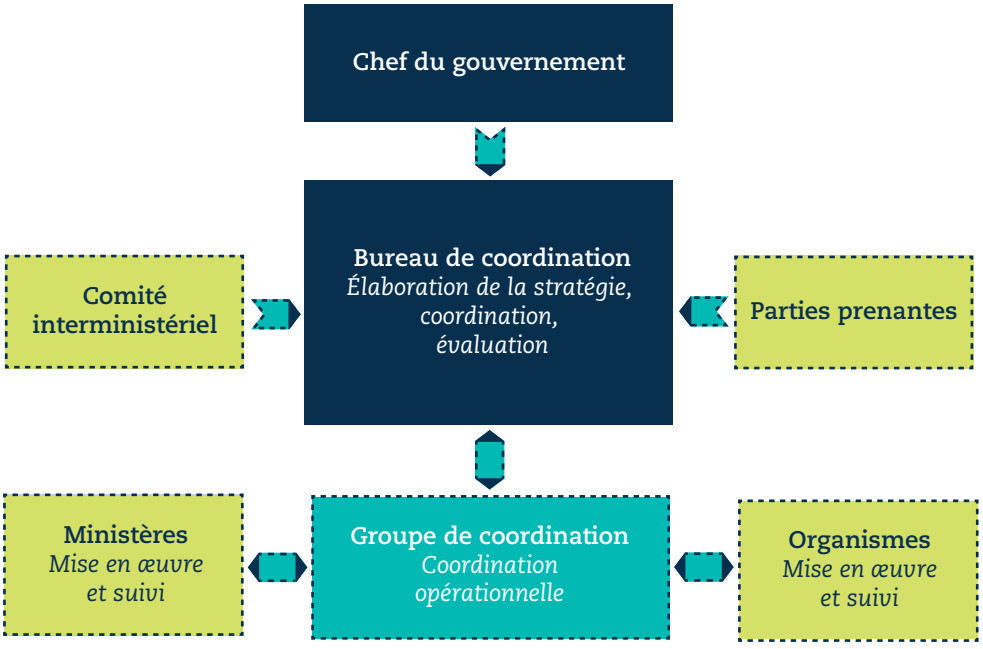
Cette section expose les approches les plus couramment adoptées pour la gouvernance des stratégies numériques nationales dans les pays membres de l'OCDE et les économies partenaires. Cette gouvernance concerne l'élaboration, la mise en œuvre, le suivi et l'évaluation des stratégies, la répartition des responsabilités entre les différents organismes et acteurs qui prennent part à ces activités, et les dispositifs mis en place pour garantir une coordination efficace.

Si l'ensemble des pays membres de l'OCDE et des économies partenaires disposant d'une stratégie numérique nationale ont pris des mesures pour en assurer la gouvernance, les modalités précises varient. Les diverses approches peuvent être le reflet de disparités au niveau des institutions nationales, de l'organisation des pouvoirs publics, ou de la culture et des capacités administratives. En outre, les dispositifs de gouvernance peuvent évoluer au fil du temps, sous l'effet, par exemple, des changements de gouvernements, des progrès technologiques, ou de l'évolution de la constellation d'acteurs clés du fait de la transformation numérique (OCDE, 2019[9]). Cela peut influer sur l'attribution des principales responsabilités, notamment celles liées à l'élaboration, la coordination, la mise en œuvre, le suivi et l'évaluation des stratégies.

On observe deux grands types d'approches. Dans le premier cas, les pays privilégient une direction à haut niveau et une centralisent la coordination stratégique à un échelon supra-ministériel (Graphique 2.1.). Un bureau de coordination placé sous la direction du président, du premier ministre ou de la chancellerie est alors généralement chargé d'élaborer la stratégie, en impliquant les principaux ministères et parties prenantes dans le processus. Ce bureau tend à être dirigé par un secrétaire d'État ou une personne assumant une fonction de même ordre. Dans la moitié environ des pays ayant opté pour cette approche, le bureau assure également la coordination stratégique. Dans d'autres, la coordination peut relever d'un organe exécutif dédié[5]. Les référents au sein de chaque ministère et organisme, par exemple les responsables du numérique, sont généralement chargés de la coordination opérationnelle de la stratégie. Ces ministères et organismes se chargent souvent aussi de suivre la mise en œuvre et de rapporter au bureau de coordination. Dans la plupart des cas, ce dernier assure l'évaluation de la stratégie, sous la supervision du chef du gouvernement (OCDE, 2019[9]).

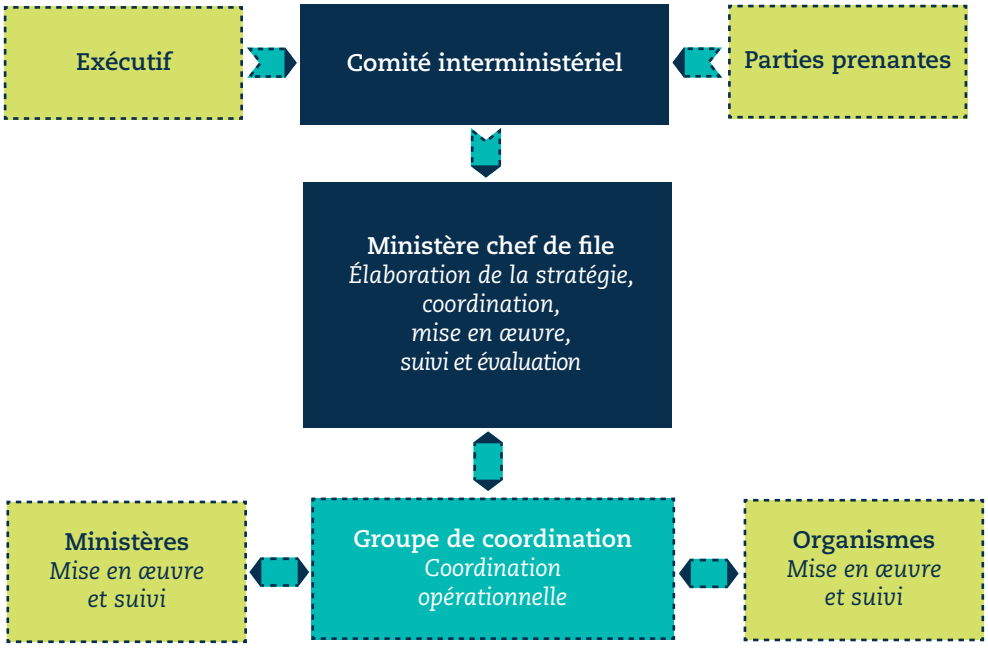
Dans le deuxième type d'approche, un ministère chef de file est généralement chargé d'élaborer la stratégie et d'assurer la coordination stratégique (Graphique 2.2.). L'efficacité de cette approche est souvent optimale lorsque le ministère chef de file est exclusivement chargé des questions numériques, plutôt que de différents portefeuilles. Les parties prenantes sont, en règle générale, associées à l'élaboration de la stratégie, sous les auspices par exemple d'un comité interministériel qui se réunit à l'invitation du ministère chef de file et est parfois présidé par le chef du gouvernement. Comme dans la première approche, la coordination opérationnelle est habituellement assurée par un groupe dédié, composé des référents des ministères et organismes chargés de la mise en œuvre. En général, ces ministères et organismes suivent aussi la mise en œuvre de la stratégie et en rendent compte au ministère chef de file et/ou au comité interministériel, lequel assure souvent l'évaluation globale de la stratégie. Dans la plupart des cas où le ministère chef de file est exclusivement chargé des questions numériques, celui-ci est également responsable du suivi et de l'évaluation (OCDE, 2019[9]).

Graphique 2.1. Coordination stratégique à haut niveau des stratégies numériques nationales



Source : OCDE (2019[9]), *Vers le numérique : Forger des politiques au service de vies meilleures*, https://doi.org/10.1787/7cba1873-fr.

Graphique 2.2. Coordination stratégique à l'échelon ministériel des stratégies numériques nationales



Source : OCDE (2019[9]), *Vers le numérique : Forger des politiques au service de vies meilleures*, https://doi.org/10.1787/7cba1873-fr.

Les informations recueillies par le biais du Questionnaire de l'OCDE sur les politiques de l'économie numérique confirment que ces deux grands types d'approches de la gouvernance continuent de co-exister, bien qu'ils aient évolué au cours des dernières années (OCDE, 2018[10]). Le Tableau 2.2.

donne un aperçu de la répartition des responsabilités liées à l'élaboration, à la coordination, à la mise en œuvre, au suivi et à l'évaluation des stratégies numériques nationales en 2016 et 2019.

Tableau 2.2. Gouvernance des stratégies numériques nationales

Nombre de pays ayant attribué les responsabilités citées

Entité responsable	Pilotage de l'élaboration de la stratégie		Contribution		Coordination		Mise en œuvre		Suivi		Évaluation
	2016	2019	2016	2019	2016	2019	2016	2019	2016	2019	2019
Cabinet du Premier ministre, Présidence, Chancellerie	4	**8**	0	**0**	5	**5**	1	**0**	6	**3**	**4**
Ministère ou organisme chargé exclusivement des questions numériques	8	**10**	1	**0**	10	**14**	3	**5**	8	**14**	**13**
Ministère ou organisme non dédié au numérique	15	**12**	2	**0**	13	**10**	1	**2**	11	**9**	**9**
Plusieurs ministères ou organismes	6	**3**	14	**9**	5	**4**	26	**15**	7	**7**	**4**
Plusieurs parties prenantes publiques et privées	1	**0**	17	**24**	0	**0**	3	**11**	0	**0**	**0**

Note : Les données pour 2016 sont basées sur les réponses de 35 pays à l'enquête. Celles pour 2019 sont fondées sur les réponses de 33 pays. L'Italie, la Hongrie et la Turquie n'ont pas fourni d'informations sur les responsabilités en matière d'évaluation. La catégorie « Plusieurs parties prenantes publiques et privées » regroupe les acteurs gouvernementaux et ceux de la société civile et du secteur privé.

Source : OCDE, questionnaires de 2017 et 2019 de l'OCDE sur les politiques de l'économie numérique.

Le nombre de pays ayant confié les responsabilités stratégiques à un organisme gouvernemental de haut niveau a doublé, passant de quatre à huit, entre 2016 et 2019. En revanche, l'organisme de haut niveau est responsable à la fois de l'élaboration de la stratégie et de la coordination stratégique dans seulement trois pays : le Chili, la Colombie et la Turquie. En Fédération de Russie, au Japon, au Luxembourg et en Suisse, la responsabilité du pilotage de l'élaboration de la stratégie incombe également à un organisme gouvernemental de haut niveau, mais la coordination stratégique est confiée à un ministère ou un organisme chargé exclusivement des questions numériques. Ces pays suivent des approches diverses pour ce qui est de la gestion du suivi et de l'évaluation de leur stratégie.

Dans la plupart des pays, un ministère ou un organisme unique continue de se charger de l'élaboration de la stratégie et de la coordination stratégique. Le plus souvent, cette entité gère un portefeuille qui s'étend au-delà des questions numériques pour couvrir d'autres domaines, comme l'économie, la science, l'innovation ou l'industrie. Les pays dotés d'un ministère ou d'un organisme dédié aux questions numériques sont l'Autriche, la Belgique, la Grèce, Israël, le Royaume-Uni, la Slovénie et la Suède. Dans ces pays, le ministère ou l'organisme chef de file dispose d'un solide mandat couvrant à la fois l'élaboration de la stratégie et la coordination stratégique. Il est en outre chargé d'assurer le suivi et l'évaluation de la stratégie. C'est également le cas en Espagne, sauf pour ce qui est de la coordination stratégique, gérée par plusieurs ministères.

