



LE HAUT REPRÉSENTANT DE  
L'UNION POUR LES AFFAIRES  
ÉTRANGÈRES ET LA  
POLITIQUE DE SÉCURITÉ

Bruxelles, le 5.6.2025  
JOIN(2025) 140 final

**COMMUNICATION CONJOINTE AU PARLEMENT EUROPÉEN ET AU CONSEIL**

**Une stratégie numérique internationale pour l'Union européenne**

## Une stratégie numérique internationale pour l'Union européenne

En Europe et dans le monde, la révolution liée aux technologies numériques et à l'intelligence artificielle (IA) remodèle les économies et les sociétés. Les acteurs économiques et les pays qui sont en mesure de maîtriser ces technologies bénéficient d'un avantage économique décisif au niveau de leur compétitivité et de leur efficacité, mais ils peuvent également les utiliser pour renforcer leur défense et leur sécurité nationales, ainsi que pour veiller à ce qu'elles soient alignées sur les valeurs fondamentales de leur société. À l'inverse, une adoption tardive de ces technologies risque d'entraîner un retard économique et de compromettre la souveraineté nationale.

Dans ce contexte, l'Union européenne (UE) est déterminée à renforcer sa compétitivité technologique et sa capacité d'innovation tout en collaborant avec ses partenaires et alliés afin de les aider dans leur propre transition numérique. Aucun pays ni aucune région ne peut faire face isolément à la révolution numérique et à la révolution de l'IA. L'UE reste attachée à l'ordre mondial fondé sur des règles et à la défense de ses valeurs fondamentales.

Pour la compétitivité, la sécurité économique et la capacité de défense de l'UE, il est essentiel de coopérer étroitement avec nos partenaires et nos alliés technologiques afin de renforcer la capacité des entreprises technologiques européennes à innover et à prospérer à l'échelle mondiale. Des efforts concertés de l'UE sont nécessaires pour que celle-ci puisse défendre ses intérêts et ses valeurs fondamentales dans le cadre de la gouvernance numérique mondiale.

La présente stratégie définit la base sur laquelle l'UE, selon une démarche concertée, s'appuiera pour atteindre ces objectifs.

### 1. LE NUMERIQUE EN TANT QU'ÉLÉMENT CENTRAL DE L'ACTION EXTERIEURE DE L'UE

Dans le contexte géopolitique actuel, l'UE demeure un partenaire fiable et prévisible, déterminé à renforcer ses relations existantes avec ses alliés internationaux et à établir de nouveaux partenariats mutuellement bénéfiques avec les acteurs qui souhaitent œuvrer à la réalisation d'objectifs communs. Le soutien de l'UE à un ordre mondial fondé sur des règles et aligné sur les valeurs de démocratie, d'état de droit et de droits fondamentaux est inébranlable.

Le réseau de partenariats bilatéraux et régionaux que l'UE ne cesse de tisser lui permet d'être plus forte sur la scène mondiale, en créant des coalitions pour la réalisation d'objectifs communs au sein des principales enceintes et organisations internationales. Qu'il s'agisse de contribuer à l'élaboration des normes dans les enceintes multilatérales ou de renforcer ses partenariats bilatéraux, l'UE entend avancer dans la réalisation de priorités concrètes et immédiates, tout en protégeant et défendant ses intérêts stratégiques<sup>1</sup>.

Comme le souligne le rapport de M. Draghi<sup>2</sup>, l'écart de productivité entre l'UE et les États-Unis qui se creuse depuis le milieu des années 1990 s'explique en grande partie par la plus grande

---

<sup>1</sup> Voir [conclusions](#) du Conseil européen du 17 avril 2024: «Le Conseil européen souligne en outre la nécessité de renforcer le rôle de chef de file de l'UE dans les affaires numériques mondiales et invite la Commission et le haut représentant à élaborer une communication conjointe sur le sujet» (p. 10).

<sup>2</sup> «L'avenir de la compétitivité européenne», rapport de Mario Draghi, 2024.

capacité des États-Unis en matière d'innovation, d'expansion à l'échelle mondiale et de réussite dans le secteur technologique. L'UE est par ailleurs confrontée au risque d'instrumentalisation de ses dépendances technologiques et économiques et au risque de fuite de technologies critiques. Comme indiqué dans la stratégie ProtectEU<sup>3</sup>, la frontière entre les menaces hors ligne et les menaces en ligne est de plus en plus floue et l'UE doit mieux coopérer avec ses partenaires pour lutter contre l'utilisation abusive des technologies.

L'UE peut compter sur plusieurs atouts pour renforcer sa compétitivité technologique et sa capacité d'innovation, comme indiqué dans la boussole pour la compétitivité de l'UE<sup>4</sup>. Elle dispose d'un marché unique numérique vaste et intégré et est le plus grand importateur et exportateur mondial de services fournis par voie numérique<sup>5</sup>. Elle accueille des entreprises qui sont des fers de lance technologiques au niveau mondial et de plus en plus de jeunes pousses technologiques y démarrent leurs activités<sup>6</sup>. Elle peut tirer parti d'activités de recherche et d'innovation d'envergure mondiale et a la capacité de fournir des solutions technologiques intégrées aux pays partenaires qui cherchent à préserver leur souveraineté numérique et à mettre en œuvre une transformation numérique centrée sur l'humain.

Dans le cadre de son programme d'action pour la décennie numérique à l'horizon 2030<sup>7</sup>, l'UE vise à stimuler les investissements dans les infrastructures de connectivité, les compétences et la recherche<sup>8</sup>, ainsi qu'à créer des conditions plus propices à l'émergence et à l'expansion de jeunes pousses de rupture européennes. Étant donné que les technologies telles que l'IA, les semi-conducteurs, l'informatique en nuage et l'informatique quantique modifient fondamentalement le paysage industriel ainsi que celui de la défense et de la sécurité, l'Europe a besoin d'une industrie capable de concevoir, de développer, de fabriquer et de fournir ces technologies et ces produits plus rapidement et à grande échelle.

En menant une **diplomatie numérique** de plus en plus active, l'UE a pu s'appuyer sur ces fondements solides qui la caractérisent pour faire progresser ses priorités internationales et établir des partenariats<sup>9</sup>. Les investissements et les initiatives lancés dans le cadre de la stratégie «**Global Gateway**», y compris dans les pays concernés par l'élargissement et les pays voisins, notamment les plans de croissance de l'UE, démontrent l'importance stratégique du secteur numérique d'un point de vue géopolitique, sécuritaire et économique.

À la lumière des atouts et des politiques et actions internes de l'UE, la stratégie numérique internationale pour l'Union européenne sera donc axée sur les objectifs suivants:

- a) **stimuler la compétitivité technologique de l'UE grâce à la coopération économique et commerciale.** L'UE continuera de coopérer avec des partenaires de confiance afin de renforcer son rôle de chef de file dans le domaine des technologies émergentes, notamment par la recherche et l'innovation et en attirant les investissements et les talents étrangers; utilisera ses outils internationaux pour élaborer ses propres solutions technologiques et les

---

<sup>3</sup> Communication intitulée «ProtectEU: une [stratégie européenne de sécurité intérieure](#)» [COM(2025) 148].

<sup>4</sup> Communication intitulée «Une boussole pour la compétitivité de l'UE» [COM(2025) 30 final].

