RAPPORT : DIPLOMATIE DU NUMÉRIQUE EN FRANCE

Contribution à l'étude « Diplomatie et droits de l'Homme » de la Commission Nationale Consultative des Droits de l'Homme

sous la direction de la sous-commission « Affaires internationales et européennes »

Pour EUCLID et la CNCDH.

JALLAD Cherifa, Master 2 Théorie et Pratique du droit international et européen.

FARACCI Alice, Master 2 Droit européen.

BUISSONNIER Laure, Master 2 Droit européen.

Université Paris Nanterre

Nous remercions la CNCDH pour cette collaboration intéressante, qui nous a permis de nous enrichir sur le plan intellectuel. Nous sommes reconnaissantes d'avoir pu participer à ce projet dans ses prémices, et d'avoir pu être présentes lors de réunions officielles.
Un spécial remerciement est dédié à Madame EUDES et Monsieur TABBAL pour leur investissement et leur confiance. Enfin, nous remercions la clinique juridique EUCLID et ses directrices pour ce partenariat.

LISTE DES ABRÉVIATIONS

CEDH : Convention européenne des droits de l'homme

CDH : Conseil des droits de l'homme

CIDE : Convention internationale des droits de l'enfant

CNCDH : Commission nationale consultative des droits de l'homme

HCDH : Haut-Commissariat des Nations unies aux droits de l'homme

IA : Intelligence artificielle

OG : Observation générale

OMS : Organisation mondiale de la santé

ONU : Organisation des Nations unies

ONG : Organisation non gouvernementale

PESC : Politique étrangère et de sécurité commune

PIDCP : Pacte international relatif aux droits civils et politiques

RGPD : Règlement général sur la protection des données

SEAE : Service européen pour l'action extérieure

UE : Union européenne

SOMMAIRE

INTRODUCTION

Le 10 décembre 2023, à l'occasion du 75e anniversaire de la Déclaration universelle des droits de l'homme, le président de la République Emmanuel MACRON a déclaré :

> « *Le XXIe siècle a vu également l'avènement d'un monde numérique. Et parler des droits humains, c'est parler de ce qui existe dans ce nouvel ordre public dans lequel les normes de l'État de droit doivent s'appliquer* »[1].

L'espace numérique ne doit pas échapper à un encadrement juridique strict. Il doit répondre à une protection équivalente aux principes fondamentaux qui régissent les autres sphères traditionnelles de l'Etat de droit. L'ampleur du défi posé par les nouvelles technologies n'aurait pas pû être anticipé par nos aînés, il y a de cela seulement 75 ans. Pourtant, bien qu'aujourd'hui les enjeux soient plus aisément mesurés, ces nouvelles technologies continuent de surprendre au détriment de la capacité à en prévenir efficacement les dérives. Si la rapidité du progrès complique son encadrement, l'Homme n'en demeure pas moins son instigateur. Après un court rappel des avancées diplomatiques et normatives depuis 2017 à l'échelle tant nationale qu'internationale, le président conclut son paragraphe par ces mots :

> « *Mais nous avons encore beaucoup à faire pour bâtir une véritable régulation en dur* »[2].

Il convient dès lors de s'interroger sur l'état véritable de la protection des droits de l'Homme au sein d'un environnement numérique en constante évolution, ainsi que sur la position de la diplomatie française au regard du numérique.

***

1. Présentation de l'étude.

Dans le cadre d'une collaboration entre la Clinique juridique de l'Université Paris Nanterre et la CNCDH, Cherifa JALLAD, étudiante en Master 2 Théorie et Pratique du droit international et européen, Alice FARACCI, étudiante en Master 2 Droit européen, ainsi que Laure BUISSONNIER, également inscrite en Master 2 Droit européen, avons participé au

[1] *Déclaration de M. Emmanuel Macron, président de la République, sur l'action de la France en faveur des droits de l'homme, à Paris*, Vie publique, 10 décembre 2023, Lien: https://www.vie-publique.fr/discours/292372-emmanuel-macron-10122023-droits-de-lhomme
[2] *Ibidem*

programme EUCLID. Notre groupe a travaillé en partenariat avec la sous-commission « Affaires internationales et européennes ». Notre participation consistait à prendre part aux travaux relatifs à la mise à jour de l'étude *Diplomatie et droits de l'homme*. L'actualisation de cette recherche portait plus spécifiquement sur l'aspect « Diplomatie numérique de la France ».

2. Définitions du « numérique », de la « diplomatie » et de la notion de « diplomatie numérique ».

Jean-François CERISIER, Professeur de l'Université de Poitiers au sein de l'unité de recherche Techné, définit le numérique comme « *un ensemble de techniques, d'équipements de logiciels de ressources, mais aussi d'usages, de pratiques, de comportements et de valeurs* »[3]. Marcello VITALI-ROSATI, Professeur de littérature et de culture numérique à l'Université de Montréal, insiste sur le fait que le « numérique » : « *ne se rapporte pas seulement à des outils informatiques ou des technologies, mais plutôt à des pratiques et des visions du monde qui engendrent des changements sociétaux profonds liés à l'utilisation d'internet* ». Depuis les années 2000, les modes de vie et les interactions ont été profondément modifiées par l'utilisation d'outils et de logiciels numériques. La diplomatie doit permettre d'accompagner ces transformations afin qu'elles s'inscrivent dans une dynamique éthique et respectueuse des droits fondamentaux.

La diplomatie est, quant à elle, définit comme la « *mise en œuvre de la politique étrangère d'un Etat* »[4]. Etymologiquement, le terme « diplomatie » tire son origine du grec ancien « διπλΪŒειν »[5], qui a donné le mot latin « *diploma* » signifiant « double », l'expression « diplomatie numérique » possède une double interprétation. Cette notion peut signifier à la fois « *l'impact du numérique sur les normes, les valeurs, les pratiques et les institutions diplomatiques* » et la « *gestion diplomatique des enjeux numériques et technologiques* ». Cette distinction a été mise en avant par Ilan Manor dans son blog *Exploring Digital Diplomacy*[6]. Elle souligne que la « diplomatie numérique » renvoie tant à

[3] Réseau Canopé, *Le numérique et l'évaluation : définitions*, Agence des usages TICE. Lien : https://www.reseau-canope.fr/fileadmin/user_upload/Projets/agence_des_usages/Evaluation_et_numerique/1_Le_numerique_et_l_evaluation__definitions.pdf (consulté le 25 mai 2025).
[4] *« Qu'est-ce que la diplomatie ? »*, Vie-publique, 16 septembre 2024. Lien : https://www.vie-publique.fr/fiches/269886-quest-ce-que-la-diplomatie
[5] DEPRET François, *« Les origines de la diplomatie »*, Le Monde, 31 décembre 1945. Lien : ttps://www.lemonde.fr/archives/article/1945/12/31/les-origines-de-la-diplomatie_1857157_1819218.html
[6] LYUBAREVA I. et NOCETTI J. (2024). *La diplomatie numérique Évolution des stratégies diplomatiques et d'influence à l'ère (du) numérique*. Réseaux, 245(3), 11-35. Lien :

l'influence du numérique sur la pratique diplomatique, notamment par l'utilisation des plateformes et réseaux sociaux en politique, qu'à l'activité diplomatique visant à instaurer des normes plus ou moins structurantes du numérique.

3. Champ de l'étude.

Le champ de cette étude se concentrera principalement sur l'action diplomatique menée par la France en matière de droits de l'Homme face aux enjeux soulevés par le numérique. Cependant, l'interdépendance des différentes acceptions de la diplomatie numérique, ainsi que l'usage qui en sont faits dans le monde, amèneront parfois à dépasser les limites du champ d'étude, sans pour autant en contredire les délimitations principales. Par ailleurs, cette étude portera essentiellement sur la décennie 2015 à 2025 afin de rester en phase avec l'actualité de ce sujet en mutation permanente.

4. Histoire.

L'ampleur du défi posé par les nouvelles technologies n'aurait pas pu être anticipé par nos aînés, il y a de cela seulement 75 ans. Afin de mieux appréhender la diplomatie numérique, il est important de comprendre le monde numérique et son évolution par l'étude de quelques dates clés en lien avec les droits de l'Homme.