Entre 2016 et 2019, la contribution de plusieurs ministères ou organismes à l'élaboration des stratégies a diminué, passant de 14 à 9. Cette tendance pourrait s'expliquer, au moins partiellement, par l'augmentation de la participation d'autres acteurs publics et privés (acteurs gouvernementaux, de la société civile et du secteur privé). Il s'agit là d'une évolution positive, la contribution de diverses parties prenantes étant un gage d'inclusivité et, par conséquent, de qualité pour une mise en œuvre réussie de la stratégie (OCDE, 2019[9]).

Suivi et évaluation des stratégies numériques nationales

Le suivi et l'évaluation sont essentiels pour vérifier si la stratégie est correctement mise en œuvre et si elle donne des résultats concluants. Pour ce faire, les pays s'appuient sur différentes méthodes comme des enquêtes comparatives, des rapports d'étapes et des bilans annuels ou semestriels, ou des tableaux de bord assortis de prévisions.

Selon les résultats du Questionnaire de 2019 de l'OCDE sur les politiques de l'économie numérique, tous les pays pour lesquels on dispose de données suivent l'avancement de la mise en œuvre de leur stratégie numérique nationale, et ils sont 24 à avoir défini des objectifs précis au regard desquels ils mesurent les progrès faits. Le Japon, par exemple, a fixé des objectifs de réduction des coûts d'exploitation des systèmes d'information, tandis que l'Estonie, la Finlande, la Norvège et la Suède ont défini des objectifs ambitieux en matière d'accélération du débit Internet. D'autres encore ont établi des cibles d'amélioration du développement du commerce électronique (Lettonie) ou de création de start-ups (Belgique).

La plupart des pays utilisent en outre les indicateurs et tableaux de bord internationaux pour mesurer leurs progrès au regard des objectifs d'action énoncés dans les stratégies numériques nationales. Ils se tournent pour ce faire vers les indicateurs fournis par les Perspectives de l'économie numérique de l'OCDE, la Boîte à outils de l'OCDE sur la transformation numérique, l'indice de l'Union européenne relatif à l'économie et à la société numériques, l'enquête de l'ONU sur l'administration électronique, ou encore l'indice de la compétitivité mondiale du Forum économique mondial. En République tchèque, le Comité interministériel pour la société de l'information mène à intervalles réguliers une enquête comparative à partir d'un ensemble d'indicateurs de performance destinés à évaluer la maturité et les résultats de chaque entité prenant part à la stratégie numérique nationale.

Au-delà du suivi et de l'évaluation de la réalisation des objectifs et des cibles propres aux stratégies numériques nationales, il peut également être intéressant pour les pays de mesurer les effets de la réalisation des objectifs énoncés dans ces stratégies sur les objectifs nationaux à plus haut niveau, notamment en termes de croissance, de productivité et d'innovation. En Islande, par exemple, les initiatives lancées dans le cadre de la stratégie *Digital Iceland* servent également les objectifs de la stratégie financière du pays (Ministère des Finances et des Affaires économiques, 2019[11]). Au Japon, la Quatrième révolution industrielle telle qu'envisagée dans la nouvelle stratégie du pays en matière de technologies de l'information, devrait, avec le développement de l'Internet des objets (IdO), du «*big data* » et de l'IA, contribuer à la croissance du produit intérieur brut (PIB) nominal au cours des prochaines années. De même, en Fédération de Russie, plus de la moitié de la croissance du PIB d'ici à 2030 devrait provenir des gains d'efficience et de compétitivité liés à l'adoption des technologies numériques à grande échelle.

Principales évolutions de l'action des pouvoirs publics

Cette section présente les principales évolutions de l'action des pouvoirs publics dans différents domaines de l'économie numérique, de la connectivité à l'utilisation du numérique, en passant par la gouvernance des données, la sécurité, la protection de la vie privée, l'innovation, le travail ou encore les technologies clés (IA, technologie du « *blockchain* » et informatique quantique). Une vision approfondie de chacun de ces domaines est exposée dans les chapitres thématiques.

Accès et connectivité

Au cours des dernières années, décideurs et régulateurs se sont attachés à adapter leurs cadres réglementaires en vue de stimuler la concurrence, l'innovation et l'investissement dans les marchés des télécommunications (chapitre 3).

La crise économique et sanitaire liée à la COVID-19 a renforcé le caractère essentiel de la connectivité en ce qu'elle a permis aux activités économiques de se poursuivre à distance. Les inégalités d'accès aux services de communication à l'échelle local comme internationale étant susceptibles d'aggraver les conséquences de la crise du COVID-19, il est crucial de mettre en œuvre des politiques visant à réduire les fractures numériques. Il en va de même pour la réglementation et les politiques favorisant la concurrence et l'investissement dans les infrastructures de communication, qui jouent un rôle encore plus déterminant. De fait, à moyen et long termes, la mise à niveau des réseaux vers la nouvelle génération de haut débit fixe et sans fil aidera à assurer une connectivité fiable et résiliente à tous les usagers.

Les marchés des télécommunications évoluent avec notamment une certaine tendance à converger qui a conduit certains pays, à l'image de l'Allemagne, de la Colombie et de la Finlande, à modifier les missions et les responsabilités des régulateurs compétents. D'autres, tels l'Italie et le Royaume-Uni,

ont profité de l'évolution de leurs réseaux et services historiques, notamment des réseaux fixes cuivre, pour adapter leurs cadres réglementaires.

Certains pays de l'OCDE, dont l'Allemagne, l'Autriche, la Corée et la France, tendent à compléter les outils réglementaires traditionnels par des réglementations fondées sur des données réelles. Les données relatives à la qualité des réseaux, par exemple, incitent les opérateurs à s'autoréguler et à améliorer leurs réseaux.

Par ailleurs, les pays de l'OCDE cherchent des moyens d'étendre et d'améliorer l'accès aux réseaux par le biais de politiques destinées à réduire les coûts de déploiement du haut débit. Ils mènent à ce titre des travaux favorisant le partage d'infrastructures et le co-investissement ainsi que des politiques dites de « dig-once », qui consistent à coordonner les travaux d'excavation afin de minimiser les coûts de déploiement.

Le partage d'infrastructures passives est devenu courant dans les pays de l'OCDE – l'Australie, la Corée, la France et la Suisse y ont recours. Les exemples de partage d'infrastructures actives se multiplient également. Dans cette optique, certains états ont conclus des accords de partage de réseau d'accès radio (Allemagne, Espagne, France, République tchèque, Suède, Suisse) ou d'itinérance nationale (Colombie, France).

Plusieurs pays de l'OCDE se sont concentrés sur les politiques de partage d'infrastructures de type « dig-once ». L'objectif est de se servir de projets d'infrastructure dans d'autres domaines que le haut débit (réseaux publics d'eau ou d'énergie, éclairage public, construction de routes ou d'autoroutes, etc.) afin de réduire les coûts de déploiement des réseaux haut débit. Par exemple, les pays membres de l'Union européenne (UE) avaient jusqu'à janvier 2016 pour transposer la Directive relative à des mesures visant à réduire le coût du déploiement de réseaux de communications électroniques à haut débit (2014/61/UE) dans leur législation nationale. La Directive contient notamment des dispositions visant à autoriser les opérateurs de réseaux de communications à accéder aux infrastructures d'autres entreprises de réseau. La Suisse a également pris des mesures allant dans le même sens.

Sur les marchés mobiles, les pays de l'OCDE continuent de concentrer leurs efforts sur la gestion efficiente du spectre afin de favoriser le déploiement des réseaux sans fil de nouvelle génération. Les attributions de spectre pour les services d'accès sans fil se sont multipliées dans la zone OCDE depuis 2016. Les 15 pays qui ont procédé à de telles attributions sont l'Allemagne, l'Autriche, le Canada, le Chili, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, l'Irlande, l'Italie, la Lettonie, le Royaume-Uni, la Suède et la Suisse.

La « densification des réseaux » nécessaire au déploiement de la 5G aura d'importantes répercussions techniques, réglementaires et politiques pour tous les niveaux d'administration – y compris les municipalités –, pour les secteurs privé et public. Plusieurs pays de l'OCDE, dont les États-Unis et le Royaume-Uni, ont entrepris de rationaliser les droits de passage pour faciliter cette densification. D'autres, comme la Corée, l'Irlande et la Suède, ont adopté des politiques visant à améliorer la connectivité aux réseaux de collecte et aux réseaux dorsaux.

Au cours des trois dernières années, de nombreux pays, dont l'Allemagne, l'Australie, l'Autriche, la Colombie, l'Espagne, la France et le Royaume-Uni, ont adopté des stratégies nationales en matière de 5G. L'Union européenne a lancé plusieurs initiatives en la matière, à l'image du « Plan d'action pour la 5G » et du partenariat public-privé 5G-PPP pour l'infrastructure. La Corée a adopté une stratégie complète, intitulée « 5G+ » afin de promouvoir la mise en place d'un « écosystème 5G » dans lequel la 5G constitue l'infrastructure sous-jacente permettant la connexion d'appareils perfectionnés et de services innovants. Aux États-Unis, la Federal Communications Commission (FCC) a défini une stratégie exhaustive destinée à « asseoir la supériorité de l'Amérique en matière de technologie 5G », dénommée « 5G FAST Plan ».

La quasi-totalité des pays de l'OCDE ont fixé des objectifs chiffrés d'accès au haut débit. À cela s'ajoutent, dans certains cas, des objectifs d'utilisation. La Corée, par exemple, a l'objectif le plus élevé en termes de débit descendant : 10 gigabits par seconde (Gbit/s) pour 50 % des ménages urbains d'ici à 2022. Le Luxembourg entend offrir un débit de 1 Gbit/s à l'ensemble des ménages d'ici à 2020. Arrive ensuite la Suède, qui s'est fixé pour objectif de connecter 98 % des ménages et des entreprises à un réseau offrant

un débit de 1 Gbit/s d'ici à 2025, tandis que l'Autriche vise, sur l'ensemble de son territoire, un débit de 1 Gbit/s sur ses réseaux haut débit fixe comme mobile, d'ici à 2030. Le Canada a pour objectif d'offrir à 90 % des Canadiens des débits descendants de 50 mégabits par seconde (Mbit/s) à l'horizon 2021. D'ici à 2020, les États-Unis entendent fournir un débit d'au moins 100 Mbits/s à 80 % des ménages, tandis que la Norvège a un objectif de même ordre pour 90 % des ménages.

Un nombre croissant de pays de l'OCDE ont modifié leur cadre juridique de manière à inclure le haut débit dans leur cadre de service universel. La Suisse a été la première à montrer la voie, suivie de l'Australie, de la Belgique, du Canada, de l'Espagne, de la Finlande et de la Suède, pour ne citer que quelques exemples. En Corée, le haut débit fixe a été désigné en tant que service universel en 2020.

Plusieurs politiques ont été adoptées en vue de faciliter l'entrée sur le marché et de réduire les coûts de transfert pour l'Internet des Objets (IdO). L'Italie, par exemple, a autorisé l'utilisation extraterritoriale de ressources de numérotation pour l'IdO, établissant par là même un cadre réglementaire clair pour les cartes SIM qui équipent les véhicules connectés. Les États membres de l'UE pourraient autoriser l'utilisation extraterritoriale de ressources nationales de numérotation, notamment certains numéros non géographiques, ce qui pourrait permettre de créer de nouvelles perspectives de développement pour les communications de machine à machine (M2M).

Au cours des dernières années, certains pays et territoires ont revu leurs cadres législatifs autour de la neutralité des réseaux. Ainsi l'Union européenne, a réexaminé sa législation sur l'accès à un Internet ouvert (2015/2120) et publié un rapport sur sa mise en œuvre en avril 2019. L'Organe des régulateurs européens des communications électroniques a entrepris de revoir ses Lignes directrices pour la mise en œuvre par les régulateurs nationaux des règles européennes en matière de neutralité de l'Internet. Le Japon a lancé des discussions sur la neutralité des réseaux ; le groupe d'étude dédié, mis en place par le ministère des Affaires intérieures et des Communications, a publié un rapport sur le sujet en 2019. Aux États-Unis, la FCC a adopté en 2017 le décret *Restoring Internet Freedom Order* établissant une approche réglementaire plus modérée. Entre autres changements, le décret classe les services d'accès à l'Internet haut débit dans la catégorie des services d'information, met fin à certaines obligations de reporting et autorise la Federal Trade Commission à superviser les pratiques des fournisseurs d'accès à l'Internet en matière de protection de la vie privée.