<sup>5</sup> Voir source [OMC](#).

<sup>6</sup> COM(2025) 270 du 28.5.2025 – «Stratégie de l'UE en faveur des start-up et des scale-up».

<sup>7</sup> Voir texte complet du [programme d'action pour la décennie numérique](#).

<sup>8</sup> Comme indiqué dans la communication sur l'union des compétences [COM(2025) 90 final].

<sup>9</sup> Comme indiqué dans les [conclusions du Conseil des affaires étrangères sur la diplomatie numérique](#) de juin 2023.

promouvoir dans le monde entier; et élargira encore son réseau d'accords sur le commerce numérique;

- b) **promouvoir un niveau élevé de sécurité pour l'UE et ses partenaires.** Conformément aux engagements existants<sup>10</sup>, l'UE continuera de renforcer sa cybersécurité et sa cyberdéfense, en particulier en ce qui concerne les infrastructures critiques essentielles; renforcera la sécurité de la recherche tout en intensifiant la recherche dans les domaines liés à la sécurité; luttera contre les menaces hybrides et les activités de manipulation de l'information et d'ingérence menées depuis l'étranger; renforcera la résilience, la sécurité et la stabilité des chaînes d'approvisionnement des TIC, y compris au-delà de ses frontières; luttera contre la cybercriminalité au moyen d'opérations conjointes<sup>11</sup>, y compris dans le cadre d'une coopération bilatérale et multilatérale; et favorisera l'essor de fournisseurs fiables de technologies numériques, y compris dans le domaine des technologies à double usage telles que l'IA et l'informatique quantique;
- c) **façonner la gouvernance numérique mondiale et ses normes avec un réseau de partenaires.** L'UE continuera de défendre son approche fondée sur des valeurs pour la gouvernance numérique et les normes numériques afin de faire en sorte que la transformation numérique mondiale soit centrée sur l'humain, digne de confiance et respectueuse des droits de l'homme et des libertés fondamentales. En agissant avec détermination, l'UE peut être un acteur de premier plan pour faire avancer de façon responsable le progrès technologique au niveau mondial.

## 2. ÉLARGIR LE RESEAU DE PARTENAIRES INTERNATIONAUX DE L'UE

Grâce aux Conseils ministériels du commerce et des technologies<sup>12</sup>, aux partenariats numériques<sup>13</sup> et aux dialogues numériques<sup>14</sup>, l'UE a mis en place une **coopération numérique régionale et bilatérale forte avec ses partenaires**. Elle entretient des dialogues sur le cyberspace avec un large éventail de partenaires<sup>15</sup>, et les questions numériques sont une considération de plus en plus importante dans les partenariats globaux et stratégiques sur mesure<sup>16</sup>.

De plus, la coopération numérique s'appuie également sur l'association des pays partenaires à des programmes clés de l'UE, notamment Horizon Europe<sup>17</sup> et le programme pour une Europe numérique<sup>18</sup>, pour la coopération en matière de recherche et d'innovation avancées et le déploiement des technologies numériques.

L'harmonisation des principales politiques en matière de transformation numérique, l'investissement dans une connectivité numérique sécurisée et la stimulation de l'innovation sont également au cœur de la coopération de l'UE avec **les pays concernés par l'élargissement**

---

<sup>10</sup> La [stratégie ProtectEU](#) [COM(2025) 148], le [livre blanc conjoint pour une défense européenne – Préparation à l'horizon 2030](#), la stratégie européenne pour une union de la préparation [JOIN(2025) 130] et la [boussole stratégique](#) (7371/22).

<sup>11</sup> Par exemple: [Europol](#).

<sup>12</sup> Avec les États-Unis et l'Inde.

<sup>13</sup> Avec le Japon, la République de Corée, Singapour et le Canada.

<sup>14</sup> Avec le Brésil, le Mexique, l'Argentine, l'Australie et les Balkans occidentaux.

<sup>15</sup> L'Inde, le Japon, la République de Corée, le Brésil, les États-Unis, l'Ukraine et le Royaume-Uni.

<sup>16</sup> Avec des partenaires tels que la Tunisie, l'Égypte ou la Jordanie.

<sup>17</sup> Dix-neuf pays sont actuellement associés à Horizon Europe: voir liste [ici](#). En outre, la Suisse, la République de Corée et l'Égypte devraient devenir des pays associés en 2025, tandis que les négociations d'association progressent avec le Japon.

<sup>18</sup> Les pays associés au programme pour une Europe numérique sont énumérés [ici](#).

**et les pays voisins**, et ce dans le cadre d'instruments tels que les accords de libre-échange approfondis et complets ou les accords de stabilisation et d'association. Ces accords commerciaux et d'autres instruments connexes, tels que les plans de croissance pour les Balkans occidentaux<sup>19</sup>, la facilité pour les réformes et la croissance en faveur de la Moldavie<sup>20</sup> et la facilité pour l'Ukraine<sup>21</sup>, constituent une base stratégique pour l'intégration progressive des pays candidats dans le marché unique numérique<sup>22</sup>.

L'UE élabore actuellement un **nouveau pacte pour la Méditerranée** avec des partenaires du voisinage méridional, en s'appuyant sur le programme pour la Méditerranée de 2021, afin d'approfondir son engagement politique et de renforcer la coopération dans des domaines d'intérêt mutuel, notamment dans le domaine numérique.

L'UE ne cesse d'élargir son réseau d'**accords de libre-échange**<sup>23</sup> et d'accords sur le commerce numérique<sup>24</sup>. Avec ceux-ci, elle vise, entre autres, à mettre en place des règles de haut niveau en matière de commerce numérique qui garantissent un environnement en ligne sécurisé et sûr pour les consommateurs, sont source de transparence, de prévisibilité et de sécurité juridique pour les entreprises, et évitent ou suppriment les obstacles injustifiés au commerce numérique, y compris pour les flux transfrontières de données. En outre, la Commission assure la liaison avec d'autres autorités de réglementation et de contrôle de premier plan, en mettant en place de nouveaux réseaux concernant les services numériques et l'IA.

La stratégie «Global Gateway» offre l'occasion d'approfondir les partenariats, dialogues stratégiques et investissements avec des pays du monde entier, notamment dans le cadre de l'alliance numérique UE-Amérique latine et Caraïbes<sup>25</sup>, de l'arrangement administratif conclu avec Smart Africa<sup>26</sup>, de l'initiative de l'Équipe Europe pour l'Asie centrale<sup>27</sup> et des trains de mesures sur l'économie numérique adoptés avec des partenaires d'Afrique, d'Asie et d'Amérique latine<sup>28</sup>, y compris avec les pays les moins avancés. Les partenariats pour des échanges et des investissements propres<sup>29</sup> permettent à l'UE de tenir compte des liens qui existent entre les questions numériques, le commerce et les technologies propres.

La coopération numérique avec l'UE suscite de plus en plus d'intérêt dans le monde entier et, dans le paysage mondial actuel, de nouvelles formes de coopération, plus approfondies et plus

---

<sup>19</sup> Communication intitulée «Un nouveau plan de croissance pour les Balkans occidentaux» [COM(2023) 691].

<sup>20</sup> De plus amples informations sur la facilité pour les réformes et la croissance en faveur de la Moldavie sont disponibles [ici](#).