---

https://doi-org.faraway.parisnanterre.fr/10.3917/res.245.0011

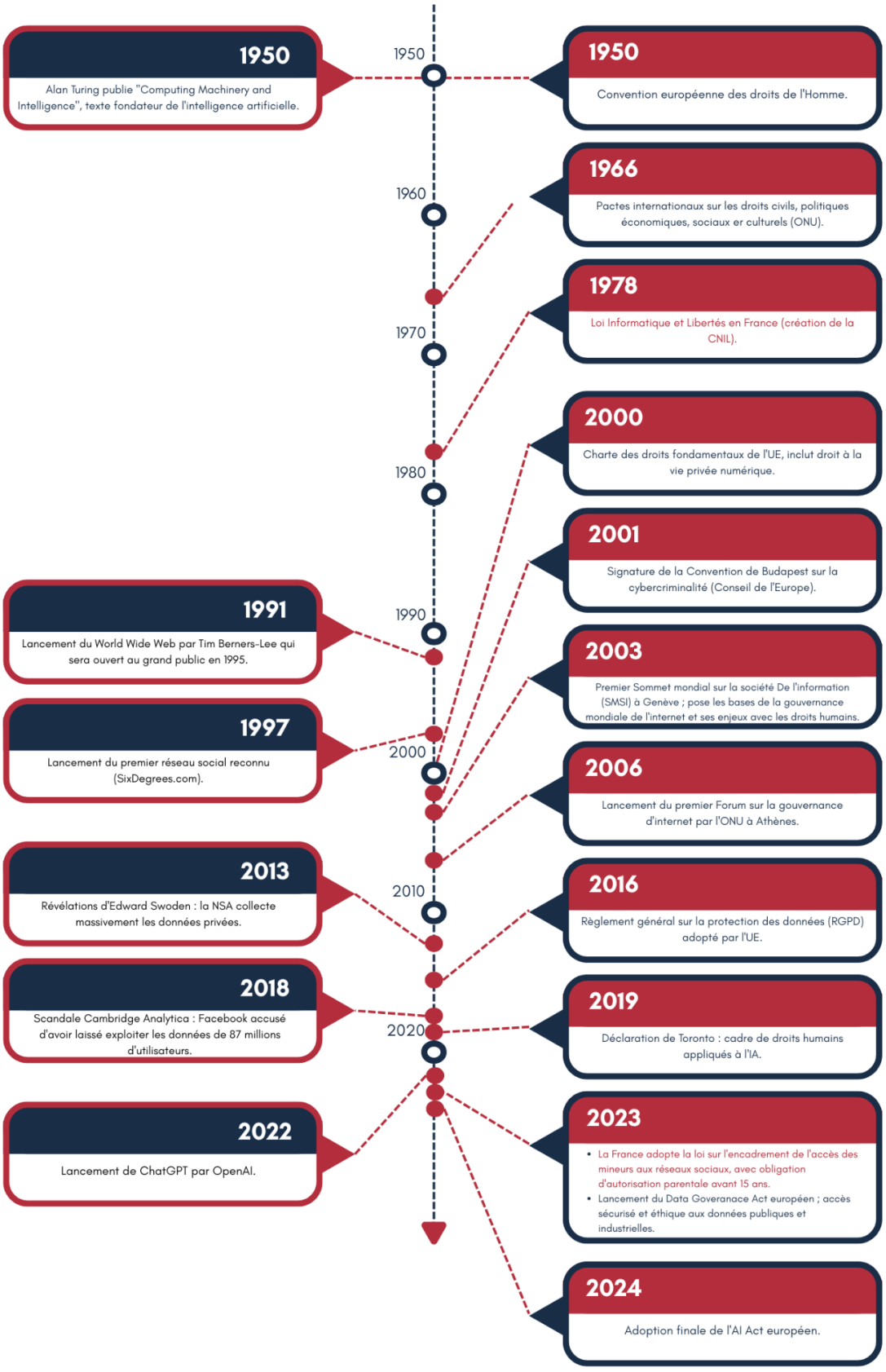

Illustration n°1 : Frise chronologique non exhaustive des dates clés d'internet et des avancées juridiques et diplomatiques en matière de droits de l'Homme.

5. Enjeux.

Le 14 février 2024, Volker TURK, Haut-Commissaire des Nations Unies aux droits de l'homme a invité l'auditoire de l'université de Stanford à réfléchir sur les dangers de posséder un pouvoir incontrôlé en s'appuyant sur le poème « L'apprenti sorcier » de GOETHE. Cette métaphore servait à rappeler qu'un immense pouvoir ne devrait être utilisé que lorsqu'il est maîtrisé. A ce sujet, Volker Türk affirme être « *convaincu que les droits de l'homme font partie intégrante de cette maîtrise et de la solution* »[7], notamment pour encadrer l'intelligence artificielle. Malgré de nombreux rapports du Haut-Commissariat des Nations Unies, le monde du numérique continue de progresser à un rythme effréné, souvent sans cadre réglementaire suffisant ni contrôle effectif, ce qui expose les sociétés à des risques majeurs tels que la violation des droits fondamentaux, la manipulation de l'information et des atteintes à la vie privée. La diplomatie numérique englobe diverses approches et peut s'incarner par plusieurs stratégies. La « *e-diplomatie, tech-diplomatie, cyberdiplomatie, ou encore réseau-diplomati*e »[8] sont autant de terminologies qui reflètent le besoin des pratiques diplomatiques de toujours s'adapter aux avancées technologiques contemporaines. Toutefois, la diplomatie numérique, traduite de « *digital diplomacy* »[9] dans la littérature anglo-saxonne, constitue une forme de diplomatie publique transnationale qui reste complètement nouvelle dans les relations internationales.

6. Méthodologie.

Afin d'appréhender les enjeux soulevés par ce sujet, cette étude s'appuie sur une démarche rigoureuse et pluridisciplinaire visant à analyser la diplomatie numérique de la France dans sa promotion et sa défense des droits de l'Homme. La méthodologie adoptée combine une analyse doctrinale, une étude critique des documents officiels et une évaluation des pratiques concrètes à travers des exemples récents. Une première phase documentaire a permis d'identifier les fondements juridiques et les orientations stratégiques de la diplomatie numérique français en matière de droits de l'Homme. Parallèlement, une analyse comparative a été réalisée afin de situer la posture française dans un contexte international, en confrontant

[7] TÜRK Volker, *« Human rights must be at the core of generative AI technologies »*, discours prononcé à l'Université de Stanford, États-Unis, 14 février 2024. Lien : https://www.ohchr.org/fr/statements-and-speeches/2024/02/human-rights-must-be-core-generative-ai-technologies-says-turk

[8] *Op. cit.* n°6, p. 7

[9] HOUGUET Adrien, JOSSET Benoît, *« Vers une diplomatie numérique transnationale »,* Questions de communication, 2023, 44, pp.155-182. Lien : https://journals.openedition.org/questionsdecommunication/pdf/33083

ses engagements et pratiques avec ceux d'autres acteurs étatiques majeurs. Enfin, des entretiens ont été menés par la CNCDH avec des professionnels issus des sphères diplomatiques, juridiques et technologiques. Ces échanges ont permis de recueillir des analyses et des retours d'expérience concrets, nous permettant d'obtenir une meilleure perspective opérationnelle et actualisée des questions étudiées.

7. Intérêt de l'étude.

Jean-Yves Le Drian, ancien ministre de l'Europe et des Affaires étrangères, a souligné l'importance de la souveraineté numérique et de la protection des droits de l'Homme en ligne lors de plusieurs déclarations. Le 11 novembre 2021[10], il a notamment salué la décision des Etats-Unis de soutenir l'*Appel de Paris pour la confiance et la sécurité dans le cyberespace*, qui vise à établir des principes communs pour protéger les droits des personnes et renforcer les normes internationales. La position de la France illustre son engagement à promouvoir un cadre réglementaire plus ferme afin de garantir que les droits fondamentaux soient respectés dans l'espace numérique. Pourtant, la CNCDH a rappelé en janvier 2022, le besoin impératif d'une « *cohérence des autorités françaises entre la politique étrangère et la politique interne* »[11] et que la France « *s'engage juridiquement en faveur des droits de l'Homme sur le plan international* »[12] afin de traduire concrètement ces engagements dans sa législation interne et en pratique. Ce sujet, croisant diplomatie et enjeux technologiques contemporains au regard du respect des droits de L'Homme, met en lumière une dimension encore peu étudiée de l'action extérieure française, en croisant la diplomatie avec les enjeux technologiques contemporains. Elle interroge en particulier la cohérence de l'engagement international et européen de la France en faveur des droits de l'Homme à l'ère du numérique.