Les pays cherchent par ailleurs à encourager l'adoption du protocole IPv6. Pour ce faire, ils mettent en place des programmes incitant à mettre à niveau les services Internet, adaptent les achats publics en conséquence et/ou invitent des groupes de réflexion multipartites à favoriser le déploiement du protocole IPv6. Par exemple, en 2019, la Suède a suivi la recommandation formulée par l'OCDE dans son Examen de la situation du pays au regard de la transformation numérique et alloué au régulateur des communications des fonds destinés à la promotion du déploiement d'IPv6.

Adoption et utilisation du numérique

Ménages et individus

Sur les 30 pays ayant répondu aux questions relatives à l'adoption et à l'utilisation des technologies numériques dans le Questionnaire de 2019 de l'OCDE sur les politiques liées au développement de l'économie numérique, la quasi-totalité a indiqué disposer de politiques promouvant explicitement l'utilisation des technologies numériques par les ménages et les individus (chapitre 4). Seuls quatre pays faisaient exception : l'Allemagne, l'Espagne, l'Italie et les Pays-Bas.

Les objectifs visés par les pouvoirs publics varient considérablement selon les pays, allant de la réduction de la fracture numérique au développement des compétences et de la culture numériques, en passant par l'amélioration de la connectivité, le renforcement de la cybersécurité et de la confiance, ou encore l'amélioration de l'efficience de l'administration électronique.

Il n'est pas rare que ces politiques ciblent des groupes spécifiques au sein de la population. Ceux qui reviennent le plus fréquemment sont les enfants (Japon, Portugal, République tchèque), les étudiants (Colombie, Singapour), les personnes âgées (Australie, Autriche, Japon), les ménages modestes (Costa Rica, Singapour) ou les personnes handicapées (Costa Rica, Israël, Japon).

Les aides non financières sont généralement l'instrument privilégié pour promouvoir l'utilisation des technologies numériques par les ménages et les individus. En particulier, les portails ou les plateformes officiels fournissent un espace virtuel propice au partage d'expérience (Corée, Japon), à l'exécution de campagnes de sensibilisation (Colombie, Danemark, Mexique, Portugal) et aux activités de formation (Singapour). La cybersécurité, la confiance et la protection des consommateurs sont des sujets d'intérêt courants.

Les aides financières directes sont versées par les organismes chefs de file chargés de gérer la mise en œuvre des programmes, ou l'octroi de prêts, de subventions, de bons ou du financement de formations spécifiques. Ces aides ciblent les programmes visant à réduire la fracture numérique, dans toutes ses dimensions, qu'il s'agisse d'augmenter le débit et l'accessibilité des réseaux (Australie, Colombie, Estonie, États-Unis, Finlande Singapour, Suède) ou de favoriser le développement des compétences numériques (Fédération de Russie, Portugal). Dans certains pays (Costa Rica, Estonie, États-Unis), ces programmes bénéficient également d'aides financières indirectes.

Les aides financières indirectes sont souvent apportées dans le domaine de l'éducation. Certains pays s'attachent à améliorer le système éducatif (Portugal, République tchèque), d'autres à promouvoir les progrès technologiques (Fédération de Russie), d'autres encore, à développer les compétences numériques des étudiants et des enseignants (Danemark). En Autriche, le coût des services publics au niveau fédéral est réduit lorsque la demande de tels services est transmise par voie électronique.

Les pays ont recours à la réglementation et aux dispositions législatives pour jeter les bases juridiques dans un large éventail de domaines, principalement ceux de la protection des consommateurs (Mexique, Turquie) ; de la protection des données à caractère personnel (Portugal, Singapour) ; de la sécurité numérique (Autriche, Danemark) ; de l'administration électronique (Australie, Japon) et de la santé en ligne (Lettonie).

Entreprises

Sur les 30 pays ayant répondu au Questionnaire sur les politiques de l'économie numérique, tous sauf trois (les États-Unis, l'Italie et le Royaume-Uni) ont indiqué disposer de politiques visant à promouvoir l'utilisation des technologies numériques par les entreprises.

Les objectifs visés par les pouvoirs publics varient considérablement. Certaines mesures ont pour but d'encourager l'adoption de technologies numériques favorisant des gains de productivité, d'autres de faciliter l'accès aux connaissances et aux compétences, ou de soutenir le développement de produits et de services sociaux innovants (dans le domaine de la santé en ligne, par exemple).

Les politiques axées sur le renforcement des compétences numériques et l'amélioration de de la connaissance et de l'adoption des technologies, ainsi que les campagnes de sensibilisation à la sécurité numérique et à la protection de la vie privée ciblent avant tout les petites et moyennes entreprises (PME).

Les aides financières directes sont généralement privilégiées. Elles prennent notamment la forme de subventions accordées aux entreprises qui adoptent les technologies numériques, telles que le « *cloud computing* » (Corée) ou le « *big data* » (Portugal), font appel à des services de conseil dans le domaine du numérique et développent les compétences des individus dans le domaine du numérique (Danemark, Slovénie). De nombreux pays font également état de subventions ou de bons destinés à soutenir les activités de recherche et de développement – R-D – (bien que ces dispositifs ne visent pas directement les technologies numériques). L'Allemagne, par exemple, a mis en place des aides directes ciblant le « *big data* » , les systèmes autonomes, la sécurité des technologies de l'information et les plateformes de services.

Quant aux aides financières indirectes, elles se présentent sous plusieurs formes. Le Brésil et le Japon, par exemple, ont recours à des crédits d'impôts ou des allègements fiscaux en faveur des investissements dans les TIC. D'autres pays proposent des aides fiscales plus larges en faveur de la R-D ; celles mises en place en Fédération de Russie ciblent explicitement les technologies numériques.

Des aides non financières sont proposées sous diverses formes. L'Australie, la Lituanie, Singapour et la Suède fournissent aux entreprises des avis et des services de conseil adaptés à leurs besoins. La Turquie offre pour sa part des conseils sur les réglementations applicables aux nouveaux modèles économiques. La Lettonie et la Norvège proposent des formations, tandis que le Portugal et la Slovénie encouragent le partage d'expérience et le mentorat.

Les pays font appel à des dispositions réglementaires et législatives pour jeter les bases juridiques dans un large éventail de domaines, de la cybersécurité (République tchèque) aux Fintech (Mexique), en passant par les dispositifs de signature électronique (Chili) et la facturation électronique dans le cadre des marchés publics (Autriche, Norvège). Certains ont également entrepris de formuler des principes directeurs pour la réglementation des nouveaux modèles économiques reposant sur les technologies numériques (Danemark).

Administration numérique

Au cours des dernières décennies, des réformes de grande ampleur du secteur public ont permis d'accroître l'efficience et l'efficacité des services publics en mettant à profit la transformation numérique. Dans le cadre de ces efforts, les administrations ont investi massivement dans de nouvelles pratiques et ont modernisé les services afin de mieux répondre aux besoins des citoyens. En particulier, des plateformes de services en ligne communes à plusieurs organismes du secteur public ont été mises en place pour simplifier les procédures administratives et améliorer les interactions avec les citoyens.

La plupart des pays de l'OCDE ont confié la responsabilité des stratégies en matière d'administration numérique aux autorités centrales ou fédérales, comme le montrent les résultats de l'édition 2019 de l'Enquête de l'OCDE sur l'administration numérique. Ils sont également nombreux à avoir créé des organismes dédiés, dotés de degrés de responsabilité divers en matière de conseil et de prise de décision. Ces organismes ont un mandat particulièrement large au Canada, en Corée, en Islande, en Israël, au Luxembourg et en République tchèque, tandis que leur champ d'action est plus restreint en Belgique et en Suède.

Selon la même enquête, 22 pays de l'OCDE, auxquels s'ajoute le Brésil, utilisent un modèle type pour la gestion des projets liés aux TIC. De plus, 22 ont adopté une approche axée sur des analyses de rentabilité, fondées sur l'évaluation du rapport coûts-avantages et/ou coûts-efficacité. En outre, 24 pays disposent d'une stratégie spécifique pour les achats de TIC par le secteur public, tandis que 10 autres ont défini une stratégie d'approvisionnement couvrant l'ensemble de l'administration pour les achats de TIC. Seuls 12 des 31 pays de l'OCDE pour lesquels on dispose de données ont adopté les trois types de moyens d'action (gestion des projets TIC, approche fondée sur des analyses de rentabilité et stratégie en matière d'achats TIC) dans le cadre de leur stratégie d'administration numérique.

Compétences

Au cours des dernières années, plusieurs pays ont adapté les programmes scolaires à l'évolution des compétences requises dans le cadre de la transformation numérique. En Australie, le cadre de développement des capacités en matière de TIC vise à développer les compétences numériques grâce à la mise en place de cours dédiés aux TIC, ainsi que via d'autres domaines d'apprentissage. Au Canada, plusieurs gouvernements provinciaux ont adopté une approche globale des compétences numériques. En République tchèque, la Stratégie en faveur de l'éducation numérique pour 2020 vise à ouvrir l'éducation à de nouveaux modes d'apprentissage par le biais des technologies numériques et à améliorer les compétences des élèves dans les domaines des TIC et de la pensée computationnelle. La France a introduit il y a peu des cours obligatoires portant sur le numérique et les sciences informatiques pour les élèves du secondaire. La Suède a modifié ses programmes scolaires de manière à renforcer les compétences numériques des élèves, leurs connaissances générale du secteur des médias et de l'information, ainsi que leur sens critique vis-à-vis des différentes sources d'informations.

Depuis plus de dix ans, les pays de la zone OCDE s'attellent à la nécessité de renforcer les compétences en TIC des enseignants par le biais de diverses politiques. Pour ce faire, ils élaborent des plans nationaux en ce sens, ou mettent en place des formations obligatoires, des normes d'accréditation nationales ou une certification nationale des enseignants. Ainsi le Danemark a créé une « licence » volontaire attestant de l'acquisition de connaissances pédagogiques et de compétences de base en matière de TIC.

Au Portugal, le programme de formation des enseignants a pour objectif d'améliorer les compétences des enseignants, notamment dans le domaine du numérique.

De nombreux pays de l'OCDE ont mis en place des programmes axés sur la maîtrise du numérique afin de renforcer l'inclusion numérique, en particulier au sein des groupes les plus vulnérables (chapitre 4). En Autriche, par exemple, le Pacte de compétence numérique cible les jeunes actifs ; les personnes qui n'utilisent pas l'Internet ; les professionnels de plus de 45 ans ; et les personnes âgées. D'autres initiatives voient le jour ailleurs, telles le programme de citoyenneté numérique en Colombie ; le programme de développement des compétences numériques chez les personnes âgées, en Israël ; ou encore le projet Father's Third Son, en Lettonie, dans le cadre duquel les bibliothèques proposent des conseils sur l'utilisation des services en ligne et la navigation sans risque sur l'Internet. En Norvège, le programme « Inclusion numérique pour tous » s'adresse aux personnes âgées, aux femmes et aux immigrants. Au Portugal, l'initiative nationale en faveur des compétences numériques « e.2030 » aide les citoyens et les actifs à améliorer leurs compétences numériques. Enfin, le programme *Future Digital Inclusion Programme* mis en place au Royaume-Uni soutient l'apprentissage des adultes.

Les pays de l'OCDE ont également multiplié les programmes de valorisation des compétences ou de recyclage. Certains ont mis en place des bons devant servir au développement des compétences numériques (Slovénie) ou des centres de compétences (Allemagne) ; d'autres proposent des formations aux TIC destinées aux PME (Israël), un soutien à la formation des salariés du secteur des TIC (Lettonie), des conseils aux PME (Lituanie), des programmes de valorisation des compétences ou de formation continue (Portugal), ou des cours en ligne gratuits (Royaume-Uni).