<sup>21</sup> [Facilité pour l'Ukraine – Commission européenne](#).

<sup>22</sup> Par exemple, après avoir transposé l'acquis pertinent de l'UE, l'Ukraine et la Moldavie sont en bonne voie pour se voir accorder un traitement mutuel sur le marché intérieur de l'itinérance.

<sup>23</sup> Des accords de libre-échange comportant des chapitres complets sur le commerce numérique ont été conclus avec le Royaume-Uni, la Nouvelle-Zélande et le Chili et sont en cours de négociation avec l'Inde, l'Indonésie, la Thaïlande, les Philippines et la Malaisie.

<sup>24</sup> L'accord sur le commerce numérique entre l'UE et Singapour a été signé le 7 mai 2025. Les négociations en vue de la conclusion d'un accord sur le commerce numérique avec la Corée se sont achevées en mars 2025. Les règles relatives aux flux transfrontières de données avec le Japon, qui complètent l'accord de libre-échange UE-Japon, sont entrées en vigueur en juillet 2024.

<sup>25</sup> [https://international-partnerships.ec.europa.eu/policies/global-gateway/eu-latin-america-and-caribbean-digital-alliance\\_en](https://international-partnerships.ec.europa.eu/policies/global-gateway/eu-latin-america-and-caribbean-digital-alliance_en).

<sup>26</sup> <https://digital-strategy.ec.europa.eu/en/news/eu-and-africa-strengthen-cooperation-digital-transformation>.

<sup>27</sup> [https://ec.europa.eu/commission/presscorner/detail/fr/ip\\_22\\_6963](https://ec.europa.eu/commission/presscorner/detail/fr/ip_22_6963).

<sup>28</sup> Depuis 2022, l'UE a lancé des trains de mesures sur l'économie numérique au Nigeria, en Colombie, en République démocratique du Congo, au Kenya et aux Philippines.

<sup>29</sup> [https://commission.europa.eu/topics/eu-competitiveness/clean-industrial-deal\\_fr](https://commission.europa.eu/topics/eu-competitiveness/clean-industrial-deal_fr).

souples, sont nécessaires pour favoriser des partenariats mutuellement bénéfiques en reconnaissant les progrès accomplis par bon nombre de nos partenaires dans le domaine numérique, qu'il s'agisse de la dématérialisation des services publics, de la facilitation des paiements électroniques, du soutien aux droits des citoyens ou du renforcement de la résilience locale. L'UE continuera de rechercher des formes de coopération, non seulement avec des partenaires de longue date qui partagent les mêmes valeurs, mais également avec tout pays désireux d'atteindre des objectifs communs.

Face à la nécessité d'accélérer sa transformation numérique dans un contexte géopolitique plus difficile, l'UE élargira donc son réseau de partenaires internationaux dans quatre directions:

- 1) l'UE **approfondira** ses partenariats et dialogues numériques existants, afin de **favoriser la coopération dans des domaines clés**, tels que la recherche et l'innovation, la coopération industrielle et stratégique en matière de technologies émergentes, la transparence et la résilience des chaînes d'approvisionnement mondiales, la sécurité et la durabilité des infrastructures numériques, le déploiement de l'IA et l'innovation, en privilégiant les avantages économiques mutuels et le renforcement de la sécurité économique. Elle proposera que ces partenariats intègrent de façon plus poussée des priorités supplémentaires, telles que la cybersécurité, la sécurité de la recherche, la protection des technologies sensibles et les aspects liés aux technologies à double usage. Elle continuera de participer à des activités avancées de coopération réglementaire. L'approfondissement des partenariats et dialogues numériques supposera également de renforcer le rôle des entreprises de l'UE et des pays partenaires, de stimuler la coopération entre les entreprises ainsi qu'entre les entreprises et les pouvoirs publics, et de rechercher en priorité des possibilités d'investissement;
- 2) l'UE **agrandira** le réseau de coopération existant en mettant en place de **nouveaux partenariats et dialogues numériques** et en élargissant le réseau d'**accords sur le commerce numérique**. Des partenaires prioritaires seront choisis sur la base des priorités de l'UE et de la coopération bilatérale et régionale existante au niveau de l'UE et des États membres. Dans le cadre de la stratégie «Global Gateway», l'UE s'emploiera à accroître les investissements européens dans les pays partenaires, afin de renforcer ses liens avec les centres de croissance numérique et de contribuer à sa sécurité économique;
- 3) l'UE **reliera** ces partenariats pour leur permettre de **fonctionner en réseau**. Plus le réseau de partenariats s'élargira, plus il existera des possibilités de travailler ensemble à la réalisation d'intérêts communs. De même, la coopération est de plus en plus nécessaire étant donné que nous sommes confrontés à des défis communs. Elle pourrait consister en des échanges techniques réguliers sur des enjeux communs (par exemple, les technologies émergentes, la connectivité sécurisée et fiable, la normalisation ou la coopération réglementaire), en la préparation de projets communs (par exemple, une coopération en matière de recherche et d'innovation, des projets pilotes en matière d'interopérabilité, des projets communs dans des pays tiers) et en l'organisation d'un réseau rassemblant des représentants de haut niveau de l'UE, de ses États membres et de ses partenaires;
- 4) l'UE **renforcera** les **partenariats en matière de sécurité et de défense**<sup>30</sup> en ce qui concerne les questions numériques, compte tenu de l'importance croissante des infrastructures et technologies numériques avancées. Mobiliser des investissements dans des capacités technologiques avancées à double usage et s'assurer que l'industrie

---

<sup>30</sup> L'UE a conclu de tels partenariats avec le Royaume-Uni, la Norvège, la Moldavie, la Corée du Sud, le Japon, l'Albanie et la Macédoine du Nord.

des technologies de sécurité et de défense de l'UE devienne un partenaire central et un moteur de l'innovation dans le domaine de l'IA, des technologies quantiques et d'autres technologies émergentes sont des priorités dans ce domaine.

L'UE est d'avis que le développement de l'IA est fondamental pour l'avenir de l'humanité et qu'il ne faut pas simplement y voir une lutte pour la suprématie entre les puissances à la pointe dans ce domaine. C'est pourquoi l'UE continuera de promouvoir son modèle ouvert et collaboratif pour le développement d'une IA digne de confiance, qui repose sur la participation des chercheurs et du secteur privé dans des «fabriques d'IA». À cet égard, la coopération avec des partenaires et alliés attachés aux mêmes principes qui partagent notre respect de l'état de droit et des valeurs fondamentales et démocratiques sera essentielle.

#### Exemples de futures actions

- Préparation de **nouveaux partenariats et dialogues numériques** potentiels, dans le cadre d'une approche de l'Équipe Europe, pour assurer une coopération étroite avec les États membres, l'industrie, les parties prenantes et les pays partenaires, notamment dans le cadre de la coopération de l'UE avec les pays voisins.
- Mise en place d'un **réseau de partenariat numérique** associant l'UE, ses États membres et ses partenaires.
- Renforcement de la coopération pour favoriser les **synergies entre les partenariats numériques** et les questions technologiques relevant des **partenariats de l'UE en matière de sécurité et de défense**.
- Élargissement du réseau d'**accords sur le commerce numérique** et poursuite des négociations en vue de la conclusion d'**accords de libre-échange, y compris dans le domaine du commerce numérique**.