8. Choix des thèmes.

Une série de thèmes sera développée au sein de cette étude. Cependant, l'ensemble de la diplomatie du numérique ne pourrait pas être résumée dans cette étude. Elle ne prétend pas à l'exhaustivité et ne saurait à elle seule résumer l'ensemble des enjeux portés par la diplomatie du numérique en France. Il s'agit d'un choix conscient qui répond à une volonté

[10] LE DRIAN Jean-Yves, *Discours sur le cyberespace*, 11 novembre 2021. Lien : https://www.vie-publique.fr/discours/282457-jean-yves-le-drian-11112021-cyberespace
[11] *Avis sur la diplomatie française et les droits de l'homme*, CNCDH, 20 octobre 2022. Lien : https://www.cncdh.fr/publications/avis-sur-la-diplomatie-francaise-et-les-droits-de-lhomme
[12] *Ibidem*.

de circonscrire le propos à des enjeux immédiatement structurants dans les rapports de force technologiques actuels.

Parmi les thématiques non développées, la question des politiques culturelles à l'ère numérique aurait pu s'inscrire dans cette étude puisqu'elle aborde le droit de propriété intellectuelle. Par ailleurs, les enjeux liés à l'usage du numérique dans les processus de recrutement et les pratiques des entreprises soulèvent des problématiques de discrimination algorithmique et de transparence. Ces thématiques, qui ont une incidence sur les droits fondamentaux, mériteraient une étude complémentaire. De même, la situation des travailleurs de plateformes numériques, souvent soumis à des formes d'emploi précaires, constitue une question sociale et politique majeure à l'échelle nationale comme internationale. En outre, les interactions entre écologie et numérique sont souvent reléguées au second plan mais doivent être prises en compte dans toutes les réflexions à long terme. Elles interrogent la durabilité et la viabilité de notre modèle technologique face à l'urgence climatique. Concernant le secteur de l'éducation, les plateformes algorithmiques, comme celle de Parcoursup, ont suscité de nombreuses inquiétudes quant au respect des droits de l'Homme. Enfin, les débats sur les crypto actifs et la cryptomonnaie dans l'économie mondiale ont soulevé de nouvelles problématiques liées à la souveraineté monétaire, la sécurité financière et la régulation des échanges numériques à l'échelle globale. Ces enjeux, bien qu'économiques en apparence, soulèvent également des questions fondamentales au regard de la CEDH, notamment en ce qui concerne la protection du droit de propriété inscrit à l'article 1 du *Protocole n°1*. Une autre thématique très présente dans le quotidien de nos jours concerne les éléments techniques des appareils électroniques, à savoir les matières premières. Pour les téléphones portables, ordinateurs ou autres appareils, l'origine des batteries, le *sourcing* est souvent problématique. En effet, certaines matières premières qui composent ces appareils sont souvent issues de l'exploitation de personnes vulnérables, souvent d'enfants ou de personnes sous-payés. L'exploitation des personnes vulnérables est également utilisée dans le cadre de la consommation de masse facilitée par la rapidité des plateformes, accrue par le développement des technologies.

Ces sujets, bien qu'en lien avec la diplomatie numérique de la France et le respect des droits de l'Homme, ne seront pas traités dans cette étude.

9. Problématique.

La problématique qui guidera l'étude est donc la suivante :

Quelle place les droits de l'Homme occupent-ils dans la diplomatie numérique de la France, et dans quelle mesure cette diplomatie reflète-t-elle les droits de l'Homme que la France prétend promouvoir sur la scène internationale et européenne ?

10. Annonce de plan.

La diplomatie du numérique de la France doit s'inscrire dans le respect des cadres juridiques internationaux et européen existants relatifs au numérique et aux nouvelles technologies, tout en adoptant une approche cohérente, proactive et éthique face aux enjeux liés au numérique (PARTIE I). Des instruments juridiques internationaux (Chapitre I) mais également européens, tant de droit de l'Union européenne que du Conseil de l'Europe (Chapitre II) viennent ainsi encadrer l'intelligence artificielle, s'attaquer à la cybercriminalité et garantir la liberté d'expression en ligne mais également protéger les enfants dans l'environnement numérique.

Ces différentes thématiques sont au cœur de la diplomatie numérique active menée par la France (PARTIE II). Cette action diplomatie entend promouvoir les droits de de l'Homme dans l'univers numérique, avec une attention particulière au développement d'une IA responsable (Chapitre I), à la sécurité du cyberespace et la promotion et la protection de la liberté d'expression (Chapitre II) ainsi que des droits de l'enfant en ligne (Chapitre III). Dans un environnement en constante évolution, où des risques nouveaux défis émergent, la France doit formuler des réponses juridiques et politiques adaptées, conformes aux droits de l'Homme.

PARTIE I. LE CONTEXTE DU DÉPLOIEMENT DE LA DIPLOMATIE NUMÉRIQUE DE LA FRANCE

La diplomatie française ne saurait être menée sans une mise en perspective globale. La position de la France ne peut être pleinement comprise qu'à la lumière des dynamiques juridiques et politiques qui structurent son environnement international et européen. En effet, la diplomatie numérique française s'inscrit dans un cadre juridique vaste, influencé à la fois par les initiatives multilatérales à l'échelle internationale et par les orientations stratégiques de l'Union européenne. La France insère son action diplomatique dans un contexte qui révèle sa volonté d'affirmer et de promouvoir une vision humaniste et équilibrée de l'espace numérique au niveau international (Chapitre I). A l'échelle européenne, la France opte pour une position engagée dans la construction d'un cadre juridique commun capable de répondre aux défis posés par les nouvelles technologies (Chapitre II).

Chapitre I. La France et la diplomatie numérique au niveau international

Le droit international des droits de l'Homme et ses principes s'appliquent aux États qui y ont consenti, notamment par la ratification des instruments internationaux pertinents. Son application repose sur le principe du consentement des États. Cependant, certains droits considérés comme relevant du droit international coutumier ou des droits indérogeables s'imposent indépendamment d'une ratification formelle. La protection des droits de l'Homme par le droit international est primordiale. Dans le cadre du numérique, le cadre juridique international de manière générale et de manière sectorielle est conséquent, bien qu'éclaté (I), et appelle la France à se positionner de manière claire et sans équivoque, voire d'aller plus loin que les instruments juridiques internationaux (II).

I. Le cadre juridique international

Après avoir posé le cadre juridique global, il convient de s'intéresser au cadre international relatif au domaine de l'IA (A), relatif à la cybercriminalité, notamment la lutte contre le terrorisme en ligne et relatif à la protection de la liberté d'expression, lutte contre la désinformation (B) puis relatif à la protection des droits de l'enfance (C).

Sur le cadre juridique international global

Les instruments du droit international des droits de l'Homme sont nombreux et la France a ratifié nombre d'entre eux (voir le tableau à l'annexe 1). Son engagement dans la protection et la promotion des droits de l'Homme est notable.

En matière de protection et promotion des droits de l'Homme à l'ère du numérique, le cadre juridique est éclaté. Toutefois, le droit international ne cesse de chercher à réglementer face aux nouvelles technologies, et surtout en appliquant les principes du droit international des droits de l'Homme. Bien que plusieurs instruments internationaux existent, ils sont souvent sectoriels. Dès lors, afin d'atteindre une meilleure gouvernance, une convention internationale serait utile afin de protéger au mieux les droits de l'Homme dans l'environnement numérique. C'est pourquoi un Pacte international est envisagé.