Accès aux données, partage et réutilisation

Tous les pays de l'OCDE et la plupart des économies partenaires ont lancé au moins une initiative ayant trait à l'accès aux données, à leur partage et à leur réutilisation (chapitre 5). La plupart concentrent leurs efforts sur l'accès aux données du secteur public et leur partage. Ainsi, les États-Unis, la France, le Japon et le Royaume-Uni ont entrepris d'ouvrir l'accès aux données publiques. De nombreux pays ont mis en place des initiatives axées sur les données générées par le secteur public, d'autres sur les données ouvertes, parfois sur les deux. Tel est le cas des pays membres de l'UE, suite à la Directive (UE) 2019/1024 du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public. On observe dans les pays de l'OCDE une tendance générale à la mise en place de portails de données ouvertes.

L'engagement des pouvoirs publics à davantage s'appuyer sur les données et à mettre à profit les progrès effectués dans des domaines comme celui du «*big data* » et l'IA, a permis de faciliter le partage des données au sein du secteur public. La législation sur le partage et la publication de données adoptée par l'Australie en est un exemple probant. Citons également le développement d'une zone d'échange de données, baptisée « X-Road », en Estonie, ou le cadre relatif à l'éthique en matière de données publiques (*Government Data Ethics Framework*), au Royaume-Uni.

L'ouverture des données géospatiales et des données sur les transports figure également en bonne place dans les programmes d'action ayant trait aux données du secteur public. L'initiative *Geocoded National Address File*, en Australie, en est un exemple. En Suisse, l'Office fédéral des transports entend faciliter l'échange de données entre les acteurs publics et privés du système de transports publics du pays.

Peu de pays facilitent l'échange de données au sein du secteur privé, bien qu'ils reconnaissent qu'il s'agit là d'un enjeu de plus en plus important. La plupart des initiatives reposent sur le volontariat ; les plus courantes portent sur la formulation de lignes directrices pour l'établissement de contrats ou sur la mise en place de partenariats autour des données, y compris des partenariats public-privé. Parmi les exemples d'initiatives publiques dans le domaine des directives sur l'établissement de contrats, citons notamment les orientations contractuelles sur l'utilisation de l'IA et des données, au Japon, ou les *Privacy and Security Principles for Farm Data* aux États-Unis. Pour ce qui est des partenariats, le projet *Industrial Data Space* en Allemagne, le *Data Integration Partnership* en Australie, le système de certification pour les plateformes de partage de données, au Japon, le Cadre de partage sécurisé de données, à Singapour, ou le *Digital Hub Denmark*, au Danemark peuvent être soulignés.

Lorsque le partage de données est obligatoire, les dispositifs sont généralement limités aux utilisateurs agréés. L'Australie, par exemple, envisage de mettre en place un cadre pour l'identification des « ensembles de données d'intérêt national » ou des « ensembles de données désignés ». En France, la Loi pour une République numérique définit les critères afférents aux « données d'intérêt général » (Gouvernement français, 2016[12]). La Commission européenne examine le partage des données entre les secteurs privé et public en se fondant sur la notion d'accès aux « données du secteur privé à des fins d'intérêt public ». Dans certains cas, l'accès aux données est basé sur des considérations de concurrence et d'efficience (des systèmes). Cette approche concerne avant tout les industries de réseau comme les télécommunications, l'énergie et les transports. La Loi sur les services de transport, adoptée en Finlande, en est un exemple.

La portabilité des données est souvent appréhendée comme un moyen intéressant de promouvoir une circulation et une utilisation intersectorielle des données. Dans le même temps, elle pourrait contribuer à renforcer les droits de contrôle des individus sur leurs données à caractère personnel, et ceux des entreprises, en particulier des PME, sur leurs données commerciales et de gestion. Parmi les principales initiatives relatives à la portabilité des données, citons notamment les projets *My Data* aux États-Unis et *Midata* au Royaume-Uni, le droit à la portabilité des données énoncé dans le Règlement général sur la protection des données (RGPD) de l'Union européenne, ainsi que la proposition récente de l'Australie d'instaurer un droit relatif aux données des consommateurs.

Certains pays ont mis en place des initiatives destinées exclusivement à soutenir le développement des compétences et des infrastructures liées aux données dans le secteur public. Tel est le cas du Royaume-Uni, avec le *Digital Skills Partnership*, de l'Estonie, avec des séminaires sur les solutions numériques, de la Chine, qui organise des compétitions dans le domaine de l'analytique des données, et de la Slovénie, qui a lancé des programmes d'éducation et de formation destinés aux fonctionnaires.

D'autres pays ont également créé des centres d'analyse de données et d'innovation chargés d'aider leurs organismes publics à partager et réutiliser les données. D'autres ont noué des partenariats avec de tels centres, ou les ont renforcés. C'est ainsi que l'Irlande a mis sur pied l'*Insight Centre for Data Analytics*, considéré comme l'une des plus grandes organisations européennes de recherche en analyse des données. En Australie, le centre d'innovation en matière de données, Data61, a noué un partenariat avec des organismes publics pour développer de nouvelles technologies afin de mettre les données publiques à forte valeur à la disposition d'un plus grand nombre de personnes, tout en veillant à la protection de la vie privée. La Commission européenne met actuellement en place un centre d'appui au partage des données dans le cadre de son programme *Connecting Europe Facility*.

Plusieurs pays et territoires ont par ailleurs soutenu l'innovation et la R-D dans les domaines de l'analytique des données et des technologies connexes. La Commission européenne, par exemple, dispose de plusieurs mécanismes de financement de l'innovation liée aux données. Ils servent à financer des incubateurs dédiés, des agrégateurs européens d'informations du secteur public (Portail européen de données) et des technologies destinées à renforcer la protection de la vie privée.

Les pouvoirs publics se sont tournés vers un large éventail de technologies numériques et d'outils analytiques perfectionnés pour collecter, analyser et partager les données en vue d'apporter des réponses de première ligne à la crise du COVID-19. Par exemple, Deutsche Telekom a fourni des données anonymisées sur les « flux de circulation » de ses utilisateurs au Robert Koch Institute, un centre de recherche et organisme public chargé du contrôle et de la prévention des maladies en Allemagne. Dans le même esprit, le Groupe Vodafone a publié un « Plan en cinq points » visant à lutter contre la pandémie de COVID-19 qui prévoit notamment la mise à disposition de vastes ensembles de données anonymisées destinés à aider les autorités à mieux comprendre les mouvements de population. Quant à la Commission européenne, elle a fait appel à huit opérateurs de télécommunications européens pour obtenir des données de localisation de mobiles anonymisées et agrégées en vue de coordonner les mesures de suivi de la propagation de l'épidémie.

Dans le cadre de la lutte contre la pandémie de COVID-19, des applications de traçage ont également vu le jour. Singapour, par exemple, a mis en place, dès le début de l'épidémie, un traçage des personnes ayant été en contact avec chacun des cas avérés ou suspectés. L'application permet un partage des informations médicales des malades entre les hôpitaux, les autorités et des tierces parties. De telles

applications pourraient poser des problèmes considérables de protection de la vie privée, que les utilisateurs aient la possibilité ou non d'exprimer un consentement éclairé et explicite à l'égard du partage de leurs données.

Protection de la vie privée

Les cadres de protection de la vie privée revêtent une importance toute particulière en période de crise, comme c'est le cas aujourd'hui avec la pandémie de COVID-19. Ils facilitent le partage des données lorsqu'il sert des intérêts de sécurité nationale et publique, et entre autre des enjeux liés à la santé publique et au bien-être. Des travaux récent menés par l'OCDE révèlent que, malgré l'existence de tels cadres, peu de pays disposent de politiques destinées à faciliter le partage des données au sein du secteur privé. Ils sont encore moins nombreux à être dotés de cadres de gouvernance régissant la collecte et le partage exceptionnels de données par des moyens rapides, sécurisés, fiables et évolutifs, dans le respect des réglementations applicables en matière de protection des données et de la vie privée.

En conséquence, de nombreux pays ont récemment sollicité les conseils des autorités chargées de la protection de la vie privée, de cabinets d'avocats du secteur privé, de la société civile, des milieux universitaires et d'autres acteurs. Ils souhaitent ce faisant avoir l'assurance que leurs actions sont nécessaires et proportionnées, et qu'ils en comprennent pleinement les incidences potentielles. De nombreux gouvernements ont préparé ou adopté des lois limitant la collecte de données en fonction de la population, de la période et de la finalité. Dans la majorité des pays de l'OCDE, les autorités chargées de la protection de la vie privée ont, en règle générale, privilégié une approche pragmatique, tenant compte du contexte. À cette fin, elles abordent l'application des lois avec discernement, en s'assurant que le respect des principes fondamentaux de protection des données et de la vie privée ne fasse pas obstacle aux réponses nécessaires et proportionnées apportées à la crise du COVID-19. En outre, dans de nombreux pays et territoires, ces autorités formulent des orientations pour la collecte, le traitement et le partage des données à caractère personnel servant au traçage des cas contacts et aux autres mesures mises en place. Ces orientations portent pour la plupart sur la façon dont les fonctionnalités de protection de la vie privé peuvent être intégrées par défaut aux applications de suivi et de traçage, de manière à garantir la protection des données à caractère personnel collectées.

Les deux dernières années ont été marquées par des évolutions réglementaires importantes partout dans le monde (chapitre 6). En particulier, dans l'Union européenne, le RGPD, entré en application le 25 mai 2018, a établi de nouvelles règles régissant la libre circulation des données à caractère personnel relatives aux personnes concernées au sein de l'Union européenne.

De plus, le Conseil de l'Europe a récemment modifié en profondeur sa Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108), qui date de 1985. Cette révision a pour objet de garantir son applicabilité aux nouvelles TIC et de renforcer sa mise en œuvre. L'instrument ainsi modernisé, dénommé « Convention 108+ » doit entrer en vigueur en octobre 2023.

L'OCDE assure par ailleurs le suivi de la mise en œuvre de la révision de ses Lignes directrices de 1980 sur la protection de la vie privée effectuée en 2013. L'exercice vise à recenser les lacunes de l'instrument et proposer des mesures afin de veiller à ce qu'il reste pertinent.

Par ailleurs, on observe une multiplication des accords commerciaux et des cadres destinés à promouvoir la confiance dans les flux transfrontières de données à caractère personnel. Ces instruments viennent s'ajouter à d'autres dispositifs qui continuent de façonner la protection de la vie privée et les transferts de données à l'échelle internationale, à l'instar du « bouclier UE-États-Unis de protection de la vie privée » (*EU-US Privacy Shield Framework*) ou du Cadre de protection de la vie privée du Forum de coopération économique Asie-Pacifique (APEC).

À l'échelle nationale, un nombre croissant de pays (notamment de la zone OCDE) adoptent des cadres et des politiques modernes de protection des données. Ils favorisent l'ouverture aux flux internationaux de données tout en assurant un haut niveau de protection des données et de la vie privée des individus. De nombreux gouvernements ont élaboré des politiques relatives aux données ou modifié leurs politiques existantes de manière à les adapter à l'ère du numérique. Elles définissent en outre les conditions qui régissent les transferts transfrontaliers de données ou imposent que les données soient stockées localement.

En revanche, comprendre comment les lois de protection de la vie privée s'appliquent aux technologies émergentes telles que l'IA, ainsi que leurs incidences sur les consommateurs, reste un défi. Face à ces enjeux, les pays et territoires mettent au point des réglementations et des lignes directrices dédiées. En outre, ils utilisent, élaborent ou envisagent des mesures destinées à favoriser l'innovation réglementaire dans ce domaine, se tournant le plus souvent vers des outils de droit souple tels que les «*sandboxes* » et l'expérimentation réglementaire. Les pays se sont également saisis d'autres types de mesures, telles que l'élaboration de normes internationales pour des technologies spécifiques (comme la technologie du «*blockchain*»), la mise au point d'une Charte numérique, le lancement d'un programme de subvention pour la recherche sur la protection de la vie privée, ou l'élaboration d'un cadre d'audit de l'IA.

Certaines évolutions dans le domaine de la protection de la vie privée méritent une attention particulière. Aux États-Unis, le *California Consumer Privacy Act*, adopté en 2018, confère aux consommateurs de nouveaux droits concernant la collecte, le traitement, la conservation et le partage des données à caractère personnel qui les concernent. Le Brésil a également adopté la même année une loi générale sur la protection des données. En Inde, la législation nationale sur la protection des données, attendue de longue date, a été débattue au Parlement.

La révision de 2013 des Lignes directrices de l'OCDE sur la protection de la vie privée appelle les pouvoirs publics à « élaborer des stratégies nationales de protection de la vie privée qui traduisent une approche coordonnée entre organismes gouvernementaux ». Pour autant, un peu moins de la moitié des 29 pays ayant répondu à l'enquête de 2019 sur la mise en œuvre des Lignes directrices de l'OCDE disposent d'une telle stratégie ou ont adopté une stratégie de protection de la vie privée à l'échelle de l'ensemble de l'administration.

Outre les réformes et l'innovation réglementaires, les pays apportent des réponses politiques aux défis induits par les technologies émergentes. S'ils privilégient la mise au point de nouveaux cadres de gouvernance des données, ils mettent également en œuvre de nouveaux organismes ou établissements et formulent des lignes directrices dédiées à des technologies particulières. Le Royaume-Uni, par exemple, a créé récemment un centre baptisé *Centre for Data Ethics and Innovation*, chargé d'identifier les questions éthiques soulevées par les technologies émergentes, de convenir des meilleures pratiques en matière d'utilisation des données et d'élaborer d'éventuelles réglementations afin de « susciter la confiance et de stimuler l'innovation dans les technologies fondées sur les données ».

Les pays s'attachent aujourd'hui à apporter de nouvelles réponses stratégiques et complémentaires pour renforcer la protection de la vie privée des enfants. Au niveau national, la quasi-totalité des répondants à une enquête réalisée en 2017 par l'OCDE ont indiqué que leur législation en matière de protection de la vie privée intégrait des dispositions particulières relatives à la protection des enfants. Le RGPD stipule en effet que les données à caractère personnel des enfants doivent faire l'objet une protection spécifique, notamment lorsqu'elles sont utilisées à des fins de marketing ou sont collectées. En revanche, les approches adoptées par les pays de l'OCDE diffèrent pour ce qui est de l'information et du recueil du consentement dans le cadre de la collecte, du traitement et du partage de ces données.

À mesure que les pays adoptent des cadres de protection des données et de la vie privée, une attention croissante est portée aux moyens d'améliorer la conformité à ces cadres, notamment par le biais de mesures d'application accrues. Les gouvernements investissent notamment dans des actions de sensibilisation aux obligations énoncées dans les cadres de protection. Ils promeuvent également la redevabilité des responsables du traitement des données et la coopération internationale en matière de protection des données et de la vie privée. Parmi les principaux mécanismes multilatéraux mis en place, par exemple le Réseau mondial d'application des lois de protection de la vie privée (Global Privacy Enforcement Network, ou GPEN), l'accord de coopération en matière d'application des lois de protection de la vie privée de la Conférence internationale des commissaires à la protection des données et de la vie privée, devenue l'Assemblée mondiale pour la protection de la vie privée (Global Privacy Assembly), ou encore l'Accord sur le contrôle des mesures transfrontières de protection de la vie privée de l'APEC.

Sécurité numérique

Plusieurs pays de l'OCDE ont adopté des stratégies nationales en matière de sécurité numérique visant à soutenir la prospérité économique et sociale et/ou à susciter la confiance dans l'environnement numérique (chapitre 7). Le renforcement des capacités, la protection des infrastructures critiques, le partage d'informations et la coopération internationale sont les principaux piliers de ces stratégies.

Face à la crise du COVID-19, les organismes publics chargés de la sécurité numérique dans les pays de l'OCDE ont pris plusieurs types de mesures. Ils ont déployé des efforts de sensibilisation, assuré un suivi des menaces, apporté de l'aide en tant que de besoin et coopéré avec l'ensemble des parties prenantes concernées, y compris à l'échelle internationale. Aux États-Unis, par exemple, la Cyber and Infrastructure Security Agency a créé sur son site Internet une section dédiée aux risques inhérents à la crise du COVID-19 (*www.cisa.gov/coronavirus*). En Europe, la Commission européenne, l'Agence de l'UE pour la cybersécurité (ENISA), l'Équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union européenne (CERT-EU) et Europol ont coopéré afin de traquer les activités malveillantes liées à la pandémie de COVID-19 et d'alerter leurs communautés respectives. Le Centre canadien pour la cybersécurité a, pour sa part, recommandé que les organisations de santé canadiennes participant à la lutte contre la pandémie engagée à l'échelle nationale fassent preuve de vigilance et veillent à la mise en œuvre de meilleures pratiques en matière de sécurité numérique. L'Office national tchèque pour la cybersécurité et la sécurité de l'information a enjoint à certains organismes de santé de renforcer la sécurité de leurs systèmes TIC clés et leur a proposé à cet effet des consultations et un appui.

Les mécanismes de coordination diffèrent selon les pays. Au Danemark, par exemple, l'Agence pour le numérique (qui relève du ministère des Finances) et le Centre pour la cybersécurité (qui dépend du ministère de la Défense) partagent les responsabilités y afférentes. Aux Pays-Bas, le ministère de la Justice est chargé de la coordination générale. Dans certains pays, comme l'Espagne, les États-Unis ou la Lettonie, un conseil national réunit des représentants de l'ensemble des ministères et des organismes concernés.

La nature et le périmètre de la coopération multipartite varient eux aussi sensiblement. Si certains gouvernements coopèrent ponctuellement avec des associations professionnelles ciblées, d'autres associent plus largement les parties prenantes, dès la phase de conception. Tel est le cas du Brésil, qui a mis en place trois groupes de travail chargés respectivement des questions liées à la gouvernance numérique, à la prévention et la réduction des menaces, et à la protection des infrastructures publiques et critiques.

Au-delà des stratégies et des politiques nationales, les gouvernements des pays de l'OCDE favorisent également le recours à de nouvelles formes de partenariats multipartites et internationaux en vue de renforcer la sécurité numérique. L'Appel de Paris pour la confiance et la sécurité dans le cyberespace et les initiatives Charter of Trust et Cybersecurity Tech Accord en sont des exemples.

On observe une montée en puissance de l'innovation en matière de sécurité numérique dans les pays de l'OCDE, qui ont créé des centres d'innovation ouverte afin d'encourager son développement. Les exemples se multiplient, du campus CyberSpark en Israël, au réseau Australian Cyber Security Growth Network en Australie, en passant par le London Office for Rapid Cybersecurity Advancement au Royaume-Uni, l'Innovation Cybersecurity Ecosystem à Singapour, l'Agence pour l'innovation en matière de cybersécurité en Allemagne, le Cyber Campus France ou encore l'Organisation européenne de cybersécurité.

Les pouvoirs publics soutiennent par ailleurs la mise en place de programmes d'éducation afin de parer à la pénurie de professionnels de la sécurité numérique. Aux États-Unis, par exemple, le National Institute of Standards and Technology, au sein du Department of Commerce, a lancé la National Initiative for Cybersecurity Education. Le Canada encourage le développement des talents en enseignant aux jeunes enfants la programmation informatique et en les dotant de compétences numériques. Les pouvoirs publics peuvent en outre promouvoir l'établissement de relations durables entre les universités, l'industrie, l'administration elle-même, les entrepreneurs et les acteurs financiers. Par exemple, le Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity (Global EPIC) coordonne la coopération entre les écosystèmes de sécurité numérique à l'échelle mondiale.

Certains pays de l'OCDE ont lancé des dispositifs de labélisation volontaire destinés à améliorer la transparence sur les produits et réduire les vulnérabilités. Ainsi, le gouvernement finlandais a établi un partenariat avec l'industrie pour lancer un label de sécurité pour l'IdO. Dans la même veine, les gouvernements du Japon et de l'Allemagne prévoient de créer leurs propres dispositifs de labélisation, respectivement pour les produits de l'IdO et les routeurs.

Autre outil à la disposition des pouvoirs publics : l'établissement de partenariats multipartites. Le gouvernement néerlandais, par exemple, travaille de concert avec les parties prenantes afin de surveiller et de renforcer la sécurité numérique des appareils connectés. Aux États-Unis, la National Telecommunications and Information Agency encourage les développeurs à établir une « nomenclature logicielle ». D'autres pays de l'OCDE ont financé et/ou favorisé l'exécution de travaux conjoints sur les réseaux de zombies (*botnets*), à l'image de l'Allemagne, avec le projet « botfrei » de lutte contre les botnets, ou du Japon qui a lancé une campagne nationale baptisée NOTICE (*National Operation Towards IoT Clean Environment*).

Certains pays ont quant à eux recours à la réglementation pour rendre obligatoire l'intégration de fonctions de sécurité de base dans tous les produits de l'IdO. Au Royaume-Uni, par exemple, le gouvernement entend rendre obligatoire l'application des principes phares de ses lignes directrices relatives à la sécurité de l'IdO pour les fabricants. Au Japon, le régulateur a également défini des exigences concernant les produits de l'IdO.

Plusieurs acteurs du secteur ont mis en place des coalitions afin de renforcer la sécurité numérique de leurs produits. L'initiative Charter of Trust, par exemple, rassemble des entreprises prenant part à la chaîne de valeur afin de créer des conditions propices à la confiance dans l'environnement numérique. De même, 120 entreprises du secteur des TIC se sont réunies au sein du Cybersecurity Tech Accord pour coopérer dans le cadre d'initiatives destinées à améliorer la sécurité, la stabilité et la résilience du cyberespace. Dans le même temps, la France a lancé l'Appel de Paris pour la confiance et la sécurité dans le cyberespace dans le but de renforcer la sécurité des processus, des produits et des services numériques, tout au long de leur cycle de vie et de la chaîne logistique.

Politique à l'égard des consommateurs

Les pouvoirs publics doivent réfléchir aux moyens d'adapter, de modifier et de mettre en œuvre leur politique à l'égard des consommateurs en ces temps de mutations technologiques rapides (chapitre 8). Si, en règle générale, les politiques à l'égard des consommateurs ont un champ d'application suffisamment large pour couvrir les technologies et modèles économiques nouveaux, les pouvoirs publics doivent néanmoins s'assurer qu'elles ne présentent aucune lacune qui rendrait les consommateurs vulnérables. Ils ont en cela un rôle essentiel à jouer pour favoriser une utilisation des nouvelles technologies qui soit centrée sur l'humain, éthique et inscrite dans une logique de durabilité, afin de préserver la confiance des consommateurs.

Autre défi de taille, les pouvoirs publics doivent disposer de l'expertise technique nécessaire pour comprendre ces problématiques émergentes de manière à garantir une élaboration et une mise en œuvre efficaces des politiques. Il n'est pas rare que les risques couvrent plusieurs domaines – protection des données, de la vie privée et des consommateurs, concurrence, sécurité. D'où la nécessité pour les autorités chargées de la protection des consommateurs de coopérer et de coordonner leurs activités avec leurs homologues œuvrant dans d'autres disciplines pertinentes. De plus, la portée mondiale de la transformation numérique rend nécessaire une coopération plus rapprochée entre les pays qui pourrait, notamment se faire en mettant en œuvre les dispositions énoncées en ce sens dans la Recommandation de 2016 du Conseil de l'OCDE sur la protection du consommateur dans le contexte du commerce électronique (OCDE, 2016[13]) et dans les Lignes directrices de 2003 de l'OCDE sur *la Protection des Consommateurs Contre les Pratiques Commerciales Transfrontières Frauduleuses et Trompeuses* (OECD, 2003[14]).

Les politiques à l'égard des consommateurs devraient tenir compte des vulnérabilités des différents groupes de consommateurs afin de cibler les mesures de protection et de sensibilisation en conséquence et de s'assurer que les nouvelles technologies profitent à l'ensemble de la société. Par exemple, certains groupes de consommateurs, à l'instar des personnes âgées, peuvent être davantage exposées aux escroqueries en ligne. De la même façon, les questions de protection des données et de la vie privée peuvent devenir plus épineuses encore lorsque des produits de l'IdO s'adressent à des enfants, parfois moins conscients des risques auxquels ils s'exposent. En outre, la crise du COVID-19 montre que les décideurs devraient s'interroger sur le risque qu'un événement de grande ampleur, qu'il s'agisse d'une pandémie ou d'une catastrophe naturelle, puisse rendre des groupes plus larges de consommateurs vulnérables à une exploitation commerciale en ligne. Par ailleurs, la pandémie a eu pour effet d'exposer des hordes de consommateurs ordinaires à des pratiques abusives sur Internet, certains exploitant les

vulnérabilités induites par les suppressions d'emplois, les pertes financières, ou la crainte et l'anxiété à l'égard du virus. L'augmentation des prix de certains produits de première nécessité pour lesquels la demande a explosé en est une illustration.

Il importe par conséquent d'encourager les entreprises et les associations professionnelles, ainsi que les groupements de consommateurs et autres organisations de la société civile, à contribuer aux politiques relatives à l'intégration des nouvelles technologies dans les produits de consommation. Cela permettra de s'assurer que les nouveaux produits profitent aux consommateurs sans leur nuire économiquement, mettre en péril la protection de leur vie privée ou la sécurité de leurs informations personnelles, ni les exposer à quelque risque que ce soit.

Généralisation du numérique dans les politiques de la science et de l'innovation

Le numérique n'a pas seulement transformé la science, la recherche et l'innovation : désormais ses effets se font également sentir sur les processus d'élaboration des politiques dans ces domaines (chapitre 9).

Plusieurs pays ont lancé des initiatives liées aux politiques de la science et de l'innovation fondées sur le numérique (DSIP). Ils expérimentent les technologies sémantiques pour établir des liens entre les ensembles de données ; l'IA pour aider à l'analytique des données massives ; ou encore la visualisation interactive et les tableaux de bord pour promouvoir l'utilisation des données dans le cadre des processus liés aux politiques.

L'établissement de liens entre les données et la synchronisation à l'échelle des différents systèmes numériques peuvent aider à optimiser les flux de travail administratifs en vue de réduire la charge en termes de reporting. Ils peuvent également faciliter le suivi et la gestion des performances. Enfin, ils peuvent apporter des informations prévisionnelles utiles pour identifier les besoins en termes de politique d'innovation.

La concrétisation du potentiel des DSIP ne pourra se faire sans surmonter les éventuels obstacles liés à la qualité des données, à l'interopérabilité, à un financement durable et aux réglementations en matière de protection des données. Les décideurs désireux de promouvoir de telles politiques se heurtent en outre à des défis systémiques : superviser des efforts dispersés d'élaboration de politiques fondées sur le numérique et des initiatives multiples, souvent mal coordonnées ; veiller à une utilisation responsable des données produites à d'autres fins ; ou encore trouver un juste équilibre entre les avantages et les risques inhérents à la participation du secteur privé dans la fourniture des données, des composantes et des services liés aux DSIP.

Les outils numériques peuvent apporter des solutions en termes d'interopérabilité des données. La collecte d'ensembles de données auprès de tous les acteurs publics et privés menant des activités de recherche et d'innovation exige des formats de données communs, ainsi que d'autres facteurs d'interopérabilité, à savoir des interfaces de programmation (API), des ontologies, des protocoles et des identifiants uniques persistants et partageables (UPPI) pour les acteurs de la recherche, du développement et de l'innovation.

Certains UPPI font partie intégrante de produits commerciaux (ou les sous-tendent), à l'instar de bases de données de publications/citations, de systèmes d'information sur la recherche et de services de gestion de la chaîne logistique. D'autres n'existent que pour fournir un système d'identifiants à l'appui d'une large adoption et utilisation. L'identifiant ORCID (Open Researcher and Contributor Identifier), par exemple, sert à lever les ambiguïtés lorsque des noms identiques sont utilisés dans le cadre de la recherche scientifique. Le système s'appuie sur un registre numérique contenant des identifiants uniques et des informations élémentaires correspondantes sur l'identité des chercheurs.

La popularité croissante d'un système d'UPPI peut créer un « effet de réseau », dans la la mesure où chaque nouvel inscrit augmente la valeur du système pour l'ensemble des utilisateurs. À terme, le système peut alors s'imposer comme la solution de référence que les entités utilisent pour s'identifier mutuellement sans ambigüité. Ce qui, par conséquent, incite celles qui ne l'ont pas encore fait à s'enregistrer.

Outre les UPPI, les API sont devenues la norme pour les interactions de machine à machine (M2M) et l'échange de données. Dans le cadre d'initiatives en faveur de l'administration numérique, plusieurs pays ont multiplié les API pour les sites web et les bases de données des pouvoirs publics, avec à la clé une meilleure réutilisation des données. L'amélioration de l'accès aux ensembles de données administratifs a des effets positifs sur la fonctionnalité et la fiabilité des résultats des analyses générées par les systèmes DSIP.

Au-delà des organismes publics et autres bailleurs de fonds publics, les organisations menant des activités de recherche, de développement et d'innovation stockent une grande partie des données issues de la recherche et de l'innovation. Or ces données présentent souvent des formats et des structures différents, y compris pour des informations de même type. Le format européen CERIF (Common European Research Information Format) et les formats de métadonnées du Consortium pour l'avancement des normes en matière d'information sur l'administration de la recherche (CASRAI, Consortia Advancing Standards in Research Administration Information) ont été conçus à l'origine pour répondre aux besoins de gestion de données des établissements d'enseignement supérieur. Certains systèmes DSIP les utilisent pour collecter des données, après curation, auprès d'établissements de recherche et les exploiter directement dans les analyses.

Le manque d'interopérabilité reste un obstacle majeur malgré la généralisation des identifiants, des normes et des protocoles. Les décideurs pourraient être à même d'influer sur le développement de systèmes d'UPPI internationaux. Ils pourraient se concentrer sur les populations cibles, les informations recueillies, la compatibilité avec les systèmes statistiques, les systèmes de gouvernance et, en particulier, l'adoption à la fois par les institutions et par les utilisateurs potentiels. Les efforts internationaux de documentation des données et d'élaboration de normes relatives aux métadonnées pourraient être mutualisés afin d'améliorer l'interopérabilité des données.

Le travail à l'ère du numérique

Dans de nombreux pays, on observe depuis quelques années une progression des « formes de travail atypiques », expression générique utilisée pour désigner les emplois temporaires, les contrats à temps partiel et le travail indépendant. Bien que certaines d'entre elles ne soient pas nouvelles, la transformation numérique, combinée à la mondialisation et à l'évolution des réglementations et des politiques, ont contribué à leur diffusion. Les technologies numériques ont elles-mêmes ouvert la voie à de nouvelles formes de travail, comme le travail par le biais des plateformes. Les travailleurs atypiques ont été les plus durement touchés par la crise du COVID-19, car ils sont plus exposés aux risques sanitaires et perçoivent souvent moins d'aides publiques que les salariés (chapitre 10).

Plusieurs pays, dont le Royaume-Uni, les Pays-Bas et la Pologne, considèrent la mise en place d'une rémunération minimum pour certains groupes de travailleurs indépendants. Des administrations infranationales ont également fixé un salaire minimum pour les travailleurs des plateformes. La ville de New York, par exemple, a défini un salaire minimum pour les chauffeurs Uber et Lyft. Il en va de même pour certaines plateformes, qui ont pris des mesures volontaires en ce sens (Adtriboo en Espagne ; Favor aux États-Unis ; Topdesigner en République tchèque ; et Upwork et Prolific au Royaume-Uni).

En lieu et place ou en complément du salaire minimum, des pays comme l'Allemagne, le Canada, le Danemark, la France et la Suède ont étendu les droits établis par les conventions collectives à certaines catégories de travailleurs indépendants. Outre les initiatives menées par les travailleurs, des plateformes commencent également à se pencher sur la question de l'accès limité des travailleurs des plateformes à la représentation et au dialogue social. Ces actions font principalement suite aux menaces des gouvernements de requalifier leurs activités.

Les pouvoirs publics ont pris des mesures pour réglementer les contrats de travail atypiques, tels que les contrats « zéro heure », afin de limiter l'imprévisibilité des heures de travail et des revenus. La Finlande, par exemple, n'autorise le recours à ce type de contrat que lorsque les employeurs ont véritablement des besoins de main-d'œuvre variables. Le pays, tout comme la Norvège et l'Irlande, exige en outre des employeurs qu'ils fournissent, à l'avance ou dans le contrat de travail, des informations comme le nombre minimum d'heures travaillées. Ces trois pays, ainsi que les Pays-Bas et l'État de l'Oregon, aux États-Unis, les obligent à communiquer à l'avance les plannings de travail. En Australie et au Royaume-Uni, les employés ont le droit de demander, à l'issue d'une certaine période, un contrat leur offrant plus de visibilité.

Par ailleurs, des pays ont pris des mesures en vue d'étendre la protection de la sécurité et de la santé des travailleurs aux non-salariés. L'Australie, l'Irlande, la Lituanie, le Royaume-Uni et la Turquie ont dissocié cette protection de la relation employeur-salarié. L'Australie, la Bulgarie, le Canada et la Pologne lient la réglementation associée au lieu de travail plutôt qu'à un type de contrat particulier. La Corée envisage pour sa part d'étendre la loi sur la sécurité et la santé au travail à l'« ensemble des travailleurs ». Dans le même temps, en France, la nouvelle loi Travail contraint les plateformes à rembourser les travailleurs qui contractent de leur propre chef une assurance contre les risques professionnels ou une assurance santé.

Le Danemark et la France ont également adopté d'importantes réformes de leur système de protection sociale afin de garantir la portabilité des droits aux individus passant du statut de salarié à une situation de travailleur indépendant ou conjuguant les deux. En novembre 2019, l'Union européenne a adopté une *Recommandation du Conseil relative à l'accès des travailleurs salariés et non salariés à la protection sociale*. Celle-ci encourage les États membres à autoriser les travailleurs atypiques et les travailleurs indépendants à adhérer aux régimes de protection sociale, tout en renforçant l'adéquation de ces régimes aux formes de travail atypiques.

Certains pays de l'OCDE, dont la France et l'Irlande, ont étendu les incitations financières en faveur de la formation aux travailleurs indépendants, y compris ceux opérant pour leur compte propre. Ces incitations se présentent sous la forme de déductions fiscales et de subventions. D'autres approches, adoptées par exemple en Corée, en Autriche ou en Belgique, conditionnent l'octroi d'aides financières en faveur de la formation au versement de cotisations de sécurité sociale ou à la souscription à un régime d'assurance emploi. Certains pays, dont l'Autriche, la Finlande et le Luxembourg, compensent la perte de salaire des travailleurs indépendants qui suivent une formation. En France, la loi Travail oblige les plateformes à verser les cotisations patronales au titre de la formation, à prendre en charge les frais liés à la validation des acquis de l'expérience, et à verser une indemnité de formation à tous les travailleurs au cachet dont le chiffre d'affaires est supérieur à un seuil défini.

Les parcours professionnels devenant de moins en moins linéaires, plusieurs pays de l'OCDE ont mis en place des dispositifs d'apprentissage individuel. Les droits à la formation sont alors associés aux individus et non plus à un employeur ou un statut professionnel particulier. Certains pays, dont l'Allemagne, la Belgique (Flandre) et la Lettonie, ont également étendu les services de conseil en développement de compétences et d'orientation fournis par les services publics de l'emploi aux travailleurs indépendants.

Intelligence artificielle

Le Canada a été le premier pays à se doter, en 2017, d'une stratégie nationale en matière d'IA. En avril 2020, plus de 60 pays avaient adopté une stratégie ou une politique nationale dédiée – d'autres sont en cours d'élaboration. Parmi les domaines prioritaires ciblés, citons notamment la R-D et le financement de l'IA, l'industrie, les défis sociétaux, l'éducation et l'emploi, la réglementation et la coopération internationale. Parallèlement, les pays se penchent sur les risques et les enjeux éthiques liés à l'IA. Certains ont créé des organes de surveillance et formulé des orientations sur les aspects éthiques. Plusieurs ont entrepris de revoir et d'adapter les cadres politiques et réglementaires applicables (chapitre 11).

Pendant la pandémie de COVID-19, pouvoirs publics, universitaires et entreprises ont rapidement développé des systèmes d'IA afin de prévoir et surveiller la propagation du virus, d'établir des diagnostics médicaux, de lutter contre la désinformation et de mener des travaux de recherche sur les vaccins et les traitements. Par ailleurs, de nombreux pays ont déployé des assistants virtuels et des agents conversationnels pour aider les organisations de santé. Aux États-Unis, par exemple, le *Center for Disease Control and Prevention* et Microsoft proposent un service d'autocontrôle dédié au coronavirus qui aide les utilisateurs à autoévaluer leur situation au regard du COVID-19 et leur suggère la marche à suivre.

Plusieurs pays ont mis en place des organismes dédiés, chargés de coordonner la mise en œuvre de leur stratégie en matière d'IA (Canada, Égypte, États-Unis, Royaume-Uni) ; de mener à bien des activités de prospective technologique et des études d'impact (Autriche, Canada, États-Unis, Royaume-Uni) ; ou de s'atteler aux questions éthiques (Singapour, Nouvelle-Zélande, Royaume-Uni). Par ailleurs, des observatoires de l'IA ont été créés aux niveaux régional (Québec), national (Italie, France, Allemagne)

et international (projets « AI Watch » et « AI4EU » portés par la Commission européenne, Observatoire « OECD.AI » de l'OCDE).

S'inspirant des approches suivies dans le domaine de l'administration électronique, de nombreuses stratégies et politiques nationales en matière d'IA encouragent explicitement le secteur public à l'adopter. Ainsi, le Danemark incite le secteur public à recourir à l'IA pour proposer des services d'excellence servant les intérêts des citoyens et de la société. Avec son projet AuroraAI, la Finlande entend favoriser l'utilisation de l'IA pour fournir des services publics personnalisés et centrés sur l'humain, via un guichet unique. En Corée, le service fondé sur l'IA baptisé « The Work » a aidé 2 666 demandeurs d'emploi à trouver des offres pertinentes ayant débouché sur un recrutement au cours du deuxième trimestre de 2019. Le Plan coordonné dans le domaine de l'intelligence artificielle de l'UE vise à « placer les administrations publiques européennes dans le peloton de tête des utilisateurs de l'IA ».

La plupart des pays ont formulé des lignes directrices afin de tendre vers une IA digne de confiance, dans le droit fil de la Recommandation du Conseil de l'OCDE sur l'intelligence artificielle (Principes de l'OCDE sur l'IA) (OCDE, 2019[14]). Le cadre *AI Ethics Framework*, en Australie, les orientations éthiques en matière d'IA, en Hongrie, les Lignes directrices relatives à la R-D dans le domaine de l'IA et à l'utilisation de l'IA, au Japon, le Cadre type de gouvernance de l'IA, à Singapour, et les Lignes directrices en matière d'éthique pour une IA digne de confiance de la Commission européenne en sont autant d'exemples.

Plusieurs gouvernements et organismes intergouvernementaux ont adopté une législation contraignante (ou envisagent de le faire) dans les domaines d'application de l'IA jugés à haut risque. La Belgique, par exemple, a interdit l'utilisation d'armes létales autonomes par les forces armées locales. De nouvelles réglementations ont également été adoptées concernant les voitures autonomes (Belgique, Danemark) ou des systèmes d'aéronefs sans pilote (États-Unis). En février 2020, la Commission européenne a publié un livre blanc intitulé « Intelligence artificielle - Une approche européenne axée sur l'excellence et la confiance », dans lequel elle propose la mise en place d'un « label de qualité » non obligatoire pour les applications d'IA qui ne sont pas considérées comme étant à haut risque.

L'Organisation internationale de normalisation, l'IEEE (Institute of Electrical and Electronics Engineers) et d'autres organismes de même ordre mettent actuellement au point des normes sectorielles et intersectorielles relatives à l'IA. Plusieurs pays, dont l'Allemagne, l'Australie, le Canada, la Chine, les États-Unis et la Fédération de Russie, mettent l'accent sur la nécessité de définir des normes communes, notamment pour les questions liées à la sécurité. D'autres, à l'image du Danemark et de Malte, envisagent de mettre en place des programmes de certification dédiés à l'IA.

La plupart des pays cherchent à développer les capacités nationales de R-D en matière d'IA. Les États-Unis ont l'intention d'investir, en 2021, 950 millions USD supplémentaires dans la R-D en IA non militaire et de créer des établissements nationaux de recherche en IA. Au Canada, les autorités fédérales et provinciales ont consacré, au cours de la période 2017-22, plus de 300 millions CAD (227 millions USD) à la recherche en IA menée par les trois instituts d'IA nationaux qui prennent part à la mise en œuvre de la Stratégie pancanadienne en matière d'intelligence artificielle. Le programme Horizon 2020 de l'UE consacre à la recherche en IA un budget de 1.5 milliard EUR sur deux ans et table sur 20 milliards EUR supplémentaires de la part du secteur privé et des États membres en 2020.

Dans le cadre de leur stratégie en matière d'IA, plusieurs pays créent ou ont créé des référentiels centralisés et accessibles de données publiques ouvertes liés à l'IA (Espagne, États-Unis, Norvège, Portugal). D'autres entendent encourager le partage de données au sein du secteur privé (Royaume-Uni, Union européenne).

Les pays favorisent également la création d'écosystèmes de recherche en IA innovants, via la mise en place de plateformes de mise en relation et de collaboration. Citons par exemple l'Initiative des « *Superclusters d'innovation* » au Canada, la plateforme numérique pour les partenariats public-privé en matière d'IA au Danemark, le programme en faveur des entreprises d'IA en Finlande, la plateforme électronique en libre-service IA en pratique, en Hongrie, ou encore les plateformes d'innovation numérique au Portugal.

À cela s'ajoute la mise en place de nombreuses initiatives destinées à stimuler l'innovation et l'adoption de l'IA dans les PME. Le projet AI4EU de la Commission européenne, l'Accélérateur d'IA, en Finlande, les Centres d'excellence PME 4.0, en Allemagne, et la plateforme d'innovation ouverte en matière d'IA, en

Corée, en sont quelques exemples. Les pays expérimentent également des environnements contrôlés pour la réalisation de tests sur les systèmes d'IA, y compris par des PME (Émirats arabes unis, États-Unis, Lituanie, Nouvelle-Zélande, Royaume-Uni).

Toutes les stratégies nationales d'IA mettent l'accent sur l'éducation et le développement des compétences. Certaines initiatives s'inscrivent dans le cadre de programmes d'éducation et de formation structurés sur l'IA, notamment dans des disciplines comme les sciences, les technologies, l'ingénierie et les mathématiques (Australie, États-Unis, Finlande, Royaume-Uni). D'autres prévoient des incitations pour attirer et fidéliser des spécialistes et d'éminents talents étrangers dans le domaine de l'IA (Belgique, Royaume-Uni).

Les pays misent également sur les programmes de formation professionnelle et d'apprentissage tout au long de la vie pour aider les citoyens à suivre le rythme des évolutions technologiques et sociétales. Par exemple, en Finlande, le programme Éléments d'IA vise à développer les connaissances en IA de la population, par le biais d'un cours en ligne ouvert à tous de dix heures.

Parallèlement, dans le cadre des stratégies nationales en matière d'IA, des collaborations se créent entre les pouvoirs publics, les entreprises et les communautés éducatives et à but non lucratif dans le but de créer des programmes, outils et technologies éducatifs. La plateforme coréenne de formation intelligente et la plateforme allemande de systèmes d'apprentissage (Plattform Lernende Systeme) en sont deux exemples.

Certains pays, dont l'Allemagne, la France, la Pologne et la République tchèque, ont mis en place des observatoires du marché du travail dédiés afin de mieux appréhender les incidences de l'IA sur l'emploi.

Par ailleurs, la coopération internationale en matière d'IA s'organise dans le cadre de forums tels que l'OCDE, le G7, le G20, l'Union européenne, le Conseil de l'Europe et l'Organisation des Nations Unies pour l'éducation, la science et la culture. Autre priorité : la recherche transfrontalière dans le domaine de l'IA. L'Agence nationale de la recherche française, la Fondation allemande pour la recherche et l'Agence japonaise de science et de technologie ont ainsi appelé à la mise sur pied de projets trilatéraux de recherche collaborative en IA.

Certains pays (Allemagne, Canada, Italie, États-Unis, France, Royaume-Uni) ont lancé des activités d'analyse des politiques afin d'évaluer la mise en œuvre de leurs stratégies nationales en matière d'IA. Au niveau européen, le projet AI Watch collecte des indicateurs de suivi des investissements consacrés à l'IA. En février 2020, l'OCDE a lancé l'Observatoire des politiques relatives à l'IA *(OECD.AI)*[6], une plateforme destinée à aider les décideurs à suivre l'évolution des politiques connexes. L'OCDE héberge par ailleurs le nouveau Partenariat mondial sur l'intelligence artificielle (PMIA), une coalition lancée en juin 2020 et chargée de veiller à ce que l'IA soit utilisée de manière responsable, dans le respect des droits humains et des valeurs démocratiques. L'Allemagne, l'Australie, le Canada, la Corée, les États-Unis, la France, l'Inde, l'Italie, le Japon, le Mexique, la Nouvelle-Zélande, le Royaume-Uni, Singapour, la Slovénie et l'Union européenne en sont les membres fondateurs.

Le PMIA rassemble des experts issus de l'industrie, de l'administration, de la société civile et du monde universitaire, chargés de mener des travaux de recherche et des projets pilotes sur l'IA. Il vise à établir des ponts entre la théorie et la pratique dans le domaine des politiques relatives à l'IA. Le PMIA pourrait par exemple étudier la façon dont l'IA pourrait aider les sociétés à affronter la crise du COVID-19 et organiser la reprise.

Technologies de registres distribués

Les pays s'intéressent de plus en plus aux effets de la technologie du « *blockchain* » et des autres technologies de registres distribués (« *distributed ledger technologies* ») sur les économies et les sociétés, ainsi qu'à leur utilisation en tant qu'outil au service de l'action des pouvoirs publics. Plusieurs ont d'ores et déjà adopté des stratégies générales en la matière – tel est le cas de l'Allemagne, de l'Australie, de la Chine et de l'Inde. D'autres, dont la France et l'Italie, suivent le même chemin (chapitre 11).

La technologie du « *blockchain* » et les autres technologies de registres distribués mettent à l'épreuve les cadres politiques et réglementaires traditionnels et l'aptitude des pouvoirs publics à contrôler les risques pour les utilisateurs finaux et garantir la sécurité juridique. Ces difficultés naissent, en

particulier, de leur potentiel en termes de gouvernance ultra-distribuée et entièrement décentralisée, et du fait qu'elles sont facilement exploitables à l'échelle internationale. Dans le même temps, plusieurs projets de l'OCDE montrent, données à l'appui, qu'une réglementation excessive pourrait freiner l'innovation et induire une perte de compétitivité.

En 2018, les pays de l'OCDE sont convenus de créer le Centre de politique en matière de « *blockchain* ». Cette initiative traduit l'intérêt croissant, à l'échelle internationale, à l'égard de la technologie du « *blockchain* » et fait suite aux travaux de recherche et d'analyse de l'OCDE. Le Centre a pour mission d'aider les pouvoirs publics à mieux comprendre cette technologie, affronter les défis induits par les technologies de registres distribués et leurs applications, et saisir les possibilités qu'elles offrent en termes de réalisation des objectifs d'action et de prestation de services publics plus efficaces.

Informatique quantique

Plusieurs pays se sont dotés d'un programme national de développement de l'informatique quantique (chapitre 11).

Les États-Unis sont l'un des leaders mondiaux de la recherche dans ce domaine. Des milliards de dollars sont consacrés à son financement et environ 50 entreprises et start-ups y mènent des activités liées à la technologie et aux services connexes. Les financements servent aussi bien aux travaux menés à des fins pratiques et commerciales qu'aux activités de recherche scientifique fondamentale. En Europe, la recherche universitaire s'intéresse depuis longtemps à la mécanique quantique. Elle bénéficie de financements de la Commission européenne depuis 1998. En 2018, l'Union européenne a lancé le programme de recherche Quantum Flagship afin de bâtir un socle industriel solide mettant à profit son leadership en matière de recherche scientifique. L'initiative est dotée d'un budget attendu de 1 milliard EUR sur dix ans, destiné à venir compléter les dépenses des différents pays et à stimuler la collaboration internationale. L'initiative met l'accent sur les applications, ainsi que sur la science fondamentale sur laquelle reposent ces technologies.

Si la Chine accuse un retard en matière de développement d'ordinateurs quantiques universels, son projet QUESS (Quantum Experiments at Space Scale, en français Expériences quantiques à l'échelle spatiale) est à l'avant-garde pour ce qui est de la communication et de la cryptographie quantiques au niveau spatial. En 2016, l'Académie des sciences chinoise a lancé le premier « satellite quantique », capable d'émettre des signaux vers différentes stations de réception dans le monde afin de générer une clé secrète aléatoire partagée. Aux premières expérimentations réalisées au sein du territoire chinois ont rapidement succédé des expériences de cryptographie quantique intercontinentale entre la Chine et cinq stations au sol situées en Europe et supervisées par une équipe de l'Université de Vienne et de l'Académie des sciences autrichienne.

La Chine s'efforce par ailleurs de rattraper son retard dans le domaine de l'informatique quantique universelle. En 2015, l'Académie des sciences chinoise et Alibaba Cloud ont créé Alibaba Quantum Laboratory, premier laboratoire d'informatique quantique d'Asie. En 2018, ils ont lancé le premier service public gratuit d'informatique quantique, accessible via le cloud. Toutefois, la puissance de calcul du processeur utilisé ne représente qu'une fraction de celle des services rivaux mis au point par Google et IBM. Baidu, concurrent d'Alibaba, aurait pour sa part investi 15 milliards USD en 2018 dans son propre institut d'informatique quantique.

Outre l'Union européenne, la Chine et les États-Unis, un certain nombre de pays s'intéressent aux technologies quantiques. Ainsi, le Japon, la Corée, Israël, la Fédération de Russie et l'Inde ont défini un programme national de développement de l'informatique quantique. De plus, l'Inde a annoncé des investissements en informatique quantique afin de conserver son avance technologique et d'attirer de nouveaux investissements. Israël entend investir dans des applications des technologies quantiques et du matériel périphérique.

Par ailleurs, dans le cadre des stratégies en matière d'informatique quantique, des collaborations se nouent non seulement entre les acteurs de la communauté scientifique, mais aussi avec des partenaires industriels. Au Canada, l'Université de Waterloo et des partenaires industriels, rassemblés au sein de l'Alliance quantique, échangent des idées de recherche et participent collectivement au développement des technologies quantiques dans le cadre d'ateliers ciblés. Au Royaume-Uni, le Quantum Technology Innovation Centre de l'Université de Bristol est un établissement d'innovation en libre accès dédié.

Moyennant paiement à l'utilisation, des entreprises peuvent accéder à des laboratoires, des espaces de bureaux et des équipements de pointe, tout en bénéficiant du soutien d'experts dans différents domaines commerciaux, technologiques et industriels.

Outre les initiatives nationales, les pays cherchent également à nouer des collaborations internationales. Plusieurs gouvernements ont conclu un accord de partenariat avec IBM, qui installe ses machines sur les campus universitaires. Grâce à cette initiative, les gouvernements espèrent favoriser le développement des compétences en informatique quantique partout dans le monde, en donnant accès aux technologies quantiques les plus récentes.

Les algorithmes de chiffrement sont indispensables au commerce électronique, aux communications mobiles et sur l'Internet, aux services bancaires en ligne et au « *cloud computing* ». De nombreuses méthodes de chiffrement qui sont fiables aujourd'hui pourraient perdre leur efficacité avec l'arrivée de grands ordinateurs quantiques. De là est né le projet PQCRYPTO, lancé par l'Union européenne dans le but de développer des techniques de cryptographie post-quantique. Aux États-Unis, la US National Security Agency a créé le National Institute of Standards and Technology en 2016 pour développer des mécanismes de chiffrement capables de résister à un attaquant disposant d'un calculateur quantique.

Références

Commission européenne (2019), Council Recommendation on Access to Social Protection for Workers and the Self-Employed, 2019/C 387/01, ST/12753/2019/INIT, Bruxelles, *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H1115%2801%29*. [17]

Commission européenne (2016), *European Union eGovernment Action Plan*, page web, *https://ec.europa.eu/digital-single-market/en/egovernment-action-plan-digitising-european-industry* (consulté le 24 March 2020). [4]

Commission européenne (2015), *Stratégie pour un marché unique numérique en Europe*, COM(2015) 232 Final, Commission européenne, Bruxelles, *https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52015DC0192&from=EN*. [2]

Commission européenne (2010), *EUROPE 2020 : Une stratégie pour une croissance intelligente, durable et inclusive*, Commission européenne, Bruxelles, *https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52010DC2020&from=en*. [3]

Commission européenne (2010), *Une stratégie numérique pour l'Europe*, COM(2010) 245 Final, Commission européenne, Bruxelles, *https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52010DC0245&from=fr*. [1]

Gouvernement français (2016), *Loi pour une République numérique*, *http://www.senat.fr/leg/pjl15-744.html*. [12]

Informatics and Information Security Research Center (2016), *2016-2019 National e-Government Strategy and Action Plan (Turquie)*, page web, *https://bilgem.tubitak.gov.tr/en/urunler/2016-2019-national-e-government-strategy-and-action-plan* (consulté le 24 mars 2020). [6]

MCTIC (2018), *Digital Tranformation Strategy*, Ministère des Sciences, de la Technologie, de l'Innovation et des Communications, Brasilia, *http://www.mctic.gov.br/mctic/export/sites/institucional/sessaoPublica/arquivos/digitalstrategy.pdf*. [5]

Ministère des Finances et des Affaires économiques (2019), *Icelandic Financial Plan for the Years 2019-2023*, Ministère des Finances et des Affaires économiques, Reykjavík. [11]

OCDE (2020), « Going Digital integrated policy framework », *Documents de travail de l'OCDE sur l'économie numérique*, n° 292, Éditions OCDE, Paris, *https://dx.doi.org/10.1787/dc930adc-en*. [7]

OCDE (2019), *Recommandation du Conseil sur l'intelligence artificielle*, OECD/LEGAL/0449, OCDE, Paris. [14]

OCDE (2019), *Using Digital Technologies to Improve the Design and Enforcement of Public Policies*, Éditions OCDE, Paris, *https://dx.doi.org/10.1787/99b9ba70-en*. [8]

OCDE (2019), *Vers le numérique : Forger des politiques au service de vies meilleures*, Éditions OCDE, Paris, *https://dx.doi.org/10.1787/7cba1873-fr*. [9]

OCDE (2018), *Perspectives de l'économie numérique de l'OCDE 2017*, Éditions OCDE, Paris, *https://dx.doi.org/10.1787/9789264282483-fr*. [10]

OCDE (2016), *Recommandation du Conseil sur la protection du consommateur dans le contexte du commerce électronique*, OCDE, Paris, *http://dx.doi.org/OECD/LEGAL/0422*. [13]

OCDE (2013), *OECD Privacy Framework*, Éditions OCDE, Paris, *https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm*. [15]

OCDE (2003), *Lignes directrices de l'OCDE régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses*, Éditions OCDE Paris, *https://doi.org/10.1787/9789264103573-en-fr*. [16]

Notes

1. Les groupes de parties prenantes comprennent, entre autres, les entreprises, la société civile, la communauté technique de l'Internet et les syndicats.
2. Les pays de l'OCDE ayant répondu au Questionnaire de 2019 de l'OCDE sur les politiques de l'économie numérique sont les suivants : Allemagne, Australie, Autriche, Belgique, Canada, Chili, Colombie, Corée, Danemark, Espagne, Estonie, États-Unis, Finlande, Grèce, Hongrie, Islande, Israël, Italie, Japon, Lettonie, Lituanie, Luxembourg, Mexique, Norvège, Pays-Bas, Pologne, Portugal, République tchèque, Royaume-Uni, Slovénie, Suède, Suisse et Turquie.

3. Les économies partenaires ayant répondu au Questionnaire de 2019 de l'OCDE sur les politiques de l'économie numérique sont les suivantes : Brésil, Costa Rica, Fédération de Russie, Singapour et Thaïlande.
4. Les États-Unis ont adopté, pour leur politique en matière de numérique, une stratégie de portefeuille s'appuyant sur un ensemble de politiques, de réglementations et de lois axées sur des questions et/ou des secteurs spécifiques qui, ensemble, concourent au développement et à la progression de la transformation numérique. Cette stratégie comprend notamment (sans ordre de priorité) les politiques régissant les télécommunications et l'Internet, la protection de la vie privée dans l'environnement numérique, la cybersécurité, les données massives, l'offre intelligente de services informatiques, les données ouvertes, la R-D dans le domaine des technologies de l'information, les technologies d'enseignement, l'éducation en ligne et les systèmes d'information environnementale. Cette stratégie de portefeuille se décline aux niveaux national (fédéral) et infranational (États et localités). Les États-Unis œuvrent en faveur du développement et de l'amélioration continus des technologies qui sous-tendent l'économie de la transformation numérique et contribuent aux progrès dans ses domaines prioritaires.
5. Le centre de gouvernement est généralement chargé d'assurer un soutien au plus haut niveau de l'exécutif.
6. *https://www.oecd.ai/*.

Perspectives de l'économie numérique de l'OCDE 2020

(VERSION ABRÉGÉE)

Cette version abrégée est la traduction partielle de la version anglaise des Perspectives de l'économie numérique de l'OCDE 2020. Elle contient le résumé de la publication ainsi que le chapitre 2 où sont analysées les évolutions récentes des stratégies numériques nationales et les principales évolutions liées aux politiques centrées sur la connectivité, l'utilisation du numérique, la gouvernance des données, la sécurité, la protection de la vie privée, l'innovation, le travail et des technologies clés telles que l'intelligence artificielle (IA), la technologie du « blockchain » et l'informatique quantique.

Dans son ensemble, cette troisième édition des Perspectives de l'économie numérique de l'OCDE propose un tour d'horizon complet des tendances, de l'évolution des politiques et des données de l'économie numérique, du côté de l'offre comme de la demande. Elle illustre les incidences de la transformation numérique sur les économies et les sociétés. Enfin, elle apporte un éclairage particulier sur la façon dont la pandémie de COVID-19 amplifie les opportunités et les défis induits par la transformation numérique.

Cette publication s'inscrit dans le cadre du projet « Going Digital » de l'OCDE. Dans un monde résolument tourné vers le numérique et les données, ce projet vise à fournir aux décideurs les outils dont ils ont besoin pour aider leurs économies et leurs sociétés à prospérer.

Pour en savoir plus, rendez-vous sur : ***www.oecd.org/going-digital.***

#GoingDigital

PDF ISBN 978-92-64-93148-0

9 789264 931480