### 3. L'OFFRE DE L'UE POUR LES ENTREPRISES TECHNOLOGIQUES

Afin de pouvoir dialoguer avec un ensemble plus large de partenaires de confiance, l'UE élaborera une **offre intégrée pour les entreprises technologiques**. Cette offre intégrée soutiendra entre autres le déploiement d'une connectivité, d'infrastructures publiques numériques, d'une IA et de solutions logicielles sûres et fiables. L'objectif sera d'adapter les volets liés aux technologies et de les regrouper dans le cadre d'une approche modulaire, en mettant en balance les intérêts des pays partenaires et de l'UE, afin de créer un **ensemble d'avantages mutuels**. Cette offre sera complétée par un renforcement des capacités et par des mesures visant à combler le déficit mondial de talents, et les efforts déployés pour la formation aux compétences numériques seront coordonnés avec les partenaires internationaux. L'UE promouvra activement des solutions numériques permettant une utilisation plus rationnelle de l'énergie et des ressources dans l'industrie manufacturière, les services et d'autres applications.

L'offre pour les entreprises technologiques sera gérée conjointement par l'UE et ses États membres dans le cadre d'une approche «**Équipe Europe pour les technologies**» et les entreprises de l'UE<sup>31</sup>, les institutions de financement du développement de l'UE et les

---

<sup>31</sup> Notamment par l'intermédiaire du [groupe consultatif des acteurs du marché sur la stratégie «Global Gateway»](#).

organismes de crédit à l'exportation y seront étroitement associés, tandis que le **D4D Hub**<sup>32</sup> et l'initiative faîtière EU4Digital<sup>33</sup> joueront un important rôle de facilitateur. L'offre s'appuiera sur les instruments de financement extérieur existants et sur des investissements du secteur privé. Il sera essentiel de coordonner les investissements dans le cadre des différents programmes, entre le secteur public et le secteur privé, et de continuer à améliorer l'environnement des entreprises. Pour ce faire, une étroite coopération sera nécessaire avec les délégations de l'UE et les ambassades nationales, par exemple par l'intermédiaire des **pôles numériques informels** que l'UE a mis en place dans un certain nombre de pays partenaires<sup>34</sup> pour promouvoir la coopération avec l'Équipe Europe. Dans les pays avec lesquels des partenariats stratégiques ont été conclus ou sont en cours de négociation, l'offre sera intégrée dans le cadre du partenariat existant ou négocié.

#### 4. DOMAINES PRIORITAIRES DE LA COOPÉRATION AVEC LES PAYS PARTENAIRES

La coopération avec les pays partenaires couvrira les domaines ci-après.

##### *Infrastructures numériques sûres et fiables*

La sécurité et la résilience des réseaux et infrastructures numériques sont essentielles pour permettre des avancées dans des secteurs critiques tels que ceux de l'énergie, des transports, de la finance et de la santé. L'UE, qui a déjà joué un rôle de premier plan dans ce domaine, poursuivra ses efforts, en s'appuyant sur des instruments tels que la **boîte à outils 5G**<sup>35</sup>, afin d'aider les pays partenaires qui sont tout aussi préoccupés par la nécessité d'asseoir leur économie numérique sur des bases sûres. Conformément à la récente communication relative au renforcement de la sécurité et de la résilience des câbles sous-marins<sup>36</sup>, cette approche pourrait être étendue aux câbles sous-marins et à d'autres infrastructures numériques critiques. Les efforts dans ce domaine pourraient faire l'objet d'une conférence annuelle visant à approfondir les contacts techniques et la compréhension des possibilités et des exigences en matière de sécurité pour les routes, les partenariats et les financements futurs, en contribuant au processus «Global Gateway».

L'UE encouragera le déploiement d'une connectivité numérique sécurisée et d'infrastructures durables dans le monde entier, pour garantir en particulier la sécurité et la fiabilité des réseaux 5G, des câbles sous-marins et terrestres, de la connectivité par satellite, des infrastructures internet, des supercalculateurs et des centres de données. Elle s'emploiera également à soutenir la résilience de ses partenaires par la diversification et l'intégration des réseaux, notamment grâce à la connectivité par satellite et à d'autres formes de réseaux non terrestres. Elle œuvrera à la mise en place d'un réseau de câbles de communication sous-marins et terrestres sûrs<sup>37</sup> reliant l'UE aux pays partenaires, ainsi qu'à une connectivité spatiale souveraine et résiliente.

---

<sup>32</sup> Le [Digital for Development \(D4D\) Hub](#) est une plateforme qui vise à renforcer la coopération et la coordination numériques entre l'Union européenne et ses États membres et les partenaires d'Afrique, d'Asie-Pacifique, d'Amérique latine et des Caraïbes, ainsi que les pays voisins de l'UE.

<sup>33</sup> L'initiative faîtière EU4Digital regroupe les programmes financés par l'UE visant à étendre les avantages du marché unique numérique aux pays du [partenariat oriental](#) et aux Balkans occidentaux.

<sup>34</sup> Au Kenya, en Tanzanie, au Nigeria, en Colombie et au Brésil.

<sup>35</sup> [Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures](#).

<sup>36</sup> [Communication conjointe intitulée «Plan d'action de l'UE sur la sécurité des câbles»](#) [JOIN(2025) 9 final].

<sup>37</sup> Conformément à la [recommandation de la Commission pour des infrastructures de câbles sous-marins sûres et résilientes](#) [C(2024) 1181] et à la [communication conjointe relative au renforcement de la sécurité et de la résilience des câbles sous-marins](#) [JOIN(2025) 9].

Toutes ces mesures devraient permettre à l'UE de se positionner comme une plateforme internationale capable d'héberger des données et des capacités de calcul dans un espace résilient et fiable, en mesure d'exploiter les possibilités offertes par l'économie des données et d'attirer les investissements dans des centres de données, des capacités informatiques et des capacités d'IA durables. En coopération avec les pays partenaires, l'UE s'efforcera activement de soutenir des solutions numériques permettant une utilisation plus rationnelle de l'énergie et des ressources dans l'industrie manufacturière, les services et d'autres applications, afin de réduire l'empreinte carbone et de faciliter l'adaptation au changement climatique et la résilience à celui-ci.

#### Exemples de futures actions dans le domaine de la **connectivité sécurisée**

- La **connectivité de l'Arctique** est une priorité stratégique pour l'UE, qui collaborera avec ses partenaires pour renforcer le soutien aux projets devant déboucher sur l'installation de nouvelles routes de câbles sous-marins dans la région, en utilisant le mécanisme pour l'interconnexion en Europe afin de catalyser les investissements publics et privés.
- Un élément clé des investissements au titre de la stratégie «**Global Gateway**» dans le secteur numérique est la mise en place d'un réseau de projets stratégiques d'infrastructures de câbles de communication sous-marins afin de connecter de manière sûre et résiliente l'UE et les pays partenaires. Les investissements concernent notamment:
  - 1) **BELLA**, le premier câble à fibres optiques transatlantique entre l'UE et l'Amérique latine et les Caraïbes, qui relie les instituts de recherche latino-américains, pour donner un accès rapide aux données d'observation de la Terre provenant de la composante Copernicus du programme spatial de l'UE. Ce projet sera élargi à l'Amérique centrale et aux Caraïbes et soutiendra le développement du calcul à haute performance dans la région;
  - 2) le câble sous-marin **MEDUSA**, soutenu par la Commission européenne et BEI Monde, qui fournira une connectivité à haut débit entre le nord et le sud de la Méditerranée et sera élargi à l'Afrique de l'Ouest;
  - 3) le projet **Blue-Raman**, un futur système de câbles sous-marins sûrs de 11 700 km reliant l'Europe à l'Inde et pour lequel des raccordements sont prévus au Moyen-Orient et en Afrique orientale, le long du corridor économique Inde - Moyen-Orient - Europe (IMEC). Grâce à sa forte dimension de connectivité reliant l'Europe et l'Inde via la région du Golfe, ce projet facilitera l'échange de données et renforcera la coopération avec les pays partenaires.
- La stratégie de l'UE pour la mer Noire reconnaît la **mer Noire** comme une voie d'accès essentielle reliant l'Europe au Caucase du Sud, à l'Asie centrale et au-delà. Afin d'améliorer la connectivité et les échanges avec la région du **partenariat oriental**, l'UE soutiendra, si les conditions le permettent, des investissements ciblés dans des infrastructures numériques pour financer le développement de futures liaisons numériques en mer Noire garantissant une connexion internet sûre et à haute capacité.
- L'**initiative de l'Équipe Europe pour l'Asie centrale** permettra de rendre la connectivité plus sûre, principalement dans les zones non desservies et mal desservies d'Asie centrale, grâce à un satellite fourni par le secteur privé de l'UE.

- **IRIS<sup>2</sup>**, la nouvelle composante de connectivité sécurisée par satellite du programme spatial de l'UE, offrira une couverture mondiale lorsque l'ensemble de la constellation aura été déployé. Dans une première phase, des projets pilotes seront mis en place en Afrique subsaharienne.
- **L'initiative de l'Équipe Europe pour une connectivité durable UE-ASEAN** dans le cadre de la stratégie «Global Gateway» comprend une composante numérique qui débouchera sur l'extension du site miroir Copernicus installé aux Philippines à d'autres pays de l'ASEAN, dont l'Indonésie et la Thaïlande.

### *Technologies émergentes*

- **Intelligence artificielle:** comme indiqué dans le plan d'action pour un continent de l'IA<sup>38</sup>, l'UE poursuivra ses discussions bilatérales, régionales et multilatérales avec des partenaires de confiance afin d'attirer des investissements dans l'UE, de soutenir la mise en place de conditions de concurrence équitables au niveau mondial pour une IA digne de confiance et de promouvoir la bonne gouvernance de l'IA à l'échelle mondiale. Elle agira également avec détermination pour se positionner comme un chef de file dans l'application de l'IA à la science pour sa propre compétitivité et pour amener des scientifiques de haut niveau à choisir l'Europe<sup>39</sup>. L'UE continuera de rechercher des formes de coopération avec des partenaires de confiance, notamment en ce qui concerne les aspects de l'IA liés à l'innovation, et œuvrera ainsi, par exemple, au déploiement de fabriques d'IA en dehors de l'UE et à leur connexion au réseau des fabriques d'IA de l'UE. Cette coopération comprendra également la fourniture d'un accès aux modèles et algorithmes d'IA, en particulier dans le cadre de projets liés à l'IA au service du bien public (par exemple, la lutte contre le changement climatique et le soutien à la transition propre, l'amélioration des soins de santé ou l'agriculture). Elle permettra également de tirer parti des données et services satellitaires publics et commerciaux de l'UE pour améliorer les solutions fondées sur l'IA en vue de relever des défis mondiaux, tels que la surveillance de l'environnement et la réaction aux catastrophes. Compte tenu de la nature à double usage de certaines applications d'IA, l'UE poursuivra ses travaux sur le rôle de l'intelligence artificielle dans la politique étrangère et de sécurité commune (PESC) et la politique de sécurité et de défense commune (PSDC), en coopérant avec les États membres pour faire en sorte que la PESC et la PSDC de l'UE puissent tirer parti des avancées technologiques de l'IA.
- **5G et 6G:** l'UE est la figure de proue mondiale de l'innovation dans le domaine de la connectivité avancée, comme la 5G et les solutions de réseaux fixes. L'objectif de parvenir à des normes communes pour la prochaine génération durable dès la conception (6G) nécessite une coopération avec des pays partageant les mêmes valeurs, coopération qui devra commencer dans la recherche et l'innovation et dans la normalisation. Le principal défi réside dans le développement et le choix des technologies 6G, notamment les technologies de réseau d'accès radioélectrique, y compris l'intégration des réseaux terrestres et non terrestres. L'industrie de l'UE peut jouer un rôle moteur pour que la 6G se développe conformément aux normes de l'UE, notamment en matière de cybersécurité, d'interopérabilité et de respect des normes légales en matière d'accès, et bénéficiera de la coopération avec des pays disposant d'atouts complémentaires dans la chaîne de valeur (microélectronique, appareils, informatique en nuage ou IA, par exemple).
- **Semi-conducteurs:** face à l'incertitude géopolitique et à la complexité croissante des chaînes d'approvisionnement des semi-conducteurs, une approche adaptée et propre à

<sup>38</sup> [Communication intitulée «Plan d'action pour un continent de l'IA»](#) [COM(2025) 165].

<sup>39</sup> [Choisissez l'Europe: faites progresser votre carrière dans la recherche dans l'UE.](#)

chaque pays s'impose, l'objectif étant de faire en sorte que l'UE s'allie à des leaders mondiaux de l'écosystème des semi-conducteurs tout en préservant ses propres intérêts technologiques, économiques et sécuritaires. L'UE continuera de dialoguer avec les pays avec lesquels la collaboration dans des domaines tels que la recherche et le développement préconcurrentiels et la résilience de la chaîne d'approvisionnement est mutuellement bénéfique. Conformément à la stratégie en matière de sécurité économique<sup>40</sup>, l'UE défendra également ses intérêts en matière de sécurité économique, notamment dans le cadre de discussions bilatérales, régionales et multilatérales, en encourageant l'échange d'informations afin de prévenir les perturbations de la chaîne d'approvisionnement, en atténuant les risques et en attirant les talents mondiaux afin de combler le déficit de compétences dont pâtit l'écosystème européen des semi-conducteurs.

- **Technologies quantiques:** l'adoption de normes et d'applications communes dans le domaine des technologies quantiques exige une collaboration internationale solide, en particulier en ce qui concerne la recherche et l'innovation. L'UE renforcera ses liens, sur une base réciproque, avec les pays qui peuvent lui offrir des atouts complémentaires dans la chaîne de valeur des technologies quantiques (informatique, détection, communication ou cryptographie post-quantique sûre, par exemple) et dans des domaines connexes. Elle reste attentive au rôle des technologies quantiques dans le futur paysage sécuritaire et entretient des contacts réguliers avec l'OTAN et d'autres partenaires concernés sur le terrain. Elle unira ses forces à celles des pays partenaires pour trouver des applications concrètes des technologies quantiques dans les politiques sectorielles, par exemple pour le développement de nouveaux matériaux.

#### Exemples de futures actions dans le domaine des **technologies émergentes**

- L'UE mettra en œuvre des projets conjoints de recherche et d'innovation dans le domaine des technologies quantiques avec le **Japon**, la **République de Corée** et le **Canada**.
- Dans le cadre du **Conseil du commerce et des technologies UE-Inde**, l'UE et l'Inde travaillent à l'élaboration d'un programme spécifique qui facilitera les échanges de talents et favorisera les compétences des étudiants et des jeunes professionnels dans le domaine des semi-conducteurs.
- Dans le cadre de l'alliance numérique UE-Amérique latine et Caraïbes, l'UE établira un partenariat solide pour fédérer des ressources afin de développer le calcul à haute performance **en Amérique latine et dans les Caraïbes** et renforcer leur interopérabilité et leur intégration avec l'écosystème européen du calcul à haute performance.
- L'UE assurera le suivi des engagements pris lors de la **réunion ministérielle UE-Union africaine** (mai 2025) en vue d'une collaboration destinée au développement d'écosystèmes d'innovation régionaux, à la mise en place de stratégies d'IA et de cadres de gouvernance numérique.
- L'UE soutiendra le déploiement de **fabriques d'IA** dans les pays partenaires fiables, en les aidant à développer leur infrastructure de calcul tout en les connectant de manière sécurisée à l'UE et à son écosystème de fabriques d'IA.
- L'UE collaborera avec les États membres pour définir les domaines dans lesquels l'**intelligence artificielle** peut faciliter la mise en œuvre de la politique étrangère et de sécurité commune et de la politique de sécurité et de défense commune.
- L'UE continuera de soutenir l'**innovation dans le domaine de la défense** par l'intermédiaire de son **programme d'innovation dans le domaine de la défense (EUDIS)** et étudiera les moyens de renforcer la collaboration avec l'Ukraine dans ce domaine.

<sup>40</sup> Communication relative à la stratégie européenne en matière de sécurité économique [JOIN(2023) 20 final].

- L'UE étudiera, en dialogue étroit avec des partenaires de confiance tels que la Norvège et l'Ukraine, de nouveaux moyens d'encourager les synergies avec le pôle d'innovation européenne dans le domaine de la défense (HEDI).

## *Cybersécurité*

Dans le monde hyperconnecté d'aujourd'hui et dans le paysage géopolitique actuel en constante évolution, les cybermenaces émanant d'acteurs étatiques et non étatiques ne s'arrêtent pas aux frontières. Une cyberattaque ou un incident frappant un seul pays peut paralyser des entreprises et des infrastructures dans le monde entier, et nos citoyens et nos entreprises dépendent de produits et de solutions numériques qui proviennent de pays tiers. Le renforcement de la cybersécurité et de la cyberdéfense, y compris de la capacité à détecter les menaces et incidents de cybersécurité, à s'y préparer et à y réagir, et l'amélioration de l'échange d'informations sur les cybermenaces avec les partenaires internationaux afin d'améliorer le temps de réaction et la résilience sont des investissements qui bénéficient directement à la sécurité de l'UE. Cela se vérifie tout particulièrement dans le voisinage de l'UE, où cette dernière est pleinement déterminée à aider les pays concernés par l'élargissement à renforcer leurs capacités de cybersécurité et de cyberdéfense.

L'UE dispose également des outils nécessaires pour jouer un rôle de premier plan à l'échelle mondiale en matière de cybersécurité. Avec le règlement sur la cyberrésilience<sup>41</sup>, l'UE montre une nouvelle fois la voie en ce qui concerne la sécurité des produits dès la conception. Alors que les pays du monde entier cherchent à sécuriser leurs chaînes d'approvisionnement, le savoir-faire de l'UE en matière de sécurité des produits constitue une base solide pour l'établissement de partenariats internationaux. Dans le même ordre d'idées, à un moment où les partenaires internationaux de l'UE investissent dans la sécurisation de leurs infrastructures critiques, des débouchés commerciaux émergent dans des domaines dans lesquels l'UE peut se prévaloir d'une industrie forte, comme la cryptographie et les produits numériques hautement sécurisés.

Compte tenu de leur forte incidence sur les entreprises et les hôpitaux, les rançongiciels demeurent un fléau mondial, qu'aucun pays ne peut combattre seul. Conformément à la stratégie ProtectEU, l'UE plaidera en faveur d'une coopération internationale renforcée afin de démanteler les infrastructures qu'utilisent les groupes criminels menant des attaques par rançongiciel, de tarir leurs sources de revenus, de garantir des sanctions plus efficaces à l'encontre des auteurs et des facilitateurs et de traduire les cybercriminels en justice.

Dans le cadre de ces efforts, l'UE encouragera également le renforcement de la cyberrésilience dans les secteurs qui dépendent de plus en plus des technologies numériques, telles que ceux des transports et de la mobilité intelligente, pour lesquels des infrastructures, des données et des services sûrs sont essentiels pour garantir la continuité opérationnelle et la confiance du public.

Les efforts déployés récemment ont permis aux pays candidats associés au programme pour une Europe numérique d'accéder à la réserve de cybersécurité créée au niveau de l'UE par le règlement sur la cybersolidarité<sup>42</sup>. En outre, l'Agence de l'Union européenne pour la

---

<sup>41</sup> Règlement (UE) 2024/2847.

<sup>42</sup> Règlement (UE) 2021/694.

cybersécurité (ENISA) poursuivra sa coopération en matière de cybersécurité avec les pays tiers concernés, y compris le renforcement des capacités dans les pays candidats et les pays voisins.

#### Exemples de futures actions dans le domaine de la **cybersécurité**

- L'UE collaborera avec des partenaires pertinents pour étudier la possibilité de conclure des **accords de reconnaissance mutuelle** concernant le règlement sur la cyberrésilience et les cadres respectifs de ces partenaires afin de faciliter le respect des exigences en matière de cybersécurité des produits.
- L'UE continuera de coopérer avec les pays partenaires afin de renforcer la cyberrésilience à l'échelle mondiale et de contribuer à un cyberspace libre, ouvert, sûr et sécurisé. Solidement ancré dans la stratégie «Global Gateway», le soutien à la cybersécurité et au **renforcement des capacités en matière de cybersécurité** sera axé sur la sécurisation des infrastructures critiques et le renforcement des cyberécosystèmes, notamment grâce à l'élaboration et à la mise en œuvre de cadres réglementaires et stratégiques pertinents, ainsi que sur l'hygiène informatique et la formation à la cybersécurité.
- Aux Nations unies et au sein des organes de sécurité régionaux, l'UE continuera de plaider pour un **comportement responsable des États dans le cyberspace**, sur la base du cadre approuvé par l'Assemblée générale des Nations unies. Il s'agit notamment de faire respecter le droit international, de se conformer aux normes de conduite des États en temps de paix acceptées au niveau mondial, d'élaborer des mesures de confiance et d'aider les États à renforcer leur capacité à mettre en œuvre ces éléments du cadre.
- L'UE améliorera l'imputation des **cyberattaques** à des acteurs malveillants, y compris des acteurs étatiques, et continuera d'élaborer les **mécanismes de sanctions** y afférents.