Le *Pacte numérique mondial*[13] constitue ainsi une initiative ambitieuse de l'ONU, ancrée dans le droit international des droits de l'Homme, visant à encadrer le développement numérique dans le respect des droits de l'Homme. Il a pour objectif de garantir un accès équitable à Internet et aux technologies numériques pour toutes et tous, quel que soit le statut socio-économique et dans l'ensemble des Etats. Il promeut en effet un espace numérique inclusif, ouvert, sûr et sécurisé où les droits civils, politiques, économiques, sociaux et culturels sont pleinement respectés, en ligne comme hors ligne. C'est le troisième des cinq objectifs :

« Objectif 3. Favoriser un espace numérique inclusif, ouvert, sûr et sécurisé qui respecte, protège et promeut les droits humains. [14] *» .*

En plus d'être écrit comme un objectif, il est présenté comme un principe, afin d'affirmer l'importance de l'inclusion numérique, luttant contre les fractures existantes. Parallèlement, il a pour objectif d'assurer la protection des droits de l'Homme, tels que la liberté d'expression et le respect de la vie privée, notamment en ce qui concerne l'utilisation des données personnelles. Toutefois, l'accent est mis sur la protection des droits des enfants, des personnes handicapés, l'égalité de genre et l'autonomisation des femmes et des filles :

[13] *Pacte pour l'avenir, « Pacte numérique mondial », Projet de résolution déposé par le Président de l'Assemblée générale*, A/79/L.2, 20 septembre 2024

[14] *Ibidem* p.45

« c) Le présent Pacte est ancré dans le droit international, en particulier le droit international des droits de l'homme. Tous les droits humains, notamment les droits civils, politiques, économiques, sociaux et culturels, et toutes les libertés fondamentales ***doivent être respectés, protégés et promus en ligne et hors ligne****. La coopération que nous entendons mettre en place tirera parti des technologies numériques pour faire progresser tous les droits humains, y compris* ***les droits de l'enfant, les droits des personnes handicapées et le droit au développement*** *;*

d) L'égalité des genres et l'autonomisation de toutes les femmes et les filles, ainsi que leur participation pleine, égale et réelle à l'espace numérique, sont essentielles pour ***combler le fossé numérique entre les genres et faire progresser le développement durable****. La coopération que nous entendons mettre en place œuvrera à l'autonomisation de toutes les femmes et les filles, promouvra le leadership des femmes, favorisera la prise en compte systématique des questions de genre et permettra de combattre et d'éliminer toutes les formes de violence, y compris les violences sexuelles et fondées sur le genre,* ***ainsi que les violences permises ou amplifiées par l'usage de la technologie*** » [15].

Le Pacte appelle à une action collective impliquant les États, la société civile mais aussi les entreprises qui doivent impérativement respecter les droit de l'Homme :

« 25. Nous demandons : a) ***aux entreprises du numérique et aux développeurs de se conformer au droit international des droits de l'Homme*** *et aux principes qui y sont énoncés, notamment en appliquant des mesures de diligence raisonnable en matière de droits de l'homme et en procédant à des études d'impact tout au long du cycle de vie des technologies (tous les ODD) ;*

b) aux entreprises du numérique, aux développeurs et aux plateformes de médias sociaux ***d'assurer le respect des droits humains dans le cyberespace****, de répondre de l'action qu'ils mènent à cet égard, de prendre des mesures visant à atténuer et à prévenir les atteintes à ces droits et d'offrir de véritables voies de recours conformément aux Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme et aux autres textes applicables (ODD 5, 10 et 16).*[16] ».

[15] *Ibid*, n°14, p 14, p.45
[16] *Ibid.* n°14, p 14, p.51

La coopération internationale, notamment à travers des partenariats comme celui signé avec la Ligue des États arabes (LEA), vise à promouvoir une économie numérique inclusive et durable. En effet, un *mémorandum* d'entente a été signé avec la LEA pour favoriser le développement économique à travers la transformation numérique.

Par ailleurs, le Pacte se veut intemporel, car son champ d'application temporel ne se restreint pas aux technologies existantes mais aussi à celles à venir :

> *« 22. Nous sommes déterminés à respecter, protéger et promouvoir les droits humains dans l'espace numérique. Nous entendons faire appliquer le droit international des droits de l'homme* ***tout au long du cycle de vie des technologies numériques et émergentes*** *afin que les utilisateurs et utilisatrices puissent profiter en toute sécurité des technologies numériques et soient protégés contre toute violation de leurs droits, toute atteinte à leurs droits et toute forme de discrimination. Nous estimons qu'il incombe à toutes les parties prenantes de participer à cette entreprise et demandons au secteur privé d'appliquer les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme.*[17] *»*

Par ailleurs, l'UE a l'intention d'imposer ses règles numériques afin que les standards européens deviennent les normes internationales. En effet, la Commission européenne a pour ambition de devenir la référence mondiale en matière de politique numérique. Le RGPD, par exemple, a influencé des législations du monde entier, telles que le Brésil et l'Inde.

A) <u>Le cadre international relatif au domaine de l'IA</u>

Depuis 2011, les *principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'Homme* fournissent les bases d'un développement plus responsable de l'IA. Le projet B-Tech[18] du HCDH a produit une série de recommandations, d'outils et d'orientations. Par ailleurs, adoptée en 2018, la *Déclaration de Toronto sur la protection des droits à l'égalité et à la non-discrimination dans les systèmes d'apprentissage automatique* constitue une référence essentielle. Elle appelle les Etats, les entreprises et les développeurs d'IA à garantir que les technologies automatisées soient conçues, déployées et régulées de manière à

[17] *Ibid*, n°14 p.14, p.51
[18] HCDH, *Projet B-Tech : technologies, droits de l'homme et entreprises*, 2021. Lien : https://www.ohchr.org/fr/business/b-tech-project

prévenir les atteintes aux droits fondamentaux,en ciblant en particulier les groupes les plus vulnérables. Son préambule établit clairement son objectif :

> *« Avec l'essor, en termes de capacités et d'utilisation, des systèmes reposant sur l'apprentissage automatique, il devient nécessaire d'étudier les incidences de cette technologie sur les droits humains. Nous reconnaissons que l'apprentissage automatique et les systèmes connexes peuvent servir à promouvoir les droits humains, mais nous sommes de plus en plus préoccupés par le fait que ces systèmes pourraient potentiellement favoriser la discrimination, intentionnelle ou non, à l'égard de certaines personnes ou certains groupes de personnes »*[19].

Cette déclaration invite aussi les acteurs du numérique à éviter d'utiliser des systèmes dit de « boîte noire » car ils ne peuvent pas être soumis à des normes satisfaisantes en matière de reddition de comptes et de transparence, et même de s'abstenir d'utiliser de tels systèmes dans des contextes où les risques sont élevés. Si ce document vise à promouvoir des principes plus éthiques et clairs d'utilisation de l'IA, il ne constitue pas un instrument juridique soumis à ratification nationale. Il s'agit d'un texte normatif rédigé par la société civile. En outre, la France figure également parmi les pays ayant adhéré aux *Principes de l'Organisation de coopération et de développement économiques (OCDE) sur l'IA*. Adoptés en 2019, ces principes respectent les droits de l'Homme et les valeurs démocratiques. Ils se déclinent en cinq axes fondés sur des valeurs et cinq recommandations qui fournissent des orientations pratiques et flexibles aux décideurs politiques et aux acteurs de l'IA.

B) <u>Le cadre international relatif à la cybercriminalité, dont le terrorisme en ligne et à la liberté d'expression, notamment la lutte contre la désinformation</u>

L'utilisation d'internet à des fins criminelles représente un défi majeur dans la société actuelle. La cybercriminalité, qui peut être définie comme l'*« ensemble des infractions pénales qui sont commises dans le cyberespace »*[20], regroupe plusieurs infractions : celles intrinsèquement liées aux nouvelles technologies (diffusion de virus, piratage, copie illicite de logiciels ou d'œuvres audiovisuelles …) et celles pour lesquelles le cyberespace n'est

---

[19] *Préambule, Déclaration de Toronto sur la protection des droits à l'égalité et à la non-discrimination dans les systèmes d'apprentissage automatique*, 2018

[20] ANSSI, Glossaire. Lien : https://cyber.gouv.fr/glossaire#:~:text=Cyberattaque%2C%20n.f.,intégrité%20ou%20à%20leur%20confidentialité.

qu'un nouveau lieu d'expression et vecteur de transmission (apologie du racisme, diffusion de contenus pédophiles, harcèlement …).

Cette cybercriminalité peut notamment prendre la forme de cyberattaques, c'est à dire *« d'actions menées dans le cyberespace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité »*[21], dont le niveau de sophistication et d'intensité est en constante augmentation. La cybercriminalité représente une menace au niveau national, mais également plus globalement pour la sécurité internationale, nécessitant ainsi une coopération internationale et des actions coordonnées. En effet, la cybercriminalité a pris une ampleur considérable à l'échelle internationale avec le développement des technologies numériques, rendant les attaques plus fréquentes, complexes et difficiles à contrer. La cyberdéfense, c'est à dire l'*« ensemble des moyens mis en place par un État pour défendre dans le cyberespace les systèmes d'information jugés d'importance vitale, qui contribuent à assurer la cybersécurité »*[22] fait ainsi partie de la diplomatie numérique des Etats, notamment de la France, en vue d'assurer la sécurité du cyberespace, des infrastructures et des citoyens.

Au niveau international, la France a notamment ratifié les deux conventions majeures visant à encadrer la cybercriminalité. La première, intitulée *Convention sur la cybercriminalité* du Conseil de l'Europe, dite *Convention de Budapest*[23], a été adoptée en 2001 et ratifiée par 76 Etats, dont la France. Cette Convention fournit des orientations concernant les mesures législatives nationales à prendre en matière de cybercriminalité (relatives aux infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques ; aux infractions informatiques ; aux infractions se rapportant au contenu ; aux infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes) et sert de base à la coopération internationale dans le domaine pénal entre les États parties (en matière d'extradition, d'entraide aux fins d'investigations ou de procédures concernant les infractions liées à des systèmes et à des données informatiques, de recueil des preuves sous forme électronique d'une infraction pénale), et ce dans l'objectif de lutter contre les crimes ne pouvant être commis que par l'utilisation de la technologie. Deux *protocoles additionnels* sont venus compléter cette Convention : le premier relatif à l'incrimination d'actes de nature

[21] *Ibidem*
[22] *Ibid.* , p.17
[23] *Convention sur la cybercriminalité*, Conseil de l'Europe, 23 novembre 2001

raciste et xénophobe commis par le biais de systèmes informatiques[24] adopté en 2003 et entré en vigueur en 2006, et le deuxième relatif au renforcement de la coopération et de la divulgation de preuves électroniques[25], adopté en 2023, qui n'est pas encore en vigueur.

Une nouvelle *Convention des Nations Unies contre la cybercriminalité*[26], dont la Russie a été à l'origine des négociations, a été adoptée par consensus fin 2024[27], dans un contexte d'explosion de l'utilisation des nouvelles technologies à des fins criminelles. Cette Convention est le premier traité international qui encadre la criminalité en ligne, notamment la pornographie infantile, l'atteinte au droit d'auteur et les discours de haine, visant ainsi à renforcer la coopération internationale pour la lutte contre certaines infractions commises au moyen de systèmes d'information et de communication et en matière de partage de preuves électroniques concernant les infractions graves. Elle reconnait notamment la nécessité de *« mener, à titre prioritaire, une politique de justice pénale mondiale destinée à protéger la société de la cybercriminalité, notamment par l'adoption d'une législation appropriée, l'établissement d'infractions communes, l'instauration de pouvoirs procéduraux communs et la promotion de la coopération internationale afin de prévenir et de combattre ces activités plus efficacement aux niveau national, régional et international ».* Cette Convention prévoit également l'assistance technique et le renforcement des capacités au profit des pays en développement dans le but de prévenir et combattre la cybercriminalité. Au regard de son périmètre large, notamment le fait qu'elle prévoit qu'un Etat peut demander aux autorités d'un autre Etat toute preuve électronique liée à un cyber-crime, mais également réclamer des données à un fournisseur d'accès en vue d'enquêter sur tout crime passible de minimum quatre ans d'emprisonnement dans sa loi nationale, la société civile et des entreprises du numérique ont émis des préoccupations quant à la possibilité que celle-ci soit utilisée comme un outil de surveillance par certains Etats.

Les technologies numériques ont profondément transformé la manière de se renseigner et de s'informer, les réseaux sociaux étant devenus l'une des principales sources

---

[24] *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques* (STE N°289), 2003

[25] *Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électronique*s (STCE n°224), 2023

[26] *Convention des Nations Unies contre la cybercriminalité*, 24 décembre 2024

[27] *Résolution A/RES/79/243*, *Convention des Nations Unies contre la cybercriminalité ; Renforcement de la coopération internationale pour la lutte contre certaines infractions commises au moyen de systèmes d'information et de communication et pour la communication de preuves sous forme électronique d'infractions graves,* Assemblée générale des Nations Unies, 31 décembre 2024

d'information. Selon une étude menée par Eurobaromètre, 42 % des jeunes Européens utilisent les réseaux sociaux comme principale source d'information sur les questions politiques et sociales[28]. Cette évolution soulève des enjeux majeurs, notamment celui de la désinformation, qui constitue aujourd'hui l'un des principaux risques liés à l'utilisation d'Internet. Cette diffusion rapide de fausses informations peut influencer l'opinion publique, fragiliser les démocraties et porter atteinte aux droits fondamentaux, en particulier au droit à l'information, garanti par l'*article 19 du PIDCP* qui consacre le droit de tout individu à la liberté d'opinion et d'expression. Dans cette optique, garantir un environnement numérique sûr, fiable et ouvert est une priorité, les questions de régulation des plateformes numériques et de lutte contre la désinformation occupant désormais une place centrale au sein des instances internationales.

L'Assemblée générale des Nations Unies et le Conseil des droits de l'Homme (CDH), principal organe intergouvernemental des Nations Unies traitant de la question des droits de l'Homme dont la France fait partie des Etats membres (mandat 2024-2026), ont tous deux appelés à remédier à la désinformation, afin de promouvoir et protéger la liberté d'expression des individus et à la liberté de rechercher, de recevoir et de répandre des informations. Dans une *résolution* « *combattre la désinformation pour promouvoir et protéger les droits humains et les libertés fondamentales* »[29] de 2021, l'Assemblée générale des Nations Unies a notemment souligné que « *la désinformation, sous toutes ses formes, peut nuire à l'exercice des droits humains et des libertés fondamentales, ainsi qu'à la réalisation des objectifs de développement durable* » et « *engage les États à lutter contre la désinformation sous toutes ses formes par des mesures de politique générale, y compris l'éducation, l'augmentation des moyens de prévenir la désinformation et d'y résister, et les activités d'information et de sensibilisation* ». De plus, cette résolution s'adresse aux plateformes en ligne, leur demandant d'adopter et de rendre publiques des politiques claires, transparentes et étroitement définies en matière de contenu et de publicité qui soient conformes au droit international des droits de l'Homme. Cette résolution a par ailleurs soutenu l'appel du Secrétaire général des Nations Unies en vue de l'adoption d'un « code de conduite mondial visant à promouvoir l'intégrité de l'information publique ».

---

[28] *Les réseaux sociaux, principale source d'information des jeunes Européens*, Toute l'Europe, 20 février 2025. Lien : https://www.touteleurope.eu/societe/podcast-les-reseaux-sociaux-principale-source-d-information-des-jeunes-europeens/

[29] *Résolution A/RES/76/227, Combattre la désinformation pour promouvoir et protéger les droits humains et les libertés fondamentales*, Assemblée générale des Nations Unies, 24 décembre 2021

A la suite d'une demande formulée dans cette résolution, un *rapport sur la lutte contre la désinformation*[30] a été publié par le Secrétaire général des Nations Unies en août 2022. Ce rapport présente des propositions aux Etats mais également aux entreprises technologiques afin de lutter contre la désinformation. Au niveau des Etats, le rapport met en avant la nécessité de protéger, respecter et promouvoir la liberté d'expression, en garantissant l'accès à l'information et en promouvant le pluralisme des médias ; d'éviter de réglementer sur la base de définitions vagues, d'imposer des sanctions disproportionnées et ne jamais criminaliser les contenus légitimes ; de s'abstenir des coupures d'Internet, du blocage des sites Web et des sources d'information ; de s'assurer que les agents publics partagent des informations exactes et tiennent responsables les autorités qui diffusent de fausses informations et d'impliquer la société civile dans la conception des politiques et autres efforts visant à lutter contre la désinformation. Il est par ailleurs demandé aux entreprises technologiques d'éviter d'avoir des incidences négatives sur les droits de l'Homme, et de remédier aux incidences dans lesquelles elles sont impliquées ; de rendre publiques les politiques et pratiques pertinentes pour lutter contre la désinformation ; de revoir leurs modèles de gestion pour s'assurer qu'ils sont conformes aux principes des droits de l'Homme ; d'assurer une plus grande transparence et donner accès aux données et informations pertinentes et finalement de s'assurer que leurs pratiques de modération de contenu sont cohérentes et disposent de ressources suffisantes dans tous les lieux où ils opèrent et dans toutes les langues pertinentes.

Le projet *Réseaux sociaux pour la paix* est une autre initiative de lutte contre la désinformation et les discours de haine à l'échelle mondiale. Issu d'un partenariat entre l'UNESCO et l'Union européenne, ce projet, lancé en 2021 avec une contribution de 4 millions d'euros de l'Union européenne, vise à renforcer la résilience des sociétés face aux contenus potentiellement néfastes diffusés en ligne, en particulier les discours de haine incitant à la violence, tout en protégeant la liberté d'expression et en renforçant la promotion de la paix grâce aux technologies numériques, notamment les réseaux sociaux. Ce projet, d'abord mis en œuvre dans trois pays pilotes : la Bosnie Herzégovine, l'Indonésie et le Kenya, a été étendu en 2025 à l'Irak, le Kirghizistan et l'Afrique du Sud. L'UNESCO mène dans ces pays diverses actions et initiatives, en surveillant notamment le contexte de diffusion, les causes profondes, les intentions et les effets sur les personnes et leur comportement des contenus néfastes, en établissant une cartographie des instruments

[30] *Rapport du Secrétaire général des Nations Unies, Combattre la désinformation pour promouvoir et protéger les droits humains et les libertés fondamentales*, A/77/287, 12 août 2022

juridiques et des outils développés par les autorités nationales et les plateformes de réseaux sociaux pour remédier à la désinformation ou encore en créant une plateforme nationale multipartite (composée d'entreprises, de chercheurs et d'organisations de la société civile) pour définir les écarts entre les réalités et les mesures prises par les différentes parties prenantes pour lutter contre les contenus néfastes en ligne. L'UNESCO rédige une évaluation préliminaire des risques par pays, fondée sur les clivages sociétaux et politiques, ainsi que des recommandations visant à accroître l'efficacité des mesures et des outils de lutte, ainsi qu'à prévenir les conflits et l'instabilité. L'objectif de ce projet est également d'améliorer la lutte contre les contenus potentiellement néfastes en ligne, en développant de nouveaux outils, en renforçant les capacités des parties prenantes (autorités, judiciaire, entreprises du numérique et organisations de la société civile) afin d'améliorer les pratiques de modération de contenu, en améliorant l'accès au recours pour les utilisateurs de réseaux sociaux ou encore en informant la communauté mondiale des enseignements tirés du projet. L'UNESCO organise par ailleurs des formations, des campagnes de sensibilisation en ligne afin de promouvoir et soutenir les discours de paix dans ces pays.

La protection de la liberté d'expression en ligne passe également par la protection des défenseurs des droits de l'Homme et des journalistes en ligne. Lors de la 58e session du CDH, une *résolution sur les défenseurs des droits de l'Homme et les technologies nouvelles et émergentes*[31] a notamment été adoptée par consensus. Cette résolution a pour objectif de protéger les défenseurs et défenseuses des droits de l'Homme à l'ère numérique, en assurant un environnement sûr, ouvert et respectueux des droits de l'Homme, en ligne comme hors ligne. Elle enjoint aux Etats de prendre plusieurs mesures afin d'assurer leur protection, notamment : de renoncer à l'usage ou au transfert de technologies nouvelles ou émergentes comme les logiciels espions ou l'IA qui menacent ou sont incompatibles avec les droits de l'Homme ; d'encourager la transparence de l'information publique ; de favoriser un Internet ouvert, accessible, sécurisé, en particulier lors de crises, conflits ou élections ; de ne pas criminaliser, stigmatiser, harceler ou diffamer les défenseurs, y compris ceux en lien avec des acteurs non étatiques ; d'interdire les coupures d'Internet, le filtrage de contenu, les restrictions injustifiées ou encore d'encadrer strictement les technologies de reconnaissance biométrique comme la reconnaissance faciale. Bien que cette résolution n'ait pas de force contraignante, elle établit des lignes directrices concrètes et appelle à la responsabilité des

[31] *Résolution 58/23, Défenseurs des droits humains et technologies nouvelles et émergentes : protéger les défenseurs et défenseuses des droits humains à l'ère numérique*, Conseil des droits de l'Homme, 28 mars 2025

États et des entreprises pour garantir un espace numérique respectueux des droits fondamentaux, notamment du plein exercice de la liberté d'expression.

C) Le cadre international relatif à la protection des droits de l'enfant

Le droit international des droits de l'Homme constitue le fondement essentiel pour la protection des droits de l'enfant, notamment à travers des instruments tels que la *Convention internationale des droits de l'enfant (CIDE)*. Cette Convention, qui constitue le principal instrument international protégeant les droits de l'enfant, a été adoptée par l'Assemblée générale des Nations Unies le 20 novembre 1989 et est actuellement ratifiée par 197 Etats. La France a signé cette Convention le 26 janvier 1990 et le Parlement, par une loi du 2 juillet 1990, en a autorisé sa ratification, intervenue le 7 août 1990.

En 2021, le Comité des droits de l'enfant - organe composé d'experts indépendants chargé de surveiller la mise en œuvre de la *CIDE* par les États parties - a adopté une *observation générale sur les droits de l'enfant en relation avec l'environnement numérique*[32], qui reconnaît pour la première fois que les droits de l'enfant s'appliquent à la fois hors ligne et en ligne. Il s'agit d'un document directeur sur les droits des enfants en relation avec l'environnement numérique, qui inscrit les droits des enfants en ligne dans le cadre plus large de la *CIDE*. L'interprétation de la *CIDE* est alors actualisée et inclut désormais Internet et les avancées technologiques. Elle vise à guider les États parties dans la mise en œuvre de la *CIDE* dans le contexte de l'environnement numérique, en leur fournissant des orientations claires sur les lois, politiques et autres actions à adopter pour garantir le respect intégral de leurs obligations conventionnelles. Les Etats signataires sont donc tenus de respecter cette convention, et pourront être tenus responsables de manquements à celle-ci par le Comité des droits de l'enfant le cas échéant. Enfin, l'*observation générale* fait la synthèse des rapports des Etats, de la jurisprudence mais aussi de la consultation d'enfants lors d'ateliers participatifs avec 709 enfants vivant dans des zones urbaines et rurales de 28 pays. Durant deux ans de consultations, en plus des enfants, ont participé des Etats, des organisations intergouvernementales, des institutions nationales des droits de l'homme, la société civile. En effet, en mars 2019, le Comité a invité toutes les parties intéressées à formuler des observations sur la note conceptuelle de l'observation générale et a reçu 136 contributions à

[32] *Observation générale n°25 sur les droits de l'enfant en relation avec l'environnement numérique*, Comité des droits de l'enfant, CRC/C/GC/25, 2 mars 2021

ce sujet. La France ne fait cependant pas partie des 28 Etats contributeurs, dont des Etats européens, et n'a été représentée qu'à travers les contributions du Conseil de l'Europe et de l'UE.

De surcroit, un r*apport de la Rapporteuse spéciale sur le droit à l'éducation*[33], adoptée en octobre 2024, est venu souligner l'obligation des États parties de mettre en œuvre la *CIDE* en tenant compte des spécificités du monde numérique. Le rapport insiste sur la nécessité d'adapter les législations nationales pour garantir la vie privée, la sécurité et la dignité des enfants en ligne, tout en régulant les responsabilités des entreprises technologiques. Bien que non contraignant juridiquement, ce rapport reflète un consensus international fort et s'appuie sur l'*Observation générale n°25 du Comité des droits de l'enfant*[34], offrant ainsi une orientation normative en vue de renforcer la protection des enfants face aux défis du numérique.

Concernant l'accessibilité de tous les enfants à Internet, l'*observation générale* souligne que les États doivent lutter contre les inégalités d'accès au numérique :

> *«Le droit de ne pas faire l'objet de discrimination exige des États qu'ils veillent à ce que tous les enfants aient un* ***accès égal, effectif et satisfaisant à l'environnement numérique****. Les États parties devraient prendre toutes les mesures nécessaires pour* ***venir à bout de l'exclusion numérique****.*[35]*»*

L'intérêt supérieur de l'enfant est également un principe défendu par l'*observation générale* :

> *« les États parties doivent veiller à ce que, dans toutes les décisions concernant la fourniture, la réglementation, la conception, la gestion et l'utilisation de l'environnement numérique,* ***l'intérêt supérieur de chaque enfant soit une considération primordiale*** *»*[36]

Par ailleurs, une *résolution* concernant les droits de l'enfant[37] a été adoptée par le Conseil des droits de l'homme (CDH) afin de mettre en lumière les risques accrus d'exploitation sexuelle

[33] *Rapport de la Rapporteuse spéciale sur le droit à l'éducation,* A/79/520, 16 octobre 2024
[34] *Op. cit.*, n°31, p. 22
[35] *Ibidem*
[36] *Ibidem*
[37] *Résolution 31/7, les technologies de l'information et de la communication et l'exploitation sexuelle des enfants*, Conseil des droits de l'Homme, 23 mars 2016

des enfants liés à l'utilisation des technologies de l'information et de la communication. La résolution encourage une coopération étroite avec les organisations œuvrant pour mettre fin à l'exploitation sexuelle des enfants sur Internet, et appelle les États à élaborer des politiques nationales pour prévenir et réprimer l'exploitation sexuelle des enfants en ligne.

Lors d'une discussion axée sur les « défis et opportunités pour le plein exercice par les enfants de leurs droits dans l'environnement numérique » qui a eu lieu le 10 mars 2023, durant sa journée annuelle, la question droits de l'enfant dans l'environnement numérique a été abordée par le CDH[38], et la France est notamment intervenue lors de celle-ci. Le respect de l'intérêt supérieur de l'enfant dans toutes les activités en ligne a notamment été souligné lors de cette discussion, ainsi que l'importance de mettre à la disposition des enfants des moyens d'accès publics et gratuits, au sein de bibliothèques publiques ou au sein des écoles, au regard des difficultés d'accès à l'internet dans les régions rurales.

Une autre *résolution concernant la promotion, la protection et l'exercice des droits de l'Homme sur internet*[39] a par ailleurs été adoptée en 2016 affirmant que les droits de l'Homme, notamment la liberté d'expression, doivent être protégés en ligne comme hors ligne. Elle souligne également l'importance de combler le fossé numérique entre les sexes. La France a soutenu la résolution en participant à son élaboration en tant que co-auteur, aux côtés d'autres États.

De plus, le Secrétaire général des Nations Unies joue un rôle central dans la promotion des droits de l'Homme à travers plusieurs fonctions clés, en tant que plus haut fonctionnaire de l'ONU[40]. En tant que porte-parole mondial des droits de l'Homme, il présente régulièrement des rapports à l'Assemblée générale et au CDH. Son rapport de 2024 sur l'*Intensification de l'action menée pour éliminer toutes les formes de violence à l'égard des femmes et des filles : violence contre les femmes et les filles facilitée par les technologies*[41] met notamment en lumière l'ampleur

---

[38] *Compte rendu de séance, Conseil des droits de l'homme, Le Conseil des droits de l'homme se penche sur les défis et opportunités pour le plein exercice par les enfants de leurs droits dans l'environnement numérique*, 10 mars 2023, https://www.ohchr.org/fr/news/2023/03/it-may-be-time-reinforce-universal-access-internet-human-right-not-just-privilege-high

[39] *Résolution 32/13 : La promotion, la protection et l'exercice des droits de l'homme sur Internet,* Conseil des droits de l'Homme, 1er juillet 2016

[40] Article 97 de la Charte des Nations Unies

[41] *Rapport du Secrétaire général - Intensification de l'action menée pour éliminer toutes les formes de violence à l'égard des femmes et des filles : violence contre les femmes et les filles facilitée par les technologies, A/79/500,* 8 octobre 2024

croissante des violences en ligne à l'encontre des femmes et des filles, en insistant sur les disparités d'accès à un environnement numérique sûr. Il souligne que les inégalités structurelles - notamment liées au genre, à l'âge ou à la situation socio-économique - exposent certaines filles à un risque accru de cyber violence, de harcèlement ou d'exploitation. Le rapport s'appuie sur le cadre juridique international, notamment la *CIDE* et la *Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes*[42], pour rappeler aux États leurs obligations de prévenir les violences numériques, de promouvoir l'égalité d'accès aux technologies et de garantir des environnements numériques inclusifs, protecteurs et respectueux des droits fondamentaux des enfants et des adolescentes.

II. L'approche adoptée par la France au regard du cadre juridique international

La France adopte une approche structurée en matière du numérique. Dans les différents volets de son action, elle a pour ambition de développer une IA « éthique » (A), de lutter contre la cybercriminalité (B), de promouvoir et protéger la liberté d'expression (C) ainsi que les droits des enfants (D).

Sur l'approche diplomatique française de manière globale

Face aux nombreux instruments juridiques et institutions internationales existants, la France doit se positionner dans ses actions internationales. La prise en compte de l'environnement numérique a été progressive, mais la France reconnaît tout de même son importance.

Tout d'abord, dans sa candidature au CDH pour le mandat 2021-2023, le numérique, notamment sa régulation, ne faisait pas partie de ses axes prioritaires. La candidature soutenait cependant des engagements globaux tels que la lutte contre les inégalités et discriminations, la protection des libertés fondamentales et le soutien aux défenseurs des droits de l'Homme. Ainsi, le numérique en tant qu'espace à réguler ou champ d'action en matière de droits de l'Homme n'était pas présenté comme une priorité stratégique dans cette candidature. La mention même du numérique était marginale voire absente (le mot «

[42] Nations Unies. (1966), *Convention internationale sur l'élimination de toutes les formes de discrimination raciale*, Recueil des Traités, 660, 195

numérique » n'étant cité que deux fois). L'environnement numérique est simplement vu comme un phénomène nouveau, comme un espace où de nouvelles menaces se développent :

> *« Avec des **phénomènes nouveaux**, comme l'impact du changement climatique, l'aggravation des inégalités mondiales de développement et **l'expansion rapide des technologies numériques, sont apparues des menaces nouvelles** : l'émergence d'un terrorisme de masse, le recul des droits fondamentaux dans de nombreux États, l'aggravation des inégalités économiques et sociales, et les remises en cause nouvelles de l'égalité entre les femmes et les hommes.*[43] *»*

Concernant sa candidature pour le mandat 2024-2026, la France reconnaît cette fois l'importance des technologies numériques en tant que levier de développement (le mot « numérique » est notamment cité dans cette candidature sept fois). Elle s'engage à garantir l'accès universel aux technologies numériques, notamment dans le cadre de ses priorités en matière de solidarité et de développement durable.

Bien que la France ait renforcé sa prise en compte du numérique dans sa dernière candidature, son approche reste prudente et générale. Les droits de l'Homme à l'ère numérique. Ces enjeux sont davantage portés dans d'autres espaces que dans le cadre de sa candidature au CDH.

Par ailleurs, sur son site *France Diplomatie*[44], la France présente les quatre grands enjeux autour desquels s'articule sa diplomatie numérique, en continuité avec sa *Stratégie internationale pour le numérique*[45] présentée le 15 décembre 2017 par le ministre Jean-Yves LE DRIAN. La diplomatie numérique française s'articule ainsi autour des enjeux suivants : garantir la sécurité internationale du cyberespace, à travers le renforcement de l'autonomie stratégique européenne et la promotion de la stabilité du cyberespace dans les instances internationales et la régulation des contenus diffusés sur l'internet ainsi que la régulation des plateformes ; contribuer à la gouvernance de l'Internet en renforçant son caractère ouvert et

---

[43] *La France candidate au Conseil des droits de l'Homme 2021-2023,* MEAE. Lien : https://www.diplomatie.gouv.fr/IMG/pdf/candidature_cdh_fr_cle825da2.pdf

[44] *« Quels sont les grands principes de la diplomatie numérique de la France ? », Diplomatie numérique*, MEAE, 2020. Lien : https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/

[45] *Stratégie internationale de la France pour le numérique*, MEAE, 15 décembre 2017, https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf

diversifié, tout en renforçant la confiance dans son utilisation ; promouvoir les droits de l'Homme, les valeurs démocratiques et la langue française dans le monde numérique ; renforcer l'influence et l'attractivité des acteurs français du numérique. La France affirme ainsi sa volonté de promouvoir la langue française dans le monde numérique. Cependant, cette orientation repose sur une interprétation restrictive, dans la mesure où la France a signé la *Charte européenne des langues régionales ou minoritaires* de 1992 mais elle ne l'a jamais ratifiée.

Enfin, l'ambassadeur du numérique a pour mission de promouvoir, auprès des partenaires internationaux et des acteurs publics et privés, les positions de la France. Afin d'anticiper au mieux les problématiques numériques de demain soulevées par l'avancée du numérique, l'ambassadeur du numérique a pu participer à la table-ronde « Après la crise : construire le service public de demain », Rencontres internationales de la gestion publique (RIGP) le 8 septembre 2020, à une audition par la mission parlementaire sur la politique publique de la donnée de l'Assemblée nationale le 19 octobre 2020 ou à la table-ronde « Anticiper les enjeux de demain : illectronisme, évolution des métiers, mixité, souveraineté » par le Ministère de l'Education nationale le 4 novembre 2020.

Cependant, bien que le MEAE ait amorcé depuis deux ans un effort de compréhension des technologies du numérique et de l'IA, aucune action concrète n'a encore été mise en œuvre pour accompagner les pays en développement dans leur transition numérique. Si la nomination d'un ambassadeur du numérique et les discussions diplomatiques sur la gouvernance mondiale du numérique signalent une prise de conscience institutionnelle, ces démarches restent largement tournées vers la coordination entre États plutôt que vers l'assistance technique. Le réseau diplomatique soutient ponctuellement certaines filières à l'international, mais sans vision unifiée ni stratégie nationale claire. Aucune initiative française ne vient actuellement répliquer ou amplifier les efforts de coopération numérique mis en place dans d'autres pays du Nord. Quant à la direction du numérique du MEAE, elle est principalement focalisée sur les outils internes du ministère, sans volet opérationnel tourné vers l'extérieur. À ce jour, en réponse à la question du développement numérique dans les pays les moins avancés, le MEAE n'a engagé aucune action directe.

A) <u>La position de la France sur le plan international en matière d'IA</u>

La France affirme une position proactive sur la scène internationale en matière

d'éthique et de gouvernance de l'intelligence artificielle. Elle soutient le développement d'une *« capacité internationale de réflexion sur l'éthique de l'IA »*[46], tant sur le plan normatif que stratégique, dans un esprit de coopération technologique, démocratique et sécuritaire. La France s'est associée, aux côtés de 14 autres pays fondateurs, au lancement du *Partenariat mondial pour l'intelligence artificielle* (PMIA) en juin 2020, sous l'impulsion conjointe de plusieurs pays membres du G7 et en coordination avec l'OCDE. Cette initiative marque un jalon structurant dans cette démarche. En réunissant des représentants issus des sphères publiques, privées, académiques et de la société civile, cette plateforme encourage la convergence entre excellence scientifique et encadrement normatif. En juillet 2024, la *Déclaration de New Delhi* a été adoptée par les membres du PMIA. Elle formalise également les orientations prioritaires qui guideront les travaux futurs des membres afin de concilier innovation et responsabilité. Ces avancées ont été présentées dans le cadre du Sommet mondial de l'IA en Inde. Lors du Sommet 2024 à Belgrade du PMIA, co-présidé par la Serbie et la République slovaque, la France a été représentée par des experts et des diplomates engagés. Un des résultats majeurs du sommet fut l'adoption de la *Déclaration ministérielle de Belgrade* qui réaffirme une nouvelle fois l'importance des valeurs fondamentales partagées par ses membres :

> "*REAFFIRMING our shared core values and principles, notably the preservation of individual liberty, values of democracy, the rule of law and the protection of human rights*;"

B) La position française en faveur de l'encadrement de la cybercriminalité

La France est particulièrement active au sein des instances internationales sur les questions de cybersécurité, notamment aux discussions qui se tiennent à l'Organisation des Nations-Unies (ONU). Elle a notamment participé aux cinq derniers groupes d'experts gouvernementaux (GGE) sur la cybersécurité, dont les travaux ont permis d'affirmer l'applicabilité du droit international, notamment de la *Charte des Nations Unies* au cyberespace et de produire des recommandations liées à la sécurité du cyberespace. Ces groupes de travail ont également permis de définir des normes de comportement pour garantir le « comportement responsable » des États.

---

[46] *Rapport d'activité 2020 de l'Ambassadeur pour le numérique*, MEAE, 2020. Lien : https://www.diplomatie.gouv.fr/IMG/pdf/rapport_d_activite_ambassadeur_pour_le_numerique_2020_cle8a5815.pdf

Au sein d'autres instances internationales, la France promeut sa vision du numérique et s'engage à lutter contre le terrorisme en ligne, notamment en participant aux travaux du groupe d'experts de l'OCDE, qui ont pour objectif d'obliger les entreprises à mettre en place des rapports de transparence pour rendre compte de leurs efforts dans la lutte contre ces contenus. Elle défend également la position et les valeurs françaises sur la liberté d'expression dans la lutte contre les contenus terroristes en ligne lors de conférences (notamment lors de la conférence RightsCon du 27 janvier 2020, qui avait pour objet les droits de l'Homme à l'ère du numérique).

C) Une diplomatie numérique française de défense proactive des droits de l'enfant

La France adopte une approche proactive et engagée pour défendre les droits des enfants, tant sur le plan national qu'international, en s'appuyant sur la *CIDE* qu'elle a ratifiée en 1990. Au niveau national, le Défenseur des droits joue un rôle central en veillant à l'application de la *CIDE*. Depuis 2017, un dispositif indépendant a été mis en place pour surveiller l'effectivité des droits de l'enfant, comprenant une veille juridique, un dialogue avec les associations et le recueil de l'opinion des enfants eux-mêmes.

Sur la scène internationale, la France participe activement aux travaux du Comité des droits de l'enfant des Nations Unies, présentant régulièrement des rapports sur l'application de la Convention. Elle promeut également des initiatives telles que la lutte contre les violences faites aux enfants, y compris en ligne, et l'élargissement des droits en matière d'éducation[47].

Lors de la 79e session de l'Assemblée générale des Nations Unies en octobre 2024[48], la France a réaffirmé son engagement envers la protection des droits des enfants, en mettant l'accent sur quatre priorités majeures, notamment la protection des enfants dans l'environnement numérique. La Troisième Commission a adopté neuf projets de résolution, dont l'un, présenté par la France[49], visait à intensifier l'action pour prévenir et éliminer toutes

---

[47] *Communiqué conjoint du MEAE et du secrétariat d'État chargé de l'Enfance*, 9 mai 2023. Lien : https://solidarites.gouv.fr/nations-unies-comite-des-droits-de-lenfant-examen-du-respect-de-la-france-de-la-convention

[48] *La France appelle à assurer la protection des droits des enfants, Déclarations de la France à l'ONU, Intervention de M. Tudor ALEXIS, Secrétaire général adjoint mission AGNU 79 à l'Assemblée générale des Nations Unies,* 10 octobre 2024. Lien : https://onu.delegfrance.org/la-france-appelle-a-la-pleine-mise-en-oeuvre-de-la-convention-internationale

[49] *« La Troisième Commission adopte neuf projets de résolution, consacrant l'essentiel de son attention aux violences à l'égard des femmes dans l'environnement numérique»,* Couverture des réunions & communiqués de presse, AG/SHC/4430, 14 novembre 2024. Lien : https://press.un.org/fr/2024/agshc4430.doc.htm

les formes de violence à l'égard des femmes et des filles dans l'environnement numérique. Ce texte exhorte les États à prendre des mesures multisectorielles et coordonnées pour prévenir ces violences et remédier aux causes structurelles et aux facteