Stratégie internationale de la France pour le numérique

SOMMAIRE

PRÉFACE DU MINISTRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES ET DU SECRÉTAIRE D'ÉTAT AUPRÈS DU PREMIER MINISTRE, CHARGÉ DU NUMÉRIQUE

Nous vivons à l'âge numérique, un âge de transformation globale et de rupture stratégique. En s'accélérant, la révolution numérique bouleverse l'ensemble des sphères d'activité humaine et précipite l'émergence d'un espace numérique mondial, nouveau milieu à part entière de conduite des relations internationales. Qu'il s'agisse de la réussite de notre économie dans la compétition mondiale ou des conditions de la stabilité et de la puissance à l'échelle internationale, le numérique est désormais un enjeu de premier ordre pour notre politique étrangère et pour l'action publique dans son ensemble.

L'espace numérique est porteur de progrès et de croissance, il peut donner à nos valeurs démocratiques un nouveau souffle, mais, dans le même temps, nous faisons face au risque d'un monde numérique manipulé contre les vertus d'ouverture dont il devait être le garant. Qu'il s'agisse du domaine économique ou des enjeux de sécurité, un effort de régulation est nécessaire afin d'organiser un ordre numérique équitable et sûr, favorable au développement de chacun.

Répondre à ces défis, dessiner les contours d'un monde numérique fait de coopération, d'ouverture et de confiance, tels sont les objectifs de la stratégie internationale de la France pour le numérique. Ce document fixe ainsi un cap et une feuille de route à notre action internationale pour les années à venir. Le modèle numérique que la France souhaite promouvoir s'inscrit dans un horizon européen. L'Union européenne est, en effet, le bon niveau pour peser concrètement et promouvoir de façon efficace le modèle d'un monde numérique conforme à nos intérêts et à nos valeurs.

Élaborée en concertation avec l'ensemble des ministères concernés, cette stratégie a également fait l'objet d'une consultation publique afin de recueillir les avis de nos concitoyens. Pour une large partie d'entre eux, le numérique constitue désormais un élément quotidien de leur existence. Pour être pris en compte dans la diversité de ces enjeux, le numérique exige une diplomatie renouvelée capable de faire dialoguer la puissance publique et les acteurs privés, le monde de la recherche et les membres de la société civile.

Nous ne voulons pas nous laisser enfermer dans une alternative simplificatrice entre la fermeture et le laisser-faire ; nous voulons dessiner une autre voie, faite d'équilibre entre ouverture et protection, coopération et liberté d'action, afin d'assurer la stabilité internationale adaptée et de maintenir notre puissance à l'âge numérique. Cette créativité multilatérale, réaliste et pragmatique, c'est la méthode que la France souhaite porter afin de définir le monde numérique que nous souhaitons et le rôle que la France et l'Europe doivent y jouer dans les décennies à venir. Un monde numérique où notre autonomie est assurée, où nos acteurs économiques sont compétitifs et où nos droits sont préservés. C'est le chemin que propose la stratégie internationale de la France pour le numérique.

Mounir Mahjoubi
Secrétaire d'État
auprès du Premier ministre,
chargé du Numérique

Jean-Yves le Drian
Ministre de l'Europe
et des Affaires étrangères

AVANT-PROPOS

La croissance du monde numérique et les nouvelles possibilités qui en découlent sont liées aux principes qui ont façonné son développement : ouverture, neutralité des réseaux, liberté d'accès garantie par une architecture décentralisée. Ces principes ont permis, en près de deux décennies, la mise en réseau de plus de la moitié de l'humanité, une transformation en profondeur des modèles de création de valeur, une dynamique d'innovation qui change la vie quotidienne des individus.

L'Union européenne, et la France en particulier, a largement bénéficié de cette révolution numérique dont les potentialités ne cessent de se déployer. Il n'est pas exagéré de dire que le numérique est désormais au cœur de nos sociétés et de nos vies. Il les innerve sous de multiples formes, à travers les plateformes Internet, les réseaux sociaux, l'économie collaborative, le traitement massif des données, les objets connectés ou encore l'intelligence artificielle. Il transforme en profondeur nos relations sociales.

Alors que le numérique s'impose comme un nouveau lieu de possibilités économiques, sociales et politiques, il est nécessaire de préserver les principes sur lesquels il est fondé. Or, le monde numérique fait aujourd'hui face à plusieurs défis, qui peuvent les remettre en cause. L'instabilité et l'insécurité liées à l'accroissement des risques et des menaces dans le cyberespace, ainsi que l'usage d'Internet à des fins criminelles ou terroristes, peuvent fragiliser la confiance dans le monde numérique. Les États autoritaires, soucieux d'affirmer leur souveraineté sur le monde numérique, recherchent le contrôle des réseaux, au détriment de l'ouverture qui en constitue le fondement et aux dépens des droits fondamentaux. Parallèlement, un nombre restreint de grandes entreprises numériques joue un rôle ambivalent : les grandes plateformes se sont en effet révélées être les catalyseurs de la révolution numérique dans ses aspects les plus bénéfiques, mais sont aujourd'hui en mesure d'abuser de leur position dominante pour limiter la concurrence, et maintenir les utilisateurs dans des systèmes fermés, jouant des frontières étatiques, tantôt pour s'en prévaloir, tantôt pour s'en affranchir.

En réponse, il est nécessaire de promouvoir un environnement numérique de confiance, propice à l'éclosion de nouveaux acteurs, qui garantisse un fonctionnement démocratique du monde numérique respectueux des objectifs légitimes de politiques publiques, qui permette une égale participation à la fois des États et des sociétés attachés à un réseau ouvert, et qui favorise une plus grande inclusion numérique. C'est la vision que défend la France. Elle rejoint en cela d'autres acteurs, notamment certaines puissances émergentes, qui se sont aussi engagés dans cette voie.

L'Union européenne a vocation à jouer un rôle de premier plan pour promouvoir cette vision. Ensemble, les États membres disposent de la masse critique et des atouts nécessaires pour porter une conception du numérique qui soit fidèle aux valeurs européennes et qui assure un équilibre satisfaisant entre le développement économique, les nouvelles interactions sociales, le respect des droits et libertés fondamentaux et la sécurité, permettant à l'Union d'atteindre une autonomie stratégique en la matière. Cela nécessite que l'Union européenne soutienne, par le développement d'un marché unique numérique, une économie numérique européenne forte et innovante.

L'Union européenne peut ainsi incarner et préserver, à l'échelle mondiale, un modèle de monde numérique ouvert, diversifié et de confiance. La France contribuera à l'émergence d'un tel pôle européen au sein d'un monde numérique en pleine transformation. Elle doit, pour ce faire, consolider ses propres capacités afin de promouvoir efficacement sa vision, ses principes et ses intérêts dans le monde numérique.

La stratégie internationale de la France pour le numérique présente les principes et les objectifs qui guident notre action en vue de :

- promouvoir un monde numérique ouvert, diversifié et de confiance à l'échelle globale ;
- affirmer un modèle européen d'équilibre entre croissance économique, droits et libertés fondamentaux et sécurité ;
- renforcer l'influence, l'attractivité, la sécurité et les positions commerciales de la France et des acteurs français dans le monde numérique.

1. PROMOUVOIR UN MONDE NUMÉRIQUE OUVERT, DIVERSIFIÉ ET DE CONFIANCE

La gouvernance d'Internet, c'est-à-dire la définition et la mise en œuvre des règles qui régissent ce réseau en tant que système global, doit avoir pour objectifs d'en préserver le caractère ouvert et diversifié tout en renforçant la confiance dans son utilisation. La France a depuis longtemps reconnu l'utilité d'une approche multi-acteurs, en incluant les États, le secteur privé et les sociétés civiles. Elle a manifesté son soutien à ces mécanismes de gouvernance, auxquels elle participe activement.

Toutefois, la nature des questions auxquelles la gouvernance d'Internet doit répondre évolue profondément. Elle doit permettre d'assurer :

- la gestion des ressources critiques d'Internet, afin de préserver le caractère commun et interopérable du réseau face aux risques de fragmentation ;
- l'accès de tous à un Internet offrant la plus grande diversité de services, d'usages et d'expressions ;
- une diversité culturelle et linguistique représentative de la pluralité des cultures et des visions du numérique ;
- la régulation des conflits et la réduction des atteintes aux biens et aux personnes dans un espace numérique transnational ;
- le respect et la protection des libertés fondamentales.

Cette gouvernance n'est légitime et effective que dans la mesure où elle est aussi transparente, démocratique, inclusive et assure une représentation réelle de l'ensemble des parties. À cet égard, la France considère que les responsabilités particulières et les préoccupations légitimes des États, attachées à poursuivre l'intérêt public et bénéficiant de la légitimité démocratique de représenter leurs citoyens, doivent être mieux prises en compte. La France œuvre ainsi dans les différentes enceintes pertinentes pour mettre en place un modèle équilibré de gouvernance d'Internet où tous les acteurs (société civile, réseau académique, communauté technique, acteurs économiques et États), dans leurs compétences respectives, puissent agir efficacement et où le droit des États à réguler pour des objectifs légitimes de politique publique soit préservé.

1.1. Préserver un environnement international numérique ouvert

L'ouverture qui caractérise Internet demeure le principal facteur de sa croissance depuis trois décennies. Elle constitue la caractéristique essentielle de cette infrastructure numérique. Internet repose cependant sur des ressources critiques qui en conditionnent le bon fonctionnement, notamment le système de noms de domaine, les infrastructures physiques des réseaux et les standards techniques. Elles sont gérées principalement par l'Internet Corporation for Assigned Names and Numbers (ICANN, chargée du fonctionnement et de la gestion des serveurs racines du système de noms de domaine), l'Internet Engineering Task Force (IETF, chargé des protocoles de normalisation des couches basse de l'Internet) et le World Wide Web Consortium (W3C, chargé des standards du web).

Ces organismes présentent deux caractéristiques :

- les États-Unis, lieu de naissance d'Internet et vecteur de son expansion mondiale, y jouent un rôle prépondérant. Afin de garantir la représentativité et donc la légitimité de ces institutions, il est nécessaire de promouvoir, au sein de leur gouvernance, une plus grande diversité ;
- leur gouvernance est organisée selon un modèle multi-acteur.

La gouvernance de ces ressources doit aujourd'hui s'adapter aux nouveaux enjeux juridiques, économiques et sociaux que génèrent le développement du monde numérique et la dépendance croissante des sociétés développées aux réseaux numériques. Certains États mettent en place des infrastructures nationales restreignant l'ouverture et

l'interopérabilité avec le réseau global, tirant argument de l'influence des États-Unis sur une infrastructure devenue stratégique. Or, ce risque de fermeture et de fragmentation du monde numérique est aussi peu désirable que l'hégémonie d'un acteur. Pour cela, une réforme de sa gouvernance est nécessaire.

L'influence d'un État dans la gouvernance d'Internet dépend du poids de son économie numérique dans la mesure où le modèle multiparties prenantes laisse une large place au secteur privé. Ainsi, la stratégie internationale de la France pour accroître son influence dans la gouvernance mondiale dépend essentiellement de sa capacité à promouvoir les entreprises françaises du numérique au-delà du seul marché national et européen, et à fédérer une diversité d'acteurs publics comme privés pour déployer des actions cohérentes dans les différents foras de gouvernance.

Afin de préserver un Internet ouvert et interopérable, la France poursuivra donc les objectifs suivants :

Promouvoir une gouvernance d'Internet démocratique, représentative et inclusive

La France considère qu'Internet doit demeurer une infrastructure commune ouverte pour que les externalités positives attendues de la transformation numérique jouent pleinement leur rôle. La gouvernance multi-acteur, qui a su faire preuve de son efficacité, doit être maintenue et renforcée afin de préserver l'équilibre face à ces menaces de fragmentation internes et externes. Elle doit cependant évoluer pour retrouver la légitimité renforcée qui lui est nécessaire :

- en premier lieu, un nouvel équilibre du modèle multi-acteur doit être recherché afin d'améliorer l'articulation entre la diversité des parties prenantes et la spécificité du rôle des États sur le plan international, mais aussi permettre une meilleure association des diverses parties prenantes ;
- en second lieu, une plus grande diversité des acteurs doit être promue afin de garantir la représentativité et la légitimité des instances de gouvernance. La France poursuit l'effort qu'elle a engagé, en ce sens, au sein de l'ICANN. La fin de la tutelle américaine sur l'ICANN, officielle depuis le 1er octobre 2017, doit désormais s'accompagner d'une réelle diversification des équipes dirigeantes de cette organisation et de ses structures ; la France œuvre en ce sens en proposant la création d'une structure pérenne de promotion de la diversité ;
- enfin, les questions relatives aux conflits de juridiction sur Internet, au droit applicable aux noms de domaine génériques (gTLD) et à l'application en ligne des droits fondamentaux (tels que la protection de la vie privée) doivent être abordées au niveau international, faute de quoi la fragmentation d'Internet s'accentuera.

La France compte sur l'investissement et sur la mobilisation de la société civile et des différents services de l'État concernés afin que ces derniers continuent à s'engager et à participer aux travaux et aux négociations (notamment au sein des instances de gouvernance et des instances techniques de l'Internet) en concertation avec les différents ministères sous la coordination du ministère des Affaires étrangères (MEAE).

> **C'est au sein de diverses enceintes multi-acteurs (Internet Corporation for Assigned Names and Numbers, Forum sur la gouvernance d'Internet) et multilatérales (Union internationale des télécommunications et Organisation des Nations unies, Sommet mondial sur la société de l'information) que la France défend ses positions en faveur d'une gouvernance d'Internet démocratique, représentative et inclusive : le ministère de l'Europe et des Affaires étrangères et le ministère de l'Économie et des Finances représentent la France au sein du comité consultatif des gouvernements (GAC en anglais) de l'ICANN, dans lequel participent les gouvernements de plus de 150 pays. La France a obtenu la vice-présidence du GAC en 2016-2017.**

Pérenniser l'interopérabilité des réseaux, services et applications numériques sur Internet

L'interopérabilité des réseaux sur Internet, services et applications numériques est la condition de son ouverture. Elle repose sur des standards internationaux (ex : GSM, 4G, 5G pour l'Internet mobile) et des protocoles (ex : IPv4, IPv6) définis dans diverses enceintes (ex : Internet Engineering Task Force, World Wide Web Consortium, 3 Generation Partnership Project, UIT, GSMA, ETSI Union internationale des télécommunications). La définition de ces standards présente un intérêt stratégique en termes industriels, de sécurité et de protection des données personnelles.

Il est donc nécessaire de mieux fédérer les efforts des acteurs français et européens, publics comme privés, au sein de ces instances, afin de peser sur l'élaboration des standards et protocoles, mais également de définir une approche européenne de la normalisation, notamment au regard de l'émergence de nouvelles technologies structurantes (comme l'Internet des objets).

LA CONFÉRENCE MONDIALE DES RADIOCOMMUNICATIONS

La dernière Conférence mondiale des radiocommunications (CMR-15) de l'Union internationale des télécommunications (organisation du système des Nations unies en charge des technologies de l'information et de la communication) a eu lieu en novembre 2015. Elle a notamment permis d'identifier des bandes de fréquences au niveau mondial afin de soutenir l'essor du développement du très haut débit mobile, mais aussi la mise en place d'un suivi permanent des vols aériens par satellite. Elle a également décidé de nouvelles attributions de fréquences pour le secteur spatial (industrie et recherche), tout en assurant la préservation de fréquences déjà dédiées aux satellites.

Le bilan de cette Conférence est très satisfaisant pour la France, dont l'action est pilotée par l'Agence nationale des fréquences (ANFR), qui a su promouvoir des évolutions dans le domaine régalien tout en faisant en sorte que l'évolution du cadre international réponde aux attentes de différents secteurs utilisateurs de fréquences radioélectriques.

La prochaine conférence, qui aura lieu en 2019, la CMR-19, traitera d'enjeux d'une importance comparable à ceux de la CMR-15 : identification de nouvelles bandes pour répondre au développement de la 5G, pour augmenter la capacité des réseaux wi-fi à 5 GHz, pour de nouvelles solutions de connectivité apportées par les constellations de satellites non géostationnaires, les drones ou les ballons, ou encore pour les systèmes de transport intelligents (qu'ils soient routiers, ferroviaires ou maritimes). La CMR-19 se penchera également sur la définition des conditions réglementaires pour la mise en œuvre du système mondial pour la détresse et la sécurité aéronautique élaboré par l'Organisation de l'aviation civile internationale.

1.2. Favoriser l'accès de tous à un numérique diversifié

L'accès à Internet est encore très inégalement réparti dans le monde : trois personnes sur dix n'ont pas de téléphone mobile ni d'accès à un Internet mobile de qualité, six personnes sur dix n'ont pas d'accès à Internet. Or, un Internet ouvert doit aussi être un Internet accessible à tous, et la transformation numérique des pays en développement est un levier déterminant de l'amélioration de leurs conditions économiques, sociales et culturelles. L'accès du plus grand nombre d'utilisateurs à Internet constitue ainsi l'un des objectifs de développement durable retenus par l'ONU. Il est important que cet objectif, primordial, soit accompagné d'une politique de sensibilisation, de formation et d'accompagnement aux usages pour empêcher que cette plus grande accessibilité ne soit promue et captée par un petit nombre d'acteurs économiques. Il est également nécessaire de continuer à promouvoir, aux niveaux européen et global, le principe de neutralité du Net, garant de l'ouverture et de la démocratisation de l'Internet.

Au-delà de son accessibilité, Internet doit offrir un contenu diversifié de services, d'usages et d'expressions. La révolution numérique a entraîné une nouvelle dynamique culturelle et crée de nouvelles potentialités en matière de création et d'exposition, d'offre de biens

culturels dématérialisés, de financement comme d'égalité dans l'accès aux œuvres. Toutefois, l'abondance de l'offre culturelle numérique ne met pas nécessairement à l'abri de certains risques d'homogénéisation et de mimétisme des comportements culturels, eu égard en particulier aux nouveaux outils numériques. Les phénomènes de prescriptions automatiques (algorithmes de recommandations, réseaux sociaux) sont amplifiés dans l'économie numérique.

Aussi la France poursuivra-t-elle les objectifs suivants :

Promouvoir sur le plan international l'accès à un Internet abordable, ouvert et sûr

Le développement de l'accès à un Internet abordable, ouvert et sûr figure au nombre des principaux objectifs poursuivis par la France dans le cadre du plan « Développement et Numérique ». La France s'engage ainsi à accompagner les pays en développement dans la mise en place d'un accès universel aux services numériques. Cela nécessite de soutenir le développement des infrastructures, des services, de la régulation et de la gouvernance :

- en apportant son expertise, notamment par le biais de l'Agence française de développement (AFD) et des opérateurs d'assistance technique (Expertise France) ;
- en soutenant les grands acteurs français du numérique pour accompagner ce développement dans leurs politiques d'exportation et de pénétration de ces marchés.

La France soutiendra par ailleurs le développement d'un large accès aux réseaux numériques, aux médias numériques (par le biais d'aide au lancement de la TNT, de support à des *web activities* et d'accompagnement à la formation pour les professionnels de l'information) et la promotion des technologies innovantes transparentes et sécurisées (utilisation de la *blockchain* notamment pour les procédures de transfert d'argent aux migrants, enregistrements d'états civils et de cadastres). Comme la France a pu le souligner au sein de différentes instances (comme lors du Sommet mondial sur la société de l'information en 2015), ce soutien est nécessaire pour permettre, à terme, à chacun de pouvoir accéder à Internet, quelles que soient ses ressources et sa localisation, afin de bénéficier d'une société de l'information inclusive où chacun est en mesure de créer, d'accéder et de partager les informations et les connaissances acquises.

Dans cette perspective, la France entend continuer à développer l'accessibilité des sites Internet publics, en particulier auprès des personnes handicapées, en faisant notamment confiance à l'innovation française. Elle entend également s'engager pour promouvoir un accès aux ressources et savoirs numériques qui soit égal pour tous, quel que soit le genre.

LE PLAN DÉVELOPPEMENT ET NUMÉRIQUE

Le Plan Développement et Numérique (PDN) mis en place par la France a pour objectif d'offrir une réponse d'ensemble aux questions soulevées par l'avènement de la transition numérique dans les pays en développement. Il se structure ainsi autour de trois enjeux principaux qui rejoignent le positionnement de la France dans d'autres enceintes internationales :

- **l'accès à un Internet abordable, ouvert, sûr et multiculturel ;**
- **la construction d'une économie numérique ;**
- **l'utilisation des technologies issues du numérique au service des objectifs de développement (par exemple, développement du financement participatif).**

Les entreprises françaises du numérique (start-up, PME/ETI et grands groupes) peuvent constituer des relais et des acteurs majeurs pour porter cette transition numérique dans les marchés en développement.

L'engagement de la France se situe dans la droite ligne des objectifs de développement durable (et plus particulièrement l'objectif n° 9.C qui vise à construire un accès universel et abordable à Internet dans les pays les moins avancés d'ici à 2020). Enfin, dans le cadre du Partenariat mondial des données du développement durable, la France accompagnera les pays en développement dans leurs efforts de renforcement de leurs capacités de production et de diffusion de données scientifiques pour le suivi des ODD. La France agit pour l'accès du plus grand nombre aux technologies de l'information et de la communication au sein de diverses enceintes internationales, notamment dans le cadre des Nations unies.

Le plan développement et numérique se décline en huit objectifs et 24 actions concrètes (http://www.economie.gouv.fr/lancement-plan-daction-developpement-et-numerique).
Un exemple d'action résultant de ce plan, les journées Afrique, Développement et Numérique des 26, 27 et 28 octobre 2016, a permis de rassembler des grands groupes et des représentants des écosystèmes émergents d'Afrique afin d'améliorer l'action des entreprises numériques dans les politiques d'aide au développement et à destination des pays africains. Par ailleurs, le 27e Sommet des chefs d'État Afrique-France qui s'est tenu à Bamako le 14 janvier 2017, faisant suite au Sommet de Paris de décembre 2013, a permis à la France de :

- **rappeler son attachement à un Internet ouvert, sûr et multiculturel ;**
- **présenter et appuyer les politiques de soutien aux start-up, aux écosystèmes et à la formation des jeunes dans le secteur du numérique ;**
- **promouvoir l'offre française en matière de numérique et la volonté de collaboration avec les pays africains.**

Favoriser la diversité à l'échelle mondiale des expressions linguistiques et culturelles en ligne

La révolution numérique permet l'enrichissement et l'élargissement de l'offre et des contenus, mais crée aussi de nouvelles possibilités pour l'innovation et la créativité. Cependant, elle appelle aussi à un devoir de vigilance sur la nécessité de préserver la diversité culturelle. La captation de la valeur par les plateformes globales au détriment des producteurs de contenus et des ayants droit comporte le risque d'un tarissement du financement de la création et d'un assèchement du renouvellement des talents.

La France promeut ainsi le développement et le renforcement d'un Internet multiculturel dans le cadre de la mise en œuvre de la Convention de 2005 de l'UNESCO afin de garantir la pertinence des principes fondamentaux qui la fondent : la double nature économique et culturelle des biens et services culturels ; le droit des États d'adopter et d'appliquer les politiques nécessaires au soutien de la création afin d'assurer des expressions culturelles variées et de qualité ; la possibilité pour les publics d'accéder à l'intégralité des expressions culturelles de leur propre pays et aux autres cultures du monde, sans être limités par des considérations d'ordre économique ou idéologique ; le rôle déterminant de la culture comme facteur de développement.

La création de « l'École française numérique à l'étranger » qui permet à la fois de répondre à la demande croissante d'éducation bilingue francophone et de français dans le monde tout en soutenant la diffusion de la langue et du modèle d'enseignement, s'inscrit dans cet effort. La France promeut par ailleurs des partenariats à travers la plateforme « France Université Numérique » pour aider à la coconstruction de projets et de partenariats entre établissements français et étrangers.

Parallèlement, la France souhaite promouvoir le rôle de l'Organisation internationale de la Francophonie dans les instances internationales de régulation du réseau ainsi que la production et la diffusion de biens communs numériques (logiciels libres et contenus ouverts). La France souligne par ailleurs le dynamisme de l'OIF dans le domaine du numérique et soutient la mise en œuvre de la Stratégie de la Francophonie numérique Agir pour la diversité dans la société de l'information adoptée lors de la XIVe Conférence des chefs d'État et de gouvernement des pays ayant le français en partage.

Partager nos innovations techniques et institutionnelles avec nos partenaires

La France pourrait ouvrir à ses partenaires quelques-unes de ses innovations administratives rendues possibles par les outils numériques, comme service-public.fr ou legifrance, pour renforcer notre stratégie d'influence par le droit.

Associer les enjeux de transition écologique et la transition numérique au plan international

La transition numérique doit être pensée de pair avec la transition écologique. Il s'agit de donner du sens à la transition numérique en la mettant au service des défis écologiques, tout en

réduisant les coûts environnementaux générés par la circulation massive de données.

La France rappelle son attachement aux enjeux de transition écologique et numérique. Elle soutient ainsi de nombreuses initiatives, notamment le EU Code of Conduct for Data Centers (code de bonne conduite énergétique pour les centres de données européens) et l'initiative Green Tech (réseau d'incubateur sous l'impulsion du ministère de la Transition écologique et solidaire qui a pour but de promouvoir les start-up dont les projets innovants concourent à la transition écologique).

Faire progresser la conscience internationale sur le rôle des algorithmes et l'encadrement de leur utilisation

Les principaux acteurs du numérique – plateformes, moteurs de recherche et applications – fondent en grande partie leur activité sur l'utilisation d'algorithmes. Ces derniers constituent un facteur de compétitivité et sont protégés par les acteurs. Or, ces algorithmes sont susceptibles de créer des phénomènes de prescription automatique et de « bulles de filtres », dont les conséquences problématiques ont notamment été soulignées par le Conseil d'État en 2015 : enfermement de l'internaute dans une « personnalisation » dont il n'est pas maître, confiance abusive dans les résultats d'algorithmes perçus comme objectifs et infaillibles ; problèmes d'équité du fait de l'exploitation toujours plus fine des données personnelles. Des propositions peuvent être avancées :

- envisager la mise en place d'une agence de notation européenne qui permette de garantir la confiance et la loyauté des plateformes dans le respect de l'utilisation des données personnelles (l'Inria est notamment en train de réfléchir à ce sujet avec un projet sur la transparence des algorithmes) ;
- prolonger la réflexion – notamment éthique – sur l'impact des algorithmes et la « dépossession » des choix collectifs et individuels : financement de projets de recherche, discussion avec les acteurs, développement du testing, chartes de bonne conduite, outils mettant en évidence les biais, encadrement des algorithmes prédictifs… Au niveau national, la CNIL, missionnée par la Loi pour une République numérique, a conduit en 2017 une réflexion sur les enjeux éthiques et les questions de société soulevés par l'évolution des technologies numériques.

> **GROUPES DE TRAVAIL « NUMÉRIQUE » DU G7 ET DU G20**
> **En 2016 et en 2017, le G7 et le G20 ont mis en place des groupes de travail dédiés spécifiquement au numérique. La présidence allemande du G20 a organisé en avril 2017 une réunion des ministres du numérique à Düsseldorf, au cours de laquelle ont été adoptées une déclaration politique de haut niveau et une feuille de route. Ces documents proposent une vision commune sur les enjeux de la transformation numérique de l'économie et identifient quelques enjeux prioritaires : réduire la fracture numérique, maximiser le levier que constitue le numérique pour la croissance et l'emploi, accompagner et accélérer la numérisation de l'industrie, renforcer la sécurité et la confiance dans l'économie numérique. En septembre 2017, la présidence italienne du G7 a organisé à Turin une réunion des Ministres du numérique, au cours de laquelle une déclaration politique a été adoptée.**
> **Lors des réunions de ces groupes de travail, la France a notamment plaidé pour que le G7 et le G20 abordent des sujets tels que la cybersécurité, la concurrence dans l'économie numérique, le rôle des plateformes Internet, la transparence et la régulation des algorithmes, le développement de l'intelligence artificielle ou encore les problématiques fiscales spécifiques au numérique et permettent le renforcement de la coopération internationale sur ces sujets.**

Rester vigilant face à la désinformation et aux tentatives d'ingérence

L'élaboration et la diffusion active de fausses informations sur Internet et les réseaux sociaux ne cessent d'augmenter. Regroupés sous le vocable de fausses informations (*fake news*), ces articles ne satisfont pas aux standards de publication fiables et reposent sur des informations partiellement ou entièrement fausses (qu'elles soient créées de toutes pièces ou travesties). Ces efforts peuvent viser à manipuler l'opinion publique et nuire à la crédibilité des institutions et des médias. Des statistiques simples – environ 45 % des

Américains et des Français utilisent les réseaux sociaux comme source principale d'information (Reuters 2016[1]), 63 % des Américains s'informent d'abord en utilisant les réseaux sociaux (Pew Research Center, 2016[2]) – soulignent l'importance de l'enjeu.

L'impact de ces fausses informations, leur capacité à se diffuser rapidement sur les réseaux sociaux et à influencer les opinions publiques doivent être considérés et appréhendés par nos sociétés démocratiques en cohérence avec nos principes. Ces dernières doivent être en mesure de se saisir de ces enjeux, par exemple, en développant leurs propres outils pour lutter contre la création et la diffusion de ces fausses informations. Par ailleurs, le ministère de l'Europe et des Affaires étrangères répondra en fonction du contexte à la diffusion de fausses nouvelles concernant la politique internationale de la France.

Responsabiliser les acteurs du numérique dans la lutte contre la désinformation

Il importe également de responsabiliser davantage les plateformes numériques, notamment lorsque de fausses informations sont diffusées et amplifiées par leur intermédiaire, y compris par des puissances étrangères. Plusieurs pistes de réflexion peuvent être explorées :

- déréférencement et retrait le plus rapide possible par les plateformes des fausses informations de nature à porter atteinte au pluralisme et à l'honnêteté de l'information ;
- mobilisation des plateformes, à travers le développement de l'auto- et la corégulation (code de bonne conduite, engagement contractuel avec l'État) ;
- vigilance des plateformes sur les sources de revenus problématiques qui pourraient favoriser l'amplification et la diffusion de fausses nouvelles.

1.3 Renforcer la confiance sur Internet

La France estime que le multilatéralisme doit jouer tout son rôle dans l'élaboration de règles et de normes communes pour préserver la paix et la sécurité dans l'univers numérique. Les questions des règles et normes applicables aux actions des États dans le cyberespace et dans la lutte contre la cybercriminalité ne peuvent trouver de réponses effectives que dans un cadre multilatéral.

La France a ainsi pris une part active aux travaux menés par les cinq Groupes d'experts gouvernementaux des Nations unies sur la cybersécurité (UN GGE) successifs. Ceux-ci ont notamment permis d'acter, dès 2013, la reconnaissance de l'application du droit international public, en particulier de la Charte des Nations unies, à la conduite des États dans le cyberespace et son caractère indispensable pour la préservation de la paix et de la sécurité internationales.

La cybercriminalité est une menace croissante, car elle crée des infractions informatiques nouvelles tout en facilitant la commission des infractions classiques. Par ailleurs, les terroristes se servent d'Internet à des fins de propagande, de recrutement, d'achat d'armes ou de préparation d'attentats. La promotion et la mise en œuvre de la Convention de Budapest pour lutter contre la cybercriminalité constituent un autre enjeu global de gouvernance d'Internet. En raison de son caractère transnational, Internet soulève des problèmes nouveaux en matière de lutte contre la criminalité que seuls des mécanismes de coopération internationale fondés notamment sur des incriminations pénales communes peuvent résoudre.

La France poursuivra ainsi les objectifs suivants :

Assurer le plein respect du droit international dans l'espace numérique

La France considère comme un fondement de sa sécurité que les rapports entre États soient régis par le droit international et la Charte des Nations unies. Or si l'applicabilité du droit international public a été reconnue dans le cyberespace, les conditions et les modali-

1. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital-News-Report-2016.pdf
2. http://www.journalism.org/2015/07/14/the-evolving-role-of-news-on-twitter-and-facebook/

tés de cette application restent à définir dans un cadre multilatéral qui permette l'accord le plus large entre États.

La France, membre permanent du Conseil de sécurité, poursuivra activement les travaux visant à permettre une application efficace et pertinente du droit international dans le monde numérique, à construire le consensus nécessaire entre États sur la reconnaissance de ces conditions d'application et à mettre en œuvre effectivement ces principes juridiques.

LE GROUPE DES EXPERTS GOUVERNEMENTAUX DE L'ONU SUR LA CYBERSÉCURITÉ (UNGGE)
Depuis 2004 s'est réuni, à cinq reprises, au niveau des Nations unies, un Groupe d'experts gouvernementaux sur la cybersécurité. L'expert français au sein du Groupe est l'ambassadeur pour la cyberdiplomatie et l'économie numérique.
En 2013, le Groupe est parvenu à s'accorder sur la reconnaissance de l'applicabilité du droit international existant, et notamment de la Charte des Nations unies à la conduite des États dans le cyberespace. En 2015, les experts du Groupe ont approfondi ce travail en s'accordant sur un socle d'engagements volontaires de bonne conduite (« normes de comportement »). Les États ont ainsi été encouragés à faire preuve de transparence sur leur organisation et posture nationales en matière de cybersécurité, à renforcer leur propre cybersécurité, à adopter un comportement coopératif vis-à-vis d'États victimes d'attaques informatiques, à lutter contre la prolifération d'outils informatiques malveillants ou encore à s'engager à ne pas endommager les infrastructures critiques d'un autre État, hors contexte d'opérations militaires. En revanche, malgré plusieurs avancées importantes lors du cycle de négociations 2016-2017, le Groupe n'est pas parvenu à se mettre d'accord sur un nouveau rapport de consensus. L'échec de ce dernier cycle de négociations ne remet nullement en cause les principes agréés au cours des années précédentes. De plus, il ne doit pas mettre un terme aux efforts de la France et de la communauté internationale en vue de promouvoir des normes de comportement et mesures de confiance en faveur de la stabilité et de la sécurité internationale du cyberespace. La France fera ainsi des propositions pour poursuivre l'effort de développement de normes internationales dans ce domaine.

Combattre à l'échelle internationale la cybercriminalité

Les dispositifs internationaux de coopération doivent par leur souplesse permettre de répondre aux enjeux technologiques et juridiques des investigations transfrontières. La France soutient la mise en œuvre des outils indispensables à la coopération internationale.

LOI N° 2016-731 DU 3 JUIN 2016
Ainsi, en matière pénale (article 706-72-2 du code de procédure pénale, créé par la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale), une compétence nationale du parquet de Paris pour les infractions d'atteintes aux systèmes de traitement automatisé de données (STAD) et pour le traitement judiciaire des « rançongiciels » est instituée. Cette organisation permet une meilleure efficacité dans la lutte et la répression de ces infractions dans la mesure, notamment, où la dimension fréquemment transnationale des faits appelle une coopération internationale et le soutien d'Europol, Eurojust et Interpol.

La France estime que les efforts de la communauté internationale doivent être consacrés à la mise en œuvre des instruments existants et que la négociation d'un nouvel instrument n'est pas nécessaire. La Convention des Nations unies contre la criminalité organisée de 2000 est à même de répondre au défi de la cybercriminalité, qui est une forme de criminalité organisée. Parmi les instruments existants qui traitent spécifiquement de criminalité organisée, la Convention de Budapest de 2001 est le seul instrument international.

LA CONVENTION DE BUDAPEST (2001)
La Convention de Budapest a été ratifiée par 56 États, dont les États-Unis et huit autres États non membres du Conseil de l'Europe. Si l'on prend en compte le nombre de signataires, les États tiers qui ont été invités à adhérer et ceux qui s'inspirent de ses principes pour

élaborer leur législation nationale, la Convention rassemble une centaine d'États, ce qui en fait un instrument de référence dans la lutte contre les usages criminels du cyberespace. Cet instrument a un double objet : l'instauration d'une législation contre la cybercriminalité et la mise en place d'un cadre de coopération judiciaire et policière. Il permet ainsi une harmonisation des législations nationales à partir de définitions communes des infractions, l'adaptation des moyens procéduraux aux contraintes particulières d'Internet et la mise en place de points de contact permanents, qui sont trois éléments déterminants pour assurer l'efficacité de la lutte contre la cybercriminalité. La convention dispose de deux autres atouts : un Bureau d'assistance technique du Conseil de l'Europe sur la cybercriminalité chargé d'aider les États à renforcer leurs capacités ainsi qu'un Comité de suivi de la Convention permettant non seulement d'évaluer son application, mais aussi d'actualiser sa mise en œuvre grâce à l'adoption de notes d'orientation qui rendent la Convention vivante et évolutive. La France œuvre pour que le plus grand nombre d'États s'engagent dans la lutte contre la cybercriminalité selon les principes et les procédures établies par la convention de Budapest.

Comme le rappelle la Stratégie nationale pour la sécurité du numérique, la promotion et l'universalisation de la Convention de Budapest, mais aussi le développement des capacités juridiques et opérationnelles des pays qui ne sont pas encore dotés de structures de lutte contre la cybercriminalité, sont des objectifs prioritaires de la France dans ce domaine. Au sein de l'Union européenne, la France promeut la mise en place d'un dispositif de coopération judiciaire simplifié entre États membres. Ces coopérations techniques et structurelles constituent ainsi des compléments essentiels pour le renforcement de la coopération opérationnelle entre acteurs de l'investigation. Elles se conjuguent avec le partage des bonnes pratiques, en vue d'un rapprochement des standards et d'une efficacité opérationnelle accrue.

Au sein de l'Union européenne, la lutte contre les comportements illégaux dans l'espace numérique doit être renforcée afin de garantir la sécurité sur Internet. Cette approche doit se traduire par un effort des États membres en faveur de la mise en place de dispositifs de coopération simplifiée, au niveau judiciaire et policier, entre États membres.

En complément de ces coopérations institutionnelles, une politique active de partenariat avec le secteur privé doit être menée au niveau national européen et international. Elle doit faciliter la prévention, l'échange d'informations, la lutte contre les contenus illégaux ou contre l'utilisation par les criminels de moyens techniques leur permettant de se soustraire aux poursuites. La complète réussite de ce partenariat reste conditionnée à une détermination au niveau international des obligations juridiques des entreprises étrangères confrontées à la diversité des législations nationales. Une structuration rapide de ce dialogue tant au niveau européen qu'international doit accroître les capacités de lutte contre la cybercriminalité.

Enfin, la France pourrait favoriser les partenariats et transferts de technologies à ses partenaires qui chercheraient à renforcer leurs capacités défensives pour répondre aux menaces cyber. Elle l'a notamment déjà fait avec le projet d'implantation à Dakar d'une École nationale à vocation régionale (ENVR) annoncé le 13 et 14 novembre par le ministre de l'Europe et des Affaires étrangères. Cette école, qui devrait être installée fin 2018, aura pour vocation de permettre au Sénégal et aux partenaires régionaux de renforcer leurs capacités en cybersécurité, notamment dans le cadre de la lutte contre la cybercriminalité et en contre-terrorisme.

Combattre à l'échelle internationale l'usage du numérique à des fins terroristes

Ainsi, les récents attentats terroristes commis sur le territoire des États membres, comme les enquêtes sur les projets d'attentats déjoués, ont mis en évidence le rôle décisif des services de communications par voie électronique dans la préparation et la réalisation de ces actes. Des appels à la haine et à la violence, comme des échanges faisant l'apologie du terrorisme ou portant sur l'élaboration de projets d'attentats terroristes, sont diffusés par le biais d'applications utilisées très couramment par le grand public.

Pour y répondre, la France, en concertation avec ses partenaires, allemands d'un côté,

britanniques de l'autre, a défini les principaux objectifs suivants :

- améliorer le retrait des contenus illicites de l'Internet non seulement en encourageant les entreprises à supprimer le plus rapidement possible les contenus signalés ;
- renforcer les modalités de coopération avec les prestataires de services de communication par voie électronique, en particulier lorsqu'ils sont établis hors du territoire de l'Union : mise en place de points de contact entre les services répressifs et les prestataires de services ; renforcement de l'obligation de coopération dans le cadre des enquêtes pénales ; recherche d'une plus grande célérité et d'une plus grande réactivité dans le traitement des réquisitions des autorités judiciaires ; garantie d'accès aux données à des fins d'investigation, en préservant notamment la conservation et l'accès aux données de trafic et de localisation et en permettant l'accès au contenu chiffré sans pour autant interdire le chiffrement ou autoriser les backdoors ; accélération de l'accès aux données et aux contenus de communications au-delà des frontières, quel que soit l'endroit où elles sont stockées.
- soutenir les efforts des organisations de la société civile pour promouvoir des contre-discours pertinents en mesure de neutraliser les contenus terroristes sur l'Internet francophone et anglophone.

Promouvoir auprès des citoyens une culture du chiffrement

Aujourd'hui, le MEAE constate la nécessité de poursuivre les efforts en matière de sécurité des systèmes d'information. Le MEAE s'engagera notamment pour la généralisation de la culture du chiffrement en Europe allant dans le sens d'un renforcement des protections de l'ensemble des utilisateurs.

2. PROMOUVOIR UN INTERNET EUROPÉEN FONDÉ SUR L'ÉQUILIBRE ENTRE LIBERTÉS PUBLIQUES, CROISSANCE ET SÉCURITÉ DANS LE MONDE NUMÉRIQUE

Le numérique bouleverse l'ensemble de la société et tous les secteurs de l'économie en modifiant les processus de conception, de production et de distribution des biens et services. Il appartient à l'Union européenne d'en faire une opportunité pour rénover son modèle de développement et de croissance, sans se contenter d'être seulement une zone de consommation de services numériques développés ailleurs dans le monde. La taille de son marché intérieur confère à l'Union européenne un rôle politique qui doit lui permettre de s'affirmer face aux autres acteurs mondiaux et de constituer un pôle normatif structurant au sein du monde numérique. La fragmentation des habitudes de consommation sur des marchés nationaux divers – et le coût de pénétration de ces marchés pour des entreprises – nécessitent de développer l'intégration du marché unique numérique, afin de pallier ces surcoûts d'entrée.

En conséquence, l'Union européenne doit avoir pour ambition de faire émerger un Internet européen ouvert et interconnecté au réseau mondial, mais qui repose sur un équilibre propre entre libertés, croissance et sécurité dans le monde numérique, tout en veillant à ne pas freiner l'émergence d'offres innovantes. Cet Internet européen devra refléter le plus haut niveau d'exigence en matière de protection des droits fondamentaux et des données personnelles, en cohérence avec la tradition juridique et politique européenne. Il nécessite le développement d'une base économique et industrielle forte au sein du marché unique du numérique. Il permettra la promotion d'un environnement numérique de confiance et la recherche d'une autonomie stratégique, y compris par une meilleure maîtrise des infrastructures et technologies clés. Il favorisera des nouvelles formes d'organisation ainsi que des nouvelles pratiques politiques et économiques (innovation ouverte, économie collaborative). Le développement d'un Internet européen nécessite :

- la consolidation d'un modèle européen de société numérique, qui allie dans un environnement de confiance la liberté d'entreprendre et d'innover avec la protection des droits fondamentaux. L'émergence de ce modèle sera rendue possible par la production européenne de services numériques, par la définition de standards techniques, par le soutien à l'innovation des entreprises, et par la promotion de règles du jeu plus équitables entre l'ensemble des acteurs de cette société numérique, opérateurs économiques, grandes plateformes, start-up et créateurs ;
- la promotion de ce modèle à l'échelle internationale par la garantie de l'application de ses principes juridiques dans les négociations internationales, une participation active à la gouvernance d'Internet et la promotion internationale d'un Internet ouvert et de confiance.

2.1. Garantir l'effectivité de la protection des droits

En matière de droits, la place croissante du numérique a une incidence particulièrement forte sur la protection des données personnelles, la liberté d'expression et la propriété intellectuelle, domaines dans lesquels l'Europe a construit de longue date un cadre juridique propre. Chacun de ces domaines nécessite une adaptation aux nouveaux enjeux numériques sans remettre en cause la nature et les finalités de leur réglementation.

Dans la nouvelle société numérique, le droit à l'autodétermination informationnelle doit devenir un principe cardinal pour la protection des données. Il s'agit d'établir le droit de l'individu de décider de la communication et de l'utilisation de ses données à caractère personnel. Ce principe doit guider la définition des instruments concrets susceptibles de garantir l'effectivité des droits consacrés par l'Union européenne. L'objectif est de renforcer un cadre juridique protecteur, doté des instruments efficaces qui garantissent son effectivité, et qui contribue au développement d'une économie de la donnée.

La France poursuivra ainsi les objectifs suivants :

Assurer à chacun la maîtrise de l'utilisation de ses données personnelles y compris au-delà des frontières

L'Union européenne se distingue par un cadre juridique fondé sur des principes relatifs à la qualité des données : obligation de loyauté, finalités de collecte déterminées, explicites et légitimes, proportionnalité des données collectées aux finalités de collecte, exactitude des données et limitation de la durée de conservation. La protection des données personnelles est une des libertés consacrées par la Charte des droits fondamentaux de l'Union européenne (art. 8).

La confiance des utilisateurs, dont la protection des données personnelles est l'une des composantes essentielles avec la sécurité du réseau, peut être le fondement d'une économie de la donnée.

Le développement d'une industrie et de services numériques européens, conçus pour permettre un haut niveau de maîtrise des données personnelles (privacy by design) et de sécurité des systèmes (security by design) en cohérence profonde avec le cadre juridique européen doit être encouragé.

Le développement d'un droit à la portabilité pour l'ensemble des données qui concernent un utilisateur permet à ce dernier de bénéficier d'une mobilité numérique accrue et de conserver la maîtrise sur ses données. Ce droit doit toutefois être concilié avec la nécessité de préserver les incitations à innover pour les entreprises en matière de collecte et d'exploitation de données.

L'Union européenne doit conduire une politique active de promotion de ses standards élevés de protection des données à caractère personnel. La France s'engage à poursuivre les négociations en cours conduites par le MEAE et le ministère de l'Économie et des Finances en matière de droit à la portabilité dans les différentes instances internationales.

Par ailleurs, les transferts internationaux en dehors de l'Union européenne de données à caractère personnel sont par principe interdits sauf dérogations (notamment lorsque le pays de destination assure un niveau de protection suffisant). La protection des données personnelles doit être exclue du champ des négociations commerciales internationales afin de préserver l'application des règles européennes ainsi que le droit à réguler des États en la matière. En outre, il convient de rappeler que l'utilisation et l'accès à certaines données jugées stratégiques doivent être encadrés.

Au sein de l'Union européenne, le G29, qui rassemble les autorités nationales indépendantes de protection des données, la Commission européenne et les autorités mises en place par les institutions et organes de l'Union européenne dans ce domaine œuvrent pour consolider une approche européenne commune sur ces enjeux précis.

> **LA MISE EN ŒUVRE DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES**
> **Le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ou règlement général sur la protection des données) entrera en vigueur le 25 mai 2018. Il poursuit trois objectifs : i) faire de la norme européenne la référence mondiale en matière de protection des données ii) assurer un cadre juridique harmonisé et clair pour répondre aux nouveaux enjeux économiques et de compétitivité (harmoniser le cadre juridique de l'Union pour éviter le forum shopping, assurer aux entreprises un interlocuteur unique, assurer la sécurité juridique des responsables de traitement), iii) mettre en place un cadre juridique protecteur et effectif pour les personnes (responsabiliser les entreprises, assurer un niveau de protection optimal pour les personnes, renforcer l'efficacité de la législation européenne). Pour mettre en œuvre ce règlement, le G29 se prépare à devenir le Comité européen de la protection des données (CEPD) qui assurera en 2018 la coordination entre les autorités nationales. Ses travaux portent aussi sur la mise en place du système de guichet unique pour les entreprises. Il entend enfin diffuser, avant la fin 2016, des lignes directrices sur quatre**

thèmes prioritaires : le droit à la portabilité des données, la certification des traitements de données, les fonctions du délégué à la protection des données dans les entreprises de traitement des données et les traitements à risque. La France joue un rôle de premier plan au sein du G29 : elle en assure la présidence jusqu'en 2018.

Promouvoir notre modèle juridique en matière de maîtrise par les individus de leurs données personnelles

La France dispose, de longue date, d'un cadre juridique assurant la maîtrise par les individus de leurs données personnelles. Reposant sur la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ce cadre juridique est mis en œuvre, sous le contrôle du juge, par la Commission nationale informatique et libertés (CNIL), dont l'expertise et les recommandations sont reconnues internationalement. Forte de cette expérience, la France a joué un rôle clef dans la définition d'un cadre juridique européen de protection des données personnelles.

Conformément à cet engagement, il est important de continuer à réfléchir au développement, notamment au niveau européen, d'un droit à l'autodétermination informationnelle. De ce principe découlent de nombreux droits que la France a souhaité renforcer, *qu'il s'agisse de la possibilité de choisir la localisation de ses données en Europe, du droit à décider et contrôler les usages de ses données personnelles, du droit à la portabilité de ses données ou du droit à l'oubli. Sous cette impulsion, plusieurs de ces droits ont été récemment adoptés au niveau européen dans un texte unique qui prévoit que les autorités de protection des données assurent la cohérence de l'ensemble dans le cadre d'une activité plus intégrée (et rend notamment possible des décisions conjointes sur des cas transfrontaliers). Le recours à la CNIL, compte tenu de son expérience sur le sujet, que ce soit en matière d'accompagnement des entreprises, de valorisation de leurs bonnes pratiques et de détermination de standards respectueux des droits des personnes, a vocation à créer un cadre de régulation qui combine innovation et protection des données personnelles, la seconde étant un élément clé de compétitivité à l'ère numérique.

Veiller à transparence et à la loyauté des plateformes numériques

Les grandes plateformes numériques constituent, par les services d'intermédiation entre utilisateur et offreur qu'elles fournissent, des lieux de passage obligé. Elles concentrent une part croissante des flux de données et disposent de ce fait d'une capacité de prescription sans équivalent. La réflexion engagée au niveau européen, conformément aux conclusions du Conseil européen de juin 2015, sur le cadre réglementaire applicable aux plateformes doit être poursuivie et complétée afin de garantir le respect des principes fondamentaux suivants :

- l'égale application des règles entre les plateformes et les autres opérateurs économiques ;
- la loyauté des plateformes en ce qui concerne les mécanismes de classement et d'indexation des services proposés et des informations délivrées aux personnes qui les consultent ;
- un accès libre et facile pour les utilisateurs, dans le respect des règles de la propriété intellectuelle, aux services et contenus de leur choix ;
- la portabilité des services, contenus et données des utilisateurs des plateformes, notamment par l'interopérabilité des formats de fichiers, tout en s'assurant de la préservation des incitations à innover en matière de collecte et d'exploitation de données ;
- en matière de services audiovisuels numériques, le pluralisme des médias, la promotion de la diversité culturelle, la lutte contre le discours de haine ou l'apologie d'actes de terrorisme et la protection des mineurs au regard des contenus accessibles.

Conformément à ces orientations, la France défend la mise en place d'un observatoire européen pour la transparence des plateformes.

LA LOI POUR UNE RÉPUBLIQUE NUMÉRIQUE DU 7 OCTOBRE 2016
La loi pour une République numérique du 7 octobre 2016 est le volet législatif de la stratégie numérique du gouvernement français présentée le 18 juin 2015. L'objectif de cette loi est de favoriser une politique d'ouverture et de circulation des données publiques, de renforcer les droits des individus dans leurs usages des nouvelles technologies de l'information, et de permettre l'accessibilité du numérique par tous les publics sur l'ensemble du territoire. La transparence et la concurrence des plateformes sont l'un des grands axes de cette loi. D'abord à travers la portabilité et la récupération des données, obligation est faite aux fournisseurs de service de communication au public en ligne de proposer aux utilisateurs une fonctionnalité de récupération des données associées à leurs comptes. Ensuite via la loyauté des plateformes et de l'information à destination des consommateurs notamment s'agissant des avis en ligne, des modalités de référencement, de classement et de déréférencement ainsi que des conditions générales d'utilisation.

Protéger les droits de la propriété intellectuelle sur Internet

L'ère numérique bouleverse les modèles économiques : les plateformes sont les nouveaux créateurs de valeur et les modes de diffusion des contenus se multiplient et se diversifient. Le cadre d'application du droit d'auteur et de la propriété intellectuelle se voit également transformé.

Un nouvel équilibre doit être trouvé, afin d'encourager les usages numériques, mais aussi de stimuler la création culturelle, qui repose sur la juste rémunération des créateurs. Le cadre applicable aux plateformes doit être clarifié, afin de garantir la stabilité et la sécurité juridique nécessaires à leur développement. Le développement des services à caractère culturel du numérique ne peut être durable que s'il installe entre les plateformes et les producteurs de contenus un partage équitable de la valeur, ces équilibres étant importants pour la diversité culturelle en ligne et la protection de la propriété intellectuelle.

Il est important de renforcer la lutte contre la contrefaçon et le piratage des contenus protégés par le droit de la propriété intellectuelle en impliquant l'ensemble des acteurs de l'écosystème numérique.

Au niveau européen, le paquet « droit d'auteur », présenté le 14 septembre 2016, vise à adapter le droit d'auteur au numérique. Une première réponse à la problématique du partage de la valeur est apportée par la création de droits voisins pour les éditeurs de presse en ligne et par une obligation pour les plateformes de prendre les mesures appropriées pour éviter la diffusion de contenus illégaux, notamment par l'utilisation de logiciels de reconnaissance de contenus violant le droit d'auteur. La diffusion transfrontière de contenus en ligne est également facilitée, ce qui ne devra pas conduire à un affaiblissement du principe de la territorialité des droits (négociation des droits pays par pays pour chaque programme) en permettant aux distributeurs, dès lors qu'ils ont acquis les droits dans un État membre, de distribuer les œuvres dans les autres États membres.

La France veillera donc à ce que cette réforme ne conduise pas à un affaiblissement du droit d'auteur et permette d'assurer la rémunération des créateurs et de sauvegarder la diversité culturelle.

2.2. Renforcer l'écosystème numérique européen

L'existence d'une base industrielle et technologique forte, reposant sur un marché numérique unique, est une condition nécessaire à l'émergence d'un écosystème numérique européen. À l'inverse, il existe un risque réel de dépendance européenne en matière numérique si une action déterminée, à l'échelon européen, n'est pas entreprise. La coopération franco-allemande constitue, dans ce domaine particulièrement, un instrument privilégié de la dynamique à instaurer dans l'Union européenne. L'émergence de l'Internet des objets, tant dans son volet industriel que grand public, est une chance pour l'Europe, qui a manqué la première révolution numérique au tournant des années 2000. La maîtrise des technologies à venir est indispensable à notre autonomie stratégique, comme à notre

capacité à prévenir les risques potentiels qu'elles recèlent. Une politique industrielle du numérique est un axe fort tant pour la croissance et l'emploi que pour le positionnement de l'Europe sur la scène internationale et face aux grands groupes non européens de l'économie numérique.

À l'heure actuelle, ce sont essentiellement des acteurs non européens qui détiennent les positions centrales dans le monde numérique européen. Chacun dans leur secteur, ces acteurs ont bénéficié d'un accès ouvert aux infrastructures et aux marchés européens. Plus agiles, plus ouverts au risque, ils ont également su optimiser leur charge fiscale. Dotés de moyens financiers importants qui leur permettent d'acquérir des technologies potentiellement disruptives ou de lancer eux-mêmes des services innovants, ces acteurs sont difficiles à contourner sur les principaux marchés.

La domination des acteurs non européens dans les technologies numériques innovantes présente le risque d'un déplacement de la valeur de certains secteurs, y compris non numériques, hors de l'Union européenne. En étant présents tout au long de la chaîne de valeur, ces acteurs non européens peuvent également être en mesure de capter une partie importante de la valeur en devenant à la fois « producteurs » et « distributeurs » de contenus et de services. Cela soulève ainsi la problématique de la diversité culturelle et de la capacité de l'Europe à assurer le dynamisme de ses industries de contenus, culturels et éducatifs, qui contribuent à la croissance, à la création d'emploi et au rayonnement de l'Europe. Au cœur des enjeux du numérique, les industries culturelles et créatives européennes, dont le dynamisme et la richesse sont garants de la diversité culturelle, doivent être soutenus et les acteurs européens du secteur encouragés.

La concentration sur les marchés où les acteurs sont des plateformes numériques est souvent naturelle en raison d'effets de réseau qui la rendent bénéfique pour les utilisateurs. Elle peut être renforcée par la présence d'autres économies d'échelle (apprentissage statistique grâce aux clients, par exemple). L'analyse concurrentielle de ces plateformes est complexe, mais le droit européen de la concurrence est théoriquement en mesure d'en sanctionner les pratiques anticoncurrentielles, et notamment les abus de position dominante qui empêchent la croissance de nouveaux acteurs, et les aides d'État qui biaisent la concurrence, sous réserve qu'il soit appliqué suffisamment rapidement. Les pratiques de contournement fiscal de certaines multinationales du numérique doivent être combattues via une réforme des règles fiscales internationales et par l'application du droit européen (notamment en matière d'aides d'État). Par ailleurs, afin de faire émerger une offre de technologies numériques européenne, il est nécessaire de renforcer la formation de la population active dans les domaines scientifiques (dits STEM pour Science, Technology, Engineering and Mathematics), et en particulier en informatique.

De plus, l'innovation des entreprises européennes peut être d'une part stimulée par la poursuite des aides à la recherche et développement (R&D) privée, et d'autre part nécessite d'avoir une R&D publique de premier plan et efficace.

Au-delà, l'innovation des entreprises bénéficie de l'amélioration de l'environnement des affaires européennes, favorisée par la lisibilité fiscale et par la simplification administrative.

Enfin, pour tirer tous les bénéfices du numérique et en favoriser le développement, l'Europe doit se doter d'infrastructures de télécommunications de pointe à la fois en matière de réseaux fixes à très haut débit et de réseaux mobiles (4G, 5G) qui couvrent les zones denses mais également les zones moins denses.

La France poursuivra dans ce domaine les objectifs suivants :

Promouvoir un environnement favorable à l'économie numérique européenne

L'unification du marché intérieur numérique est un premier objectif. Mais l'Europe doit aussi prendre toute sa place dans les technologies stratégiques d'aujourd'hui et de demain (comme l'industrie 4.0, l'intelligence artificielle et les technologies issues des *blockchains*).

La transformation numérique de l'économie européenne nécessite d'abord le renforcement des capacités de financement des entreprises innovantes. L'absence de fonds de

capital-risque de très grande taille est un facteur limitant pour l'émergence de grandes entreprises numériques européennes alors que le modèle numérique est fondé avant tout sur les rendements croissants et la génération d'externalités comme des effets du réseau. L'émergence de fonds de capital-risque de taille critique doit être une priorité dans la stratégie économique de l'Europe, notamment pour accompagner la phase de croissance. Le modèle de l'hypercroissance, qui repose sur l'acquisition de parts de marchés au détriment de la rentabilité immédiate, ne peut se mettre en place qu'en présence d'une forte industrie du capital-risque pour le soutenir.

Les autorités françaises s'engagent à soutenir l'action des start-up internationales, notamment par le développement d'initiatives de diplomatie économique (par exemple, la *French Tech*).

> **Dans ce domaine, la Commission se montre active et conduit une série de travaux visant à stimuler l'investissement par les marchés financiers dans les entreprises en expansion et innovantes : plan d'action pour l'Union des marchés de capitaux d'une part, mais aussi plan d'investissement pour l'Europe avec notamment le Fonds européen pour les investissements stratégiques (FEIS et FEIS 2.0). Dans ce cadre, pour catalyser les investissements privés dans les marchés du capital-risque en Europe, la mise en place d'un fonds paneuropéen investissant dans le capital-risque européen est également étudiée par la Commission. Capitaux du secteur privé et soutien de l'Union européenne seront combinés pour attirer les grands investisseurs institutionnels vers le capital-risque européen et démultiplier l'effet du soutien apporté par l'Union européenne au secteur européen du capital-risque au bénéfice des entreprises les plus prometteuses.**

Afin de réaliser le marché unique numérique, il est nécessaire de garantir l'interopérabilité des produits et services de technologies de l'information et de la communication (TIC) qui doivent pouvoir être utilisés partout en Europe, évitant ainsi la fragmentation des marchés : la définition d'une approche stratégique pour la normalisation et la certification de sécurité des TIC, dans des domaines prioritaires, est donc primordiale. Il est également nécessaire de réaffirmer, à l'échelle internationale, le rôle central de la normalisation pour l'interopérabilité face à des logiques propriétaires ou basée sur le pouvoir de marché, de renforcer le système européen de normalisation et de certification de sécurité pour permettre à l'Union européenne d'être un acteur influent au niveau mondial et d'assurer la promotion des standards européens avec l'objectif que l'Europe conserve la maîtrise des conditions techniques d'accès à son marché et ne voie pas sa capacité de régulation remise en cause par les standards.

L'intensification des efforts en matière de formation, en particulier dans les domaines scientifiques, ainsi qu'en faveur de la R&D, sont aussi indispensables au développement d'un écosystème d'innovation européen.

Garantir des règles du jeu équitables en matière de concurrence et de fiscalité

L'application du droit de la concurrence aux activités numériques doit être systématique afin que des positions dominantes n'entravent pas la dynamique d'innovation inhérente à la numérisation de l'économie. Les plateformes numériques, si elles ont des effets positifs sur la concurrence, sont aussi susceptibles d'abuser de leur position dominante, d'exercer leur considérable pouvoir de marché au préjudice de l'innovation et du développement numérique (notamment des SME), ainsi que de verrouiller l'accès à certains marchés. L'analyse concurrentielle de ces plateformes est complexe, et si le droit européen de la concurrence fournit un premier cadre de contrôle, il semble nécessaire que de nouveaux outils soient développés pour appréhender de façon appropriée et en temps voulu les dysfonctionnements et asymétries de marchés constatés sur les transactions des plateformes numériques.

La transparence sur la nature des données collectées permet de fournir aux consommateurs un critère de comparaison des offres. De même, la portabilité des données pourra limiter les risques de verrouillage de l'offre. La pleine prise en compte, par les autorités de régulation, de la vitesse des changements technologiques peut nécessiter d'accélérer l'action des autorités nationales et européennes de la concurrence dans ces secteurs, et

peut notamment nécessiter un recours accru à des mesures conservatoires ou d'urgence. La nature même des activités numériques pose des difficultés nouvelles en matière d'applicabilité des normes et des régulations. Pour renforcer la sécurité juridique des acteurs économiques et la confiance des utilisateurs, la règle du pays de destination doit constituer la règle de droit commun pour appréhender au mieux l'activité des acteurs numériques. En matière de fiscalité indirecte, le principe de taxation de la TVA au lieu de consommation doit être généralisé, au-delà des seuls services électroniques, en y incluant les ventes de biens à distance. Par ailleurs, le développement des entreprises numériques rend nécessaire la réaffirmation des principes d'équité fiscale. Au-delà de ces pratiques d'optimisation fiscale dans les limites du droit, il importe pour favoriser la contestabilité des marchés d'assurer une application rapide du droit européen en matière d'aides d'État, notamment pour assurer l'égalité des sociétés devant l'impôt. La France a proposé une feuille de route européenne sur la fiscalité du numérique, et le Conseil européen du 19 octobre 2017 a souligné la nécessité d'un système fiscal « efficace et équitable, qui soit adapté à l'ère numérique ». Ceci est essentiel pour s'assurer que les entreprises paient toutes leur juste part d'impôts, et qu'elles aient des conditions de concurrence égales.

La France est également moteur dans cette réflexion sur la fiscalité du numérique, et a présenté, lors du Conseil ECOFIN informel des 15-16 septembre, une feuille de route pour la fiscalité du numérique, comprenant un projet de taxe d'égalisation sur la valeur créée par les géants du numérique. Si ce projet de taxe permettra de combler les lacunes du cadre fiscal à court terme, la France soutient également les travaux sur l'intégration de la dimension numérique dans l'assiette commune consolidée d'impôt sur le revenu (ACCIS) et sur la définition d'un « établissement stable virtuel », en cours à l'OCDE.

CE QUE L'UNION EUROPÉENNE ET LA FRANCE DEMANDENT POUR LA FISCALITÉ DES ENTREPRISES NUMÉRIQUES

En matière de fiscalité indirecte, le plan d'action européen pour la TVA vise à adapter le système de TVA à l'économie numérique. La France promeut en particulier la mise en œuvre du principe de neutralité technologique, pour que les taux de TVA sur le livre numérique et la presse en ligne soient alignés sur les taux réduits applicables aux publications papier. Le guichet unique TVA, qui permet à une entreprise de déclarer et payer la TVA due dans toute l'Union européenne dans le seul État membre d'origine, devrait être étendu à la vente de biens en ligne.

En matière de fiscalité directe, la Commission est actuellement particulièrement active dans le domaine fiscal, la réflexion sur la fiscalité du numérique a été relancée. Les débats portent sur trois options.

Premièrement, pour imposer les entreprises qui localisent dans des États tiers leurs bénéfices imposables réalisés sur le marché intérieur, l'UE pourrait appliquer une taxe d'égalisation numérique sur le chiffre d'affaires. L'objectif de cette taxe serait de combler l'écart entre l'impôt payé par les entreprises actuellement et celui qui aurait dû être payés, si les activités numériques avaient été prises en compte dans le calcul du chiffre d'affaires.

D'autre part, dans le cadre du projet d'ACCIS (assiette commune consolidée d'impôt sur le revenu), l'Union pourrait mettre en place des règles pour localiser et répartir entre les États membres les bénéfices liés au numérique réalisés par les entreprises.

Enfin, le droit de l'Union européenne pourrait intégrer les conclusions des travaux de l'OCDE, notamment sur la « présence fiscale numérique ». Le rapport d'étape de la task force de l'OCDE sur le sujet au printemps 2018 sera une indication pour l'Union de l'avancement de ces travaux.

Par ailleurs, depuis les scandales Lux Leaks et Panama Papers, l'Union européenne renforce ses dispositifs de lutte contre la fraude fiscale et les pratiques d'optimisation fiscale agressive qui représenteraient, selon les hypothèses prudentes de l'OCDE, entre 88 et 212 milliards d'euros par an à l'échelle mondiale. Les travaux menés au niveau international (G20 et OCDE) ainsi que la question du juste montant d'impôts dont les grandes multinationales du numérique (Google, Amazone, Apple, Facebook) doivent s'acquitter constituent d'autres facteurs incitant les institutions et les États membres à faire progresser la convergence fiscale en Europe.

L'application du principe nexus, conditionnant les régimes fiscaux préférentiels accordés aux revenus de la propriété intellectuelle, à la réalisation sur le même territoire de l'activité de recherche et développement qui a généré ces droits peut être encouragée.
Outre la défense active de la taxe d'égalisation sur la valeur créée par les géants numériques, la France copréside, au sein de l'OCDE, un groupe de réflexion sur l'économie numérique. Créée en septembre 2013 à l'initiative du G20 (projet BEPS), cette task force a été reconduite récemment (communiqué de finances de Baden-Baden). La France y défend activement des adaptations de la fiscalité internationale. Elle soutient en particulier que la collecte massive et systématique de données personnelles sur le territoire d'un État par une entreprise non résidente devrait permettre à celui-ci de caractériser une « présence fiscale numérique » et d'imposer les bénéfices correspondants. La task force doit remettre un nouveau rapport d'étape au printemps prochain.
Enfin, il convient de noter que la France a obtenu que la Commission soumette une proposition au Conseil européen d'ici début 2018. L'objectif de la France est désormais d'obtenir une approche politique commune des États membres sur cette question au Conseil ECOFIN d'ici la fin de l'année, qui pourra servir de base à la proposition législative de la Commission et à la position de l'Union européenne dans les discussions à l'OCDE. En parallèle, les travaux techniques sur les différentes options envisageables doivent être menés, et seront un enjeu déterminant pour convaincre les États membres les plus réticents.

Défendre le modèle du numérique européen dans les négociations internationales

L'Union européenne ne peut pas être absente des débats internationaux en matière de numérique. Le modèle qu'elle représente déjà, les normes et technologies que ses entreprises développent, les actions que ses États membres entreprennent dans ce domaine doivent trouver une traduction internationale. L'Union européenne doit prendre part à la définition de la gouvernance d'Internet actuelle et future, à la promotion d'un monde numérique conforme à ses principes et à ses valeurs, à la régulation des intérêts privés dans les cadres multilatéraux en défendant la vision qui lui est propre dans les enceintes internationales pertinentes.

Dans les négociations internationales, l'Union européenne doit veiller au respect des principes et des valeurs qu'elle entend promouvoir et qu'elle met en œuvre en droit interne. Eu égard au caractère transnational des activités numériques, les accords commerciaux négociés par l'UE fournissent un cadre opportun pour traiter les défis transfrontaliers, notamment les barrières à l'accès au marché, dans le domaine du numérique. Ces accords commerciaux doivent être en cohérence avec les principes établis dans le cadre du marché unique numérique. En particulier sur le principe de libre circulation des données, la Commission européenne doit mesurer l'ambition de ses propositions à l'aune des intérêts offensifs de chaque négociation, tout en maintenant une ambition forte quant à la préservation et à la diffusion du modèle européen de protection des données personnelles. Les accords commerciaux doivent donc respecter les principes suivants :

- conditions de concurrence équitable et non discriminatoire entre acteurs européens et non européens ;
- promotion des standards européens notamment en matière de protection des consommateurs en ligne ;
- maintenir la capacité de l'Union européenne et ses États membres de mener à bien leurs politiques publiques ;
- promotion du principe de *free flow of information*, principe universellement reconnu qui protège l'accès universel à la connaissance ;
- exclusion des services audiovisuels et de leurs contenus numériques ;
- la préservation d'un accès aux codes sources dans le cadre des évaluations de sécurité des produits et services numériques.

DÉFENDRE ET PROMOUVOIR LE MODÈLE EUROPÉEN DU NUMÉRIQUE DANS LES NÉGOCIATIONS INTERNATIONALES
La France a amorcé depuis quelques années un véritable effort pour promouvoir et soutenir un modèle français, européen, qui valorise les libertés fondamentales et les droits des

utilisateurs. Cet effort s'est accompagné d'une augmentation manifeste des ressources mobilisées. Ainsi, un poste d'ambassadeur pour le numérique existe depuis octobre 2015 pour promouvoir cette vision dans les négociations internationales et établir avec les grands groupes numériques et autres acteurs économiques pertinents les relations nécessaires à la promotion de la conception européenne du numérique.
L'ambassadeur est également au cœur de la task force interne qui rassemble l'ensemble des acteurs du MEAE travaillant sur ces enjeux, et qui permet de prendre en compte de manière plus complète – notamment en développant une approche coordonnée et stratégique – les enjeux économiques, sociétaux, culturels et de développement liés au numérique.
Enfin, suite aux orientations prises au G7 de Taormina en juin 2017, il a également été mandaté par le ministre d'État, ministre de l'intérieur, le ministre de l'Europe et des Affaires étrangères et le secrétaire d'État auprès du Premier ministre chargé du Numérique, une mission au titre de la lutte contre l'utilisation d'internet à des fins terroristes, de conduire un dialogue direct avec les grandes plateformes numériques américaines. Il travaillera en étroite collaboration avec les services du ministère de l'intérieur et avec le secrétariat d'État auprès du Premier ministre chargé du Numérique.
Les différentes directions des ministères économiques et financiers ont également renforcé leur mobilisation et leur coordination, pour répondre à l'importance accrue des enjeux numériques dans les négociations économiques, financières et fiscales tant au plan européen qu'au niveau international (G7 et G20 notamment), qui nécessitent de combiner expertises économique, industrielle et fiscale en particulier.

2.3. Renforcer la sécurité et l'autonomie stratégique européennes dans le monde numérique

La confiance des utilisateurs nécessite un haut niveau de sécurité. L'interconnexion des réseaux rend indispensable une action au niveau européen afin d'améliorer la sécurité globale des institutions, des États membres et des utilisateurs européens. L'existence d'acteurs industriels autonomes en matière de cybersécurité et la maîtrise des infrastructures essentielles du réseau sont nécessaires pour la sécurité des réseaux européens.

La France poursuivra ainsi les objectifs suivants :

Maîtriser les infrastructures numériques essentielles sur le territoire européen

Le caractère déterminant des activités numériques dans les sociétés européennes rend nécessaire une maîtrise des infrastructures essentielles. La dépendance actuelle sur ce plan constituerait une grande vulnérabilité pour l'ensemble des États membres et des institutions.

Une réflexion doit être engagée sur les infrastructures essentielles au fonctionnement des activités numériques afin d'identifier celles dont la maîtrise constitue la condition de la souveraineté nationale et l'autonomie européenne. Garder un droit à réguler suffisant (dans le cadre des négociations commerciales internationales notamment) est indispensable dans un contexte où la vitesse d'évolution du numérique engendre une incertitude constante sur le niveau même de régulation que nous devons pouvoir mettre en œuvre.

Maîtriser les prochaines technologies de rupture dans le domaine du numérique

Le concept d'autonomie stratégique de l'UE dans le cyberespace repose notamment sur une capacité de l'UE à se placer en pointe des prochaines révolutions technologiques dans le domaine du numérique. En effet, tout retard de l'Europe dans ce domaine ne fera qu'accroître de manière exponentielle sa dépendance actuelle. Stratégiques pour notre défense et notre sécurité, ces capacités le sont aussi pour la confiance qu'ont les citoyens européens dans l'écosystème numérique. Seule une synergie des compétences européennes – souvent excellentes en la matière – pourrait nous permettre de soutenir la compétition avec d'autres acteurs majeurs engagés dans la course, comme les États-Unis ou la Chine.

Dans le demi-siècle à venir, de nouvelles ruptures technologiques dans le domaine du

numérique auront très vraisemblablement des conséquences d'importance similaire, voire supérieure, à celles de la première révolution numérique que nous traversons aujourd'hui. Ainsi, les potentialités de l'intelligence artificielle, qui trouve aujourd'hui déjà certaines applications pratiques, sont majeures ; il en va de même dans le champ de la recherche en informatique quantique, encore balbutiante aujourd'hui. Ces domaines de recherche, qui auront des applications civiles et militaires, méritent d'être promus activement au niveau européen.

En conformité avec les annonces du président de la République à La Sorbonne en septembre 2017, la France promeut la mise en place d'une agence pour l'innovation de rupture au niveau européen.

Cet effort au niveau européen doit être soutenu par une coopération franco-allemande renforcée. C'est l'objectif des initiatives lancées lors du Conseil franco-allemand du 13 juillet dernier : échanges accrus sur les initiatives en calcul intensif et moyens futurs de calcul, projet de laboratoire franco-allemand sur le numérique ; mise au point d'une feuille de route industrielle commune (qui facilitera le transfert de connaissances de la recherche à l'industrie et désignera des mécanismes financiers) et d'une stratégie commune visant à mettre en commun et à accroître la recherche et la technologie en matière de technologie numérique à double usage au sens large (ce qui inclut l'intelligence artificielle, la robotique, l'informatique quantique).

Encourager le déploiement des infrastructures de télécommunications en Europe

La France poursuit son objectif de couverture intégrale du territoire en très haut débit. Dans le même temps, elle encourage le déploiement au sein de l'Union de réseaux de télécommunications de pointe afin de permettre aux utilisateurs de tirer tous les bénéfices du numérique et aux entreprises de proposer des services innovants à l'échelle du marché unique numérique européen.

Renforcer les capacités des Européens en matière de cybersécurité

Les standards de cybersécurité applicables aux « opérateurs de services essentiels » définis par les États membres dans le cadre de la mise en œuvre de la directive NIS (Network and Information Security) doivent constituer un niveau minimal pour l'ensemble des États membres. Le développement capacitaire au sein de l'UE constitue une priorité pour la France, qui y contribue par ses partenariats bilatéraux et son engagement actif au sein de l'ENISA, l'agence européenne pour la cybersécurité. Le renforcement des capacités propres aux institutions européennes (CERT-UE) constitue lui aussi une priorité.

La coopération en matière de de gestion de crises cyber à l'échelle européenne doit être développée. Les enceintes de coopération prévues par la directive NIS doivent parvenir rapidement à un haut niveau opérationnel (réseau des CSIRT des États membres pour le volet opérationnel, groupe de coordination des autorités de cybersécurité pour les aspects plus stratégiques), tout en préservant le caractère purement volontaire des échanges d'information.

> **LA DIRECTIVE NIS**
> **La directive sur la sécurité des réseaux et des systèmes d'information, connue sous l'appellation « directive NIS », a été adoptée le 6 juillet 2016. Elle fixe des obligations en matière de cybersécurité aux États membres (mise en place d'une stratégie nationale, identification d'opérateurs de services essentiels, imposition de règles s'appliquant à ces derniers, mise ne place d'une gouvernance nationale de la cybersécurité, etc.) et à certaines entreprises européennes (les fournisseurs de services numériques), tout en posant les bases d'une coopération accentuée et structurée dans le cadre de groupes dédiés (réseau des CSIRT et groupe de coopération) entre autorités nationales de cybersécurité. La directive conjugue haut niveau d'ambition (exemple : obligation pour les opérateurs de notifier les incidents ayant un impact sur la continuité de leurs services essentiels) et respect de la souveraineté des États membres.**

En France, l'ANSSI est chef de file ministériel pour assurer la transposition de la directive en droit français d'ici mai 2018. L'Agence européenne chargée de la sécurité des réseaux et des systèmes d'information (ENISA) avec laquelle l'ANSSI travaille étroitement, sera chargée d'aider les États dans la bonne mise en œuvre de la directive. Le mandat de l'Agence, qui expire en 2020, est en cours de révision pour lui permettre de mener à bien ses nouvelles fonctions.

Renforcer l'industrie et les services européens dans le secteur de la cybersécurité

Dans le but de favoriser le développement d'une industrie autonome, diversifiée et de confiance dans le domaine du numérique et de la cybersécurité, la France poursuivra son engagement fort au sein du nouveau partenariat contractuel public-privé pour la cybersécurité, qui vise à générer jusqu'à 1,8 milliard d'investissement à l'échelle européenne d'ici à 2020.

La France continuera à promouvoir l'accès de ses entreprises au fonds de R&D de l'UE dédié à la cybersécurité, notamment dans le cadre du prochain programme-cadre.

LE PARTENARIAT PUBLIC-PRIVÉ POUR LA CYBERSÉCURITÉ
L'Union européenne investira 450 millions d'euros dans ce partenariat, signé le 6 juillet 2016, dans le cadre de son programme pour la recherche et l'innovation Horizon 2020. Les acteurs du marché de la cybersécurité, représentés par l'organisation européenne pour la cybersécurité (ECSO), devraient investir trois fois plus. Ce partenariat regroupera également des membres d'administrations publiques nationales, régionales et locales, de centres de recherche et d'universités.
Moteur dans la mise en place de ce partenariat, la France est particulièrement impliquée dans sa gouvernance. La présidence d'ECSO a ainsi été confiée à un directeur d'une grande entreprise française du secteur ; une des vice-présidences est également assurée par le directeur général de l'ANSSI.

La mise en place d'un cadre européen de certification de sécurité permettra d'évaluer la sécurité des produits et services numériques et de renforcer leur sécurité, de contribuer à l'émergence d'un marché unique des produits et services et de renforcer la visibilité internationale des produits européens de cybersécurité. La France continuera à plaider pour la reprise des principes reconnus dans les accords de reconnaissance mutuelle existants (SOG-IS) comme étant les fondements nécessaires à la mise en place d'une véritable certification européenne, notamment pour les plus hauts niveaux de sécurité.

Le levier de la normalisation doit être mieux employé afin de faire valoir les qualités des normes européennes et d'anticiper les enjeux de sécurité et de confiance des industries à venir (notamment les objets connectés).

Afin d'assurer son autonomie stratégique, l'Europe devra enfin tirer parti de son excellence scientifique pour se placer parmi les meneurs de la prochaine révolution numérique, et ainsi acquérir la maîtrise des technologies stratégiques numériques de prochaine génération (par exemple, l'ordinateur quantique et l'intelligence artificielle).

3. RENFORCER L'INFLUENCE, L'ATTRACTIVITÉ ET LA SÉCURITÉ DE LA FRANCE ET DES ACTEURS FRANÇAIS DU NUMÉRIQUE

3.1. Faire de la France un pôle d'excellence dans le monde numérique

Le numérique constitue pour la France une nouvelle opportunité de développement, de croissance et de partage. Afin de saisir cette opportunité, notre pays a déjà entrepris des actions de fond, que ce soit par la transformation numérique de l'État ou en matière de politique économique. Il est essentiel de poursuivre dans cette voie afin de donner à notre pays une longueur d'avance. C'est pourquoi la France a décidé, en concertation étroite avec les acteurs du numérique, de poursuivre une politique combinant soutien à l'innovation et aux nouveaux modèles économiques, ouverture élargie des données, protection renforcée des personnes, renforcement de la loyauté des plateformes et déploiement de l'accès au numérique, notamment à travers le développement d'infrastructures à très haut débit. Cette politique a pour but de faire de la France une République numérique.

La France entend, à cet égard, promouvoir sa vision du numérique, que ce soit en matière de transformation numérique de l'État, d'ouverture des données publiques ou de protection des données personnelles, tout en développant des écosystèmes ouverts, depuis lesquels les start-up françaises pourront rayonner au-delà de nos frontières et dans lesquels seront accueillis des entrepreneurs, des talents et des investisseurs venus du monde entier. Il s'agit également d'explorer et de promouvoir toutes les nouvelles formes de création (transmédia, arts numériques, nouvelles écritures, etc.) et de valoriser la création française dans le domaine des arts numériques.

À cette fin, la France poursuivra les objectifs suivants :

Accompagner le développement des entreprises du numérique à l'international

Le gouvernement, en particulier les services compétents au sein du ministère de l'Europe et des Affaires étrangères (notamment DEEIT, Direction des entreprises, de l'économie internationale et de la promotion du tourisme) et du ministère de l'Économie et des Finances (notamment Direction générale du Trésor) s'engagent à continuer à accompagner le développement des entreprises du numérique à l'international, à travers deux politiques spécifiquement :

- une politique institutionnelle : mise en place d'une grande variété de programmes de soutien et d'aide à l'innovation pour différents types d'entreprises du numérique (start-up mais aussi grands groupes) afin qu'elles s'implantent, se développent et se financent plus facilement. Les exemples, notamment déclinés dans la Stratégie, sont nombreux : soutien à la *French Tech* et au dispositif de *French Tech* Ticket, mise en place du Passeport Talents, etc. ;
- une politique de soutien à l'export : accompagnement également des entreprises dans leurs démarches à l'export, notamment dans les marchés en développement (par exemple, en Afrique).

Ces politiques ont pour but de soutenir les acteurs français dans leur développement dans des marchés non nationaux (entrée dans de nouveaux marchés, scale up, consolidation). Certains segments sont ainsi particulièrement valorisés : c'est notamment le cas de la e-santé (avec le label French Healthcare, initiative du gouvernement combinant public et privé lancée à l'occasion d'une cérémonie au MEAE en mars 2017).

Soutenir au plan international une approche innovante en matière d'ouverture des données publiques

La France considère que l'ouverture des données publiques est un moyen de créer de

nouveaux services pour les citoyens, d'améliorer le fonctionnement des administrations et de répondre à l'exigence démocratique de transparence de la puissance publique. Forte de cette conviction, elle entend notamment améliorer l'accès aux documents administratifs, élargir les obligations de diffusion de données publiques ou encore ouvrir à la réutilisation des données collectées dans le cadre d'un service public industriel ou commercial. Chacune de ces actions, en grande partie menées avec le soutien d'Etalab, concoure à faire de la France un pays pionnier en matière d'open data, dans un équilibre maîtrisé entre ouverture et protection des données personnelles.

Cet engagement a conduit la France à participer activement à l'adoption de la Charte du G8 sur l'ouverture des données publiques du 18 juin 2013, qui énonce un principe d'ouverture par défaut des données publiques, affirme le principe de gratuité de leur réutilisation et encourage l'utilisation de formats ouverts et non-propriétaires. Cet engagement a également conduit la France à adhérer en 2014 au partenariat pour un gouvernement ouvert (Open Government Partnership). Ce partenariat est l'occasion pour la France de souligner son attachement aux formes participatives et innovantes de résolution des grands enjeux de société, mais aussi d'appuyer la multiplication des opportunités de dialogue entre les pouvoirs publics et une société civile créative, désireuse d'utiliser les ressources du numérique au service de l'intérêt général.

LE PARTENARIAT POUR UN GOUVERNEMENT OUVERT (PGO)
Le PGO rassemble actuellement 75 pays membres, ainsi que des centaines d'organisations non gouvernementales et représentants de la société civile. Il vise à promouvoir la transparence de l'action publique et la gouvernance ouverte, à améliorer la participation citoyenne à l'élaboration des politiques publiques, à renforcer l'intégrité publique et à combattre la corruption, grâce notamment aux nouvelles technologies et au numérique.
Au titre de sa coprésidence (2016-2017), la France a organisé le Sommet mondial du PGO à Paris en décembre 2016. Ce dernier a rassemblé plus de 4 000 participants de 150 nationalités différentes.
Au niveau national, le Deuxième « Plan d'action pour une action publique plus transparente et collaborative », en cours d'élaboration, renouvellera pour deux ans les engagements français au PGO. Les trois chantiers prioritaires des administrations françaises seront :
- **l'ouverture des données publiques ;**
- **l'innovation publique ;**
- **la participation citoyenne.**

On notera l'engagement croissant des collectivités territoriales, des Parlements et de la Cour des comptes.

Renforcer l'attractivité et l'internationalisation des écosystèmes numériques français

L'internationalisation est un facteur déterminant de réussite et de croissance pour les écosystèmes numériques français. Cette internationalisation ne peut être qu'un processus à double sens : le développement international des entreprises françaises du numérique est la condition de leur succès dans une compétition mondiale ; ce développement international est d'autant plus favorisé que la France parvient à attirer des entrepreneurs, des talents et des investisseurs venus du monde entier. L'action de la *French Tech*, qui s'est incarnée physiquement au sein de l'incubateur StationF a joué un rôle prépondérant dans la construction de cette image.

Forte de son réseau, l'action international du gouvernement a en effet pour mission d'accompagner les entreprises françaises du numérique dans leur développement international tout en favorisant le développement d'investissements étrangers dans les écosystèmes numériques français, mais également dans les pays les plus en pointe en matière de numérique, dans les pays émergents ou encore les pays francophones, dans lesquels les opportunités de croissance et de partenariats sont particulièrement nombreuses.

LA DIPLOMATIE ÉCONOMIQUE DE LA FRANCE POUR LE NUMÉRIQUE

L'Initiative *French Tech* est, depuis 2013 une ambition partagée, dont l'objectif est de favoriser l'émergence de *start-up* françaises, de les aider à grandir et à se développer internationalement tout en promouvant l'écosystème français à l'étranger. Son action internationale est structurée autour de trois piliers : l'émergence de *French Tech Hubs*, consistant à accroître la visibilité, le rayonnement et l'attractivité des écosystèmes situés dans les grandes métropoles étrangères ; le lancement de la Plateforme d'attractivité internationale de la *French Tech*, afin d'attirer des entrepreneurs et des investisseurs internationaux ; la remise d'un pack d'accueil – le *French Tech* Ticket – aux entrepreneurs étrangers désireux de créer leur start-up en France et plus récemment du *French Tech* VISA, procédure accélérée de délivrance du Passeport Talent pour les créateurs d'entreprises innovantes.

La France a aussi développé des programmes (NETVA, YEI Start in France, DARE ou encore COOPOL Innovation) qui permettent notamment aux entreprises françaises innovantes (start-up et PME de croissance) de nouer des partenariats technologiques avec des acteurs étrangers. Elle a également soutenu l'effort au développement et à l'exportation des Fin Tech (*big data*, *smart data*, robotique, intelligence artificielle, e-santé, *blockchain*), notamment à travers l'action du Fédérateur « Technologies Emergentes ».

Enfin, la France a œuvré pour que l'accès des PME aux flux de données et aux potentialités de l'économie numérique soit pleinement garanti. La France a ainsi mené une réflexion de fond sur la question de l'e-internationalisation des PME et sur les méthodes à développer pour permettre aux acteurs économiques d'avoir un accès égal aux perspectives de croissance offertes par l'économie numérique. Les travaux du Conseil National du Numérique (rapport 2016 « Croissance connectée, les PME contre-attaquent[3] ») et co-construits avec les services de l'État concernés proposent des éléments de réponses pour formuler une approche stratégique globale permettant à une diversité d'acteurs économiques d'exister et de croître dans le domaine du commerce en ligne. L'action de l'opérateur Business France sera également un pan important du développement des entreprises françaises à l'international.

3.2. Garantir la sécurité et l'autonomie stratégique de la France dans le monde numérique

L'autonomie stratégique de la France repose sur une capacité d'appréciation autonome ainsi que sur une liberté permanente de décision et d'action. Cette autonomie est aujourd'hui tributaire de la sécurité des réseaux informatiques et des infrastructures sur lesquels elle repose. Préserver les fonctions vitales remplies par ces réseaux et ces infrastructures fait donc partie des intérêts essentiels de la nation. Au-delà, la sécurité de nos entreprises et de nos citoyens dépend de plus en plus de réseaux numériques sûrs et fiables, garantissant la confidentialité, l'intégrité et la disponibilité de l'information.

Des menaces informatiques de nature, d'intensité, et d'origine variables, et provenant d'acteurs malveillants aux motivations diverses, pèsent sur ces intérêts. La fréquence et l'ampleur des attaques s'accroissent, au point de constituer un continuum de risques et de menaces, qui s'exercent sur tout le spectre d'intensité. Les menaces les plus graves proviennent à ce stade d'États qui n'hésitent pas à mobiliser de larges capacités offensives à des fins de déstabilisation, de destruction ou de poursuite de leurs intérêts économiques, en s'abritant derrière l'incertitude de l'attribution. En parallèle, des groupes d'attaquants montent en puissance, mettant leur compétence au service d'autres acteurs, selon une logique de mercenariat.

L'absence de régulation internationale, le défaut de protection de nombreux réseaux et le manque de culture de sécurité des utilisateurs créent un environnement national et international favorable à la prolifération de ces risques et menaces. Par ailleurs, l'agression est facilitée par le faible coût et la disponibilité des technologies. Enfin, l'interdépendance des réseaux signifie que la sécurité de chaque réseau dépend de la sécurité globale de l'environnement numérique.

---

3. Disponible sur le lien suivant : http://up.cnnumerique.fr/WEB_CNNum_2016_Croissance%20connecte&%23769%3Be_PE.pdf

Dans ce contexte, les réponses développées en France à titre national doivent se prolonger au plan international. La France poursuivra en priorité les objectifs suivants :

Contribuer au développement d'une pensée stratégique française sur les questions de cybersécurité

Il semble impératif de continuer à se doter, notamment au niveau national, de compétences et de connaissances en termes de prospective, de recherche et d'expertise pluridisciplinaire. Il est important également de prolonger les projets qui s'inscrivent dans cette perspective, comme l'initiative France IA mise en place par le Gouvernement et co-construite avec le monde de la recherche, les institutions publiques et les entreprises, ou le colloque « Construire la paix et la sécurité internationales de la société numérique » organisé les 6-7 avril par le SGDSN, en lien avec des acteurs privés et des chercheurs.

Plus généralement, il est important que le MEAE continue de promouvoir des pôles d'excellence spécialisés, interdisciplinaires, qui permettent de saisir les grandes transformations (dans le domaine de la sécurité mais pas seulement) à l'ère numérique.

Le MEAE s'engage également à coopérer avec les principaux *think tanks* et groupes de recherche français afin de les aider à développer une véritable expertise sur ces sujets.

LES PRINCIPAUX GROUPES DE RECHERCHE FRANÇAIS SUR LES ENJEUX NUMÉRIQUES : CHAIRE CASTEX ET AMNECYS

Inaugurée en novembre 2011, la Chaire Castex de Cyberstratégie développe la recherche fondamentale et appliquée en géopolitique du cyberespace. Elle nourrit la réflexion stratégique liée aux enjeux du cyberespace dans les domaines politique, économique, militaire et réglementaire. Pour ce faire, la Chaire Castex dispose d'une équipe de chercheurs, qui publie des articles, ouvrages scientifiques, cartographies et autres supports de réflexion. Elle constitue également une plateforme de ressources et d'échanges entre acteurs publics et privés. Elle anime des rencontres, en présence de spécialistes du cyberespace, destinées à un large public : chercheurs, entrepreneurs, militaires, élus. La Chaire a ainsi vocation à faire converger une diversité d'acteurs autour de l'étude, de la compréhension et de la sensibilisation aux enjeux du cyberespace.

Le réseau interdisciplinaire d'experts AMNECYS (*Alpine Multidisciplinary Network on Cybersecurity Studies*) travaille également sur les enjeux numériques, en orientant davantage la réflexion sur les questions juridiques de paix et de sécurité internationales. Fort de plus de 70 chercheurs issus de 9 laboratoires différents qui croisent sciences humaines et sciences dures, l'AMNECYS a déjà participé activement au développement d'une pensée stratégique en lien avec le SGDSN, notamment l'ANSSI, et d'autres équipes de recherche (*Interest Group on Peace and Security de la European Society of International Law*, etc.).

Accroître avec nos partenaires la résilience de notre environnement numérique

La France mène depuis 2008 un effort croissant de renforcement de sa cybersécurité. L'attention initialement portée sur les systèmes les plus sensibles (État, opérateurs d'importance vitale) laisse désormais place, dans la nouvelle stratégie nationale de sécurité du numérique d'octobre 2015, à une vision holistique de la cybersécurité qui innerve l'ensemble de la société française. Pour être à la mesure d'enjeux par nature transnationaux, la France doit également intégrer une dimension européenne et internationale à ses efforts.

Dans ce cadre, la France contribuera à renforcer la cybersécurité des organisations internationales dont elle est membre, notamment celles qui manipulent des informations constitutives de notre autonomie stratégique (Union européenne, OTAN). À l'échelle européenne et internationale, nous devons porter une attention particulière à la sécurité des ressources critiques et des opérateurs essentiels internationaux et transnationaux.

Dans un monde toujours plus interconnecté, nous sommes liés à la cybersécurité de nos partenaires. C'est pourquoi la France doit soutenir un effort de renforcement des capacités de cybersécurité des pays volontaires, à titre bilatéral ou dans le cadre d'initiatives

multilatérales, et avec l'appui du secteur privé. Cet effort ne pourra être conduit que dans un cadre de confiance, reposant sur une convergence d'intérêts et de valeurs.

Pour répondre à des crises affectant ses intérêts et ceux de ses principaux partenaires, la France contribue au développement d'un cadre volontaire européen de coopération pour la prévention et la résolution des incidents. Ce cadre repose en particulier sur le développement de standards opérationnels communs et de procédures de coopération entre partenaires, qui sont testés dans le cadre d'exercices paneuropéens. La France devra veiller à un renforcement des moyens dont dispose l'Union européenne pour animer ces efforts et à un renforcement de la coopération entre l'Union européenne et l'OTAN dans ce domaine.

Défendre la France et ses alliés dans le cyberespace

Le cyberespace est aujourd'hui devenu un lieu de confrontation, où la France doit garantir sa sécurité et protéger sa liberté d'action.

En effet, la France dispose, comme chaque État, d'un large panel d'options de réponses à une attaque informatique. Celles-ci sont de plusieurs ordres et fonctions de la gravité de l'attaque informatique et de sa caractérisation juridique. Dans le cyberespace, comme dans les autres domaines, le premier objectif poursuivi par la France sera la prévention des crises. Cela passe notamment par une stratégie visant à favoriser la coopération, à éviter l'escalade des tensions et à décourager les agressions.

Face à la menace, la France doit ainsi pouvoir mettre en œuvre toutes les mesures nécessaires et proportionnées en réponse à des attaques informatiques menaçant ses intérêts stratégiques. Elle renforce à cette fin ses capacités de caractérisation de la menace et d'attribution. Ces capacités pourront s'appuyer sur une échelle nationale de criticité de la menace, potentielle ou avérée, que représente une attaque informatique. Au-delà de son utilisation nationale, une telle échelle a également vocation à renforcer la coopération internationale en cas d'incident en favorisant le développement d'une compréhension commune des crises cyber.

La France répondra aux engagements qu'elle a pris envers ses alliés et ses partenaires de l'Union européenne et de l'OTAN qui seraient confrontés à des attaques de ce type, dans le respect de leur souveraineté et en tenant compte de leur responsabilité principale en matière de protection des réseaux. La solidarité avec nos partenaires ne peut être effective qu'en appui d'un effort de cyberdéfense mené par tous au niveau national.

Parfois, la réponse appropriée à une attaque informatique pourra être donnée à plusieurs. Dans tous les cas, elle se fondera sur une décision entièrement souveraine, de la France, comme de ses alliés.

> **L'ENGAGEMENT EN FAVEUR DE LA CYBERDÉFENSE DU SOMMET DE VARSOVIE**
> **À l'OTAN, la France a été à l'initiative dans l'adoption par les 28 Nations d'un Engagement pour la cyberdéfense (« *Cyberdefence Pledge* ») lors du Sommet de Varsovie en juin 2016, qui fixe à chaque nation le devoir de prévoir les ressources et la formation adéquates pour développer l'ensemble des compétences d'une cyberdéfense efficace « depuis l'hygiène informatique de base jusqu'aux moyens de cyberdéfense les plus sophistiqués et les plus robustes ». La mise en œuvre de cet engagement fera l'objet d'un suivi par l'ensemble des nations au cours des prochaines années.**

La France continuera par ailleurs d'adapter son outil de défense aux enjeux du combat numérique. En appui de ses opérations militaires, la France doit renforcer ses capacités informatiques défensives et offensives, dans le respect du droit international humanitaire. La France veillera également à l'intégration de la cyberdéfense aux opérations militaires de l'Union européenne et de l'OTAN.

Dans la durée, la France continuera à garantir son autonomie stratégique par le maintien des capacités industrielles, scientifiques et techniques nécessaires. La France s'engagera pour permettre le développement d'une base industrielle européenne compétitive en matière de cybersécurité afin de disposer de produits de confiance et de qualité.

Développer une cybersécurité collective à l'échelle internationale

Afin d'accroître la confiance au niveau global, et de limiter la prolifération des risques et des menaces dans l'environnement numérique, la France poursuivra un dialogue coopératif avec l'ensemble des acteurs privés et publics concernés, et l'ensemble des partenaires internationaux qui y sont prêts, sur le plan bilatéral comme multilatéral. La mise en œuvre de mesures de confiance (exemple : réseau de points de contact d'urgence) sera encouragée, notamment au sein de l'OSCE. L'émergence d'un cadre de cybersécurité collective, que la France appelle de ses vœux, ne pourra reposer que sur les équilibres définis par le droit international, et notamment la Charte des Nations unies.

Afin de prévenir les conflits dans le cyberespace, la France propose, dans la continuité des travaux conduits à l'ONU, la consolidation et la mise en œuvre d'un socle d'engagements de bonne conduite (« normes de comportement ») pour les États dans le cyberespace. Tout État responsable doit notamment s'engager à :

- faire preuve de transparence sur son organisation et sa posture nationale en matière de cybersécurité ;
- renforcer sur le plan national sa propre cybersécurité, et notamment celle de ses systèmes les plus sensibles, comme ceux des infrastructures critiques ;
- gérer les vulnérabilités informatiques de façon responsable, en s'assurant que son mode d'organisation institutionnel national favorise une telle gestion ;
- adopter un comportement coopératif vis-à-vis de pays victimes d'attaques émanant de son propre territoire, par application du principe de diligence requise, en particulier lorsque l'attaque vise une infrastructure critique ;
- s'engager, hors contexte d'opérations militaires, à ne pas piéger ou endommager des infrastructures critiques d'un autre État ou à détériorer leur capacité à fournir leur service au public ;
- garantir les droits fondamentaux de ses citoyens en ligne et hors ligne, conformément à ses engagements internationaux.

De plus, afin de favoriser une compréhension commune de l'applicabilité du droit international au cyberespace et de renforcer la stabilité de celui-ci, les États doivent reconnaître :

- la possibilité, pour tout État victime d'une cyberattaque, dans le cas où la situation est assez grave pour être considérée comme une menace contre la paix et la sécurité internationales, de saisir le Conseil de Sécurité des Nations unies ;
- le droit pour un État victime d'une cyberattaque dommageable de prendre les mesures techniques nécessaires et proportionnées visant à neutraliser les effets de cette attaque, dans le respect de ses obligations en matière de droit international ;
- la possibilité pour un État de considérer comme une agression armée au sens de l'article 51 de la Charte des Nations unies une cyberattaque contre une infrastructure critique paralysant, détruisant ou rendant inactives les fonctions et les activités vitales d'un État ou causant de sérieux dommages à la population.

Enfin, l'irruption du numérique comme outil et espace de confrontation confère au secteur privé, et notamment à un certain nombre d'acteurs privés systémiques, un rôle et une responsabilité inédits dans la préservation de la paix et de la sécurité internationale. Il faut donc que les États engagent entre eux, mais aussi avec le secteur privé et le monde de la recherche, de nouveaux travaux afin de définir des formes de régulation originales, adaptées à l'évolution du monde numérique et permettant de renforcer la stabilité, la coopération et la confiance de tous les acteurs dans le cyberespace. Trois axes d'efforts devront particulièrement être poursuivis :

- le renforcement de la sécurité des produits et des services numériques afin de s'assurer qu'ils ne peuvent pas être détournés de leur usage initial pour conduire des attaques informatiques ;
- la lutte contre la prolifération et la commercialisation d'éléments malveillants dans le cyberespace, notamment dans le cadre des accords de Wassenaar, où sera recherché un encadrement plus strict et rigoureux de certaines technologies dont l'export pourrait avoir

des effets néfastes pour la stabilité internationale ou le respect des droits de l'Homme ;
- l'encadrement de certaines pratiques particulièrement déstabilisatrices, comme celle du *hackback* qui consiste, pour un acteur privé, à s'arroger un droit à mener une contre-attaque dans le cyberespace dans une logique de légitime défense privée potentiellement déstabilisatrice.

La crédibilité des efforts dans ce domaine viendra de la capacité et de la volonté des États à reconnaître et rendre effectives les normes agréées au niveau international.