#### *Activités de manipulation de l'information et d'ingérence menées depuis l'étranger*

Avec ses partenaires, l'UE protégera également mieux les citoyens contre les campagnes de manipulation de l'information et d'ingérence menées depuis l'étranger ou contre d'autres risques pour la société découlant des plateformes en ligne. Dans ce but, et pour renforcer la responsabilité ainsi que la confiance du public, il est essentiel de garantir la transparence des algorithmes utilisés pour recommander et modérer les contenus.

Cet objectif est également pertinent pour les pays candidats, les pays candidats potentiels et les pays voisins, compte tenu de leurs vulnérabilités spécifiques à la désinformation et aux activités d'ingérence menées depuis l'étranger, et cela permettra de renforcer notre résilience mutuelle, y compris notre résilience démocratique.

#### Exemples de futures actions dans le domaine des **activités de manipulation de l'information et d'ingérence menées depuis l'étranger**

- À la suite d'une intensification de ses travaux en matière d'imputation des cyberattaques à des acteurs précis, l'UE améliorera l'**imputation des incidents** de manipulation de l'information et d'ingérence provoqués depuis l'étranger.

#### *Identités numériques et infrastructures publiques numériques (IPN)*

L'expérience que l'UE a acquise en ce qui concerne le développement de portefeuilles d'identité numérique open source et d'infrastructures publiques numériques sûres et conformes

aux exigences de protection des données revêt une grande valeur qui dépasse ses frontières. La coopération internationale et les accords de reconnaissance mutuelle avec des partenaires clés peuvent simplifier les activités transfrontières des entreprises et faciliter la mobilité des citoyens. L'UE continuera notamment de rechercher des formes de coopération avec des pays tiers (tels que l'Ukraine, la Moldavie, les pays des Balkans occidentaux, le Japon, l'Inde et l'Égypte) afin de parvenir à une utilisation transfrontière fluide de services de confiance. Elle promouvra également le cadre d'interopérabilité européen<sup>43</sup> afin de soutenir la modernisation administrative et l'intégration numérique transfrontière des pays partenaires, y compris l'alignement sur les normes et pratiques de l'UE. Elle continuera de promouvoir l'utilisation de normes ouvertes et de spécifications communes afin de garantir l'interopérabilité, la transparence et la réutilisation<sup>44</sup>.

#### Exemples de futures actions dans le domaine des **infrastructures publiques numériques** sûres

- L'UE soutiendra le développement de **services et de solutions d'identité numérique fiables** (sur la base des spécifications du portefeuille d'identité numérique de l'UE), en plaçant au cœur d'un ensemble interopérable et évolutif de modules et de solutions numériques, y compris open source, afin de soutenir la transformation numérique des administrations publiques et des entreprises des pays partenaires. Elle poursuivra également ses travaux avec l'Ukraine, la Moldavie et les Balkans occidentaux, afin de préparer leur intégration progressive dans le portefeuille d'identité numérique de l'UE.
- L'UE coopérera avec des pays tels que l'Inde, l'Égypte, l'Uruguay et le Brésil dans le domaine des **signatures électroniques et de l'interopérabilité des infrastructures publiques numériques**, en vue de générer des avantages pour les entreprises et les citoyens, tant dans l'UE que dans les pays partenaires.
- L'UE soutiendra une approche d'**interopérabilité par défaut** fondée sur le cadre d'interopérabilité européen, afin de faciliter l'échange continu de données par-delà les frontières.
- L'UE continuera de collaborer avec ses principaux partenaires internationaux (Japon, Inde, Singapour, Australie, Nouvelle-Zélande et Malaisie) afin de promouvoir le modèle de **facturation électronique** de l'UE, sur la base de la norme européenne en la matière et de spécifications techniques interopérables.

#### *Plateformes en ligne*

Le règlement de l'UE sur les services numériques<sup>45</sup> protège la démocratie, la liberté d'expression, la vie privée, la sûreté et la sécurité des enfants en ligne et fournit un cadre sûr pour la vente de biens conformes à la législation. Le règlement sur les marchés numériques<sup>46</sup> et la politique de concurrence de l'UE favorisent la contestabilité des marchés numériques, des conditions de concurrence équitables et une concurrence loyale entre les acteurs numériques.

<sup>43</sup> Qui fait partie de la communication intitulée «Cadre d'interopérabilité européen – Stratégie de mise en œuvre», [COM(2017) 134].

<sup>44</sup> On peut citer comme exemple pertinent le [profil d'application DCAT \(pour «Data Catalog Vocabulary» – vocabulaire du catalogage de données\)](#), devenu une norme de fait, qui facilite l'harmonisation des descriptions des métadonnées et l'échange continu de données par-delà les frontières.

<sup>45</sup> Règlement (UE) 2022/2065 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (JO L 277 du 27.10.2022, p. 1).

<sup>46</sup> Règlement (UE) 2020/1828.

Ces actes complètent la protection assurée dans l'environnement numérique par le RGPD<sup>47</sup> et la législation en matière de protection des consommateurs.

La protection et l'autonomisation des mineurs en ligne sont des priorités mondiales. En vertu du règlement sur les services numériques, toutes les plateformes en ligne doivent garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs sur leurs services. En outre, les plus grandes plateformes en ligne doivent évaluer et atténuer chaque année tout risque systémique que leurs services présentent, y compris pour le respect des droits de l'enfant et, plus généralement, pour la protection des mineurs. Le règlement sur les services numériques est soutenu et complété par la stratégie pour un internet mieux adapté aux enfants. En particulier, l'UE cofinance le réseau de lignes d'appel d'urgence mis en place dans les États membres pour lutter contre la diffusion de matériel pédopornographique en ligne. La coopération internationale est assurée par l'intermédiaire du réseau INHOPE, qui regroupe 55 lignes d'appel d'urgence opérant dans le monde entier.

La protection forte et constante des consommateurs sur les places de marché en ligne est une autre priorité que l'UE partage avec bon nombre de ses partenaires internationaux et est une considération essentielle du règlement sur les services numériques, ainsi que des cadres en matière de protection des consommateurs et de sécurité des produits. En vertu du règlement sur les services numériques, toutes les places de marché en ligne sont tenues de respecter des normes strictes en matière de sécurité, de transparence et de responsabilité afin de garantir que leurs services ne servent pas à la vente de produits illégaux et dangereux aux consommateurs de l'UE. La communication de 2025 sur le commerce électronique<sup>48</sup> complète ces règles en définissant de nouvelles mesures pour relever les défis liés à la multiplication des produits dangereux, contrefaits et autrement illicites vendus par l'intermédiaire des plateformes en ligne. L'UE accordera la priorité à la coopération avec les pays partenaires et au sein des enceintes multilatérales afin de trouver des solutions conjointes aux risques communs pour la sécurité des consommateurs qui sont liés aux places de marché en ligne.

#### Exemples de futures actions dans le domaine des **plateformes en ligne**

- L'UE continuera de promouvoir son approche réglementaire et les principes qui la sous-tendent au niveau bilatéral et multilatéral et de partager son expérience dans leur mise en œuvre.
- L'UE organisera des **événements régionaux** avec des organisations internationales, des législateurs de pays tiers, des autorités de réglementation et la société civile afin de promouvoir la liberté d'expression et la sécurité en ligne.

## 5. GOUVERNANCE NUMERIQUE MONDIALE

Pour la réalisation de ses objectifs dans le domaine numérique, l'UE continuera de suivre une **approche multilatérale et multipartite** et garantira une participation significative des parties prenantes concernées, y compris la société civile, le monde universitaire et le secteur privé, en s'appuyant sur les liens forts qui existent avec les pays partenaires.

Les partenariats et dialogues numériques de l'UE permettent une **coordination** en amont des discussions dans les enceintes multilatérales et régionales, l'UE pouvant créer des coalitions

<sup>47</sup> Règlement (UE) 2016/679.

<sup>48</sup> Une boîte à outils complète de l'UE pour un commerce électronique sûr et durable [COM(2025) 37 final].

fortes en vue de la réalisation d'objectifs communs au sein des principales enceintes et organisations internationales, telles que les Nations unies, le G7, le G20, l'OCDE et le Conseil de l'Europe, ainsi que dans le cadre des institutions mondiales de gouvernance de l'internet. En particulier, avec ses partenaires du G7, l'UE continuera d'œuvrer à l'élaboration et à l'adoption de **normes de sécurité économique** – y compris, le cas échéant, pour les technologies numériques –, en tenant compte de divers critères tels que la transparence, la diversification de l'approvisionnement, la sécurité, la durabilité, la confiance et la fiabilité.

Le **pacte numérique mondial** des Nations unies a été adopté par consensus en tant que premier cadre global pour la gouvernance numérique mondiale. Il définit les objectifs, les principes, les engagements et les actions qui devront déboucher sur un avenir numérique ouvert, libre et sûr pour tous. L'UE continuera de participer activement aux travaux de mise en œuvre du pacte numérique mondial afin de défendre ses réalisations, tout en veillant à ce que les efforts ne se chevauchent pas et en maximisant les synergies avec l'architecture numérique mondiale existante, y compris le cadre de gouvernance de l'internet.

Outre ces processus, l'UE privilégiera la **normalisation** en tant qu'outil essentiel pour faire progresser ses objectifs. Elle peut compter sur plusieurs atouts, notamment une solide base de recherche et d'innovation, des entreprises qui sont des fers de lance technologiques au niveau mondial et de nombreuses PME et jeunes pousses innovantes qu'il y a lieu d'encourager à participer à l'élaboration de normes internationales. En tirant parti de son système de normalisation afin d'accroître son influence dans le processus d'élaboration de normes internationales applicables aux principales technologies numériques, l'UE entendra renforcer la compétitivité de son industrie, favoriser la souveraineté numérique et technologique et protéger et défendre ses valeurs et intérêts fondamentaux tout en œuvrant à une coopération internationale en matière de normalisation. L'UE reconnaît le rôle important de l'Union internationale des télécommunications (UIT) dans le contexte de la normalisation mondiale.

Reconnaissant que le spectre radioélectrique est une ressource naturelle rare dont dépendent toutes les applications numériques sans fil, l'UE continuera également de défendre dans le cadre mondial de l'UIT une répartition des **radiofréquences** équitable et fondée sur des règles.

La coopération multilatérale est également essentielle pour traiter les aspects numériques d'autres secteurs, notamment le secteur de l'énergie, en raison de l'augmentation rapide de la demande d'énergie de l'IA. L'UE participe à des **initiatives internationales dans le domaine de l'énergie**, telles que la conférence ministérielle sur l'énergie propre, qui élaborent des approches collaboratives pour relever ces défis.

Alors que les technologies numériques continuent d'évoluer rapidement, la **gouvernance mondiale de l'internet** doit s'adapter aux nouveaux défis géopolitiques, tels que les risques de fragmentation, l'augmentation de l'utilisation abusive des outils numériques pour des pratiques telles que les coupures et la censure de l'internet et l'élargissement des fractures numériques. En outre, avec la transition vers le **web 4.0** – mue par des technologies de base telles que l'intelligence artificielle, la réalité étendue et la réalité virtuelle, les chaînes de blocs et l'informatique quantique –, la gouvernance est confrontée à de nouvelles complexités qui nécessitent des cadres multipartites actualisés, efficaces et inclusifs. L'UE continuera de façonner l'approche multipartite et inclusive de la gouvernance de l'internet et s'engage à améliorer en permanence son efficacité, en s'opposant aux initiatives en faveur d'architectures

internet contrôlées par les États, qui pourraient fragmenter l'internet et compromettre l'ouverture et la sécurité qui le caractérisent depuis l'Agenda de Tunis<sup>49</sup>.

L'UE continuera de défendre de manière proactive la disponibilité et l'intégrité générales de l'internet en tant que réseau de réseaux mondial et interopérable, en promouvant l'importance du modèle multipartite de gouvernance de l'internet, par exemple lors des prochaines éditions du Forum sur la gouvernance de l'internet et des négociations à l'occasion du bilan des vingt ans du Sommet mondial sur la société de l'information (**SMSI+20**). L'UE reconnaît le rôle central de l'ICANN dans la gestion des fondements de l'architecture internet.

#### Exemples de futures actions dans le domaine de la **gouvernance numérique mondiale**

- L'UE s'emploiera à assurer un suivi et un réexamen **appropriés** de la mise en œuvre des engagements pris dans le cadre du **pacte numérique mondial**.
- L'UE travaillera selon une approche «Équipe Europe» pour garantir un résultat approprié lors des négociations à l'occasion du **bilan du Sommet mondial sur la société de l'information (SMSI+20)**.
- L'UE soutiendra l'extension et l'élargissement à l'échelle internationale de la **pile de protocoles de l'internet ouvert** (la structure fondamentale des protocoles qui permettent la communication et l'échange d'informations sur l'internet), afin de répondre aux besoins des pays partenaires, notamment pour renforcer la confiance et la sécurité.

## 6. UNE EUROPE COMPETITIVE ET SURE, OUVERTE AUX ENTREPRISES ET CONNECTEE AU MONDE

Dans un monde instable, l'UE est un partenaire constant, prévisible et fiable. Face à la complexité des chaînes de valeur technologiques, aucun pays ni aucune région ne peut exploiter isolément le potentiel de la révolution numérique et de la révolution de l'IA. Les efforts dans le domaine numérique que l'UE déploie en son sein et au-delà de ses frontières sont étroitement liés et se renforcent mutuellement. C'est pourquoi, au lieu de se limiter à stimuler son propre secteur numérique, depuis les fabriques d'IA jusqu'aux technologies de la défense, l'UE conclut également des partenariats d'ampleur qui apportent des avantages visibles à ses citoyens et à ses entreprises ainsi qu'à ses partenaires.

L'UE, qui plaide toujours pour que des solutions multilatérales soient trouvées aux défis mondiaux, continuera d'apporter un soutien sans faille aux Nations unies, au G7, au G20, à l'OCDE et aux autres organismes qui nous permettent de relever ensemble les défis majeurs de notre époque.

L'UE est prête à unir ses forces à celles de ses partenaires pour trouver de nouvelles formes de coopération, plus approfondies et souples, propices à des partenariats mutuellement bénéfiques, afin de renforcer la compétitivité et la sécurité de l'Europe. Elle continuera d'agir de manière constructive dans le respect de l'ordre international fondé sur des règles.

<sup>49</sup> [Agenda de Tunis pour la société de l'information](#), 18 novembre 2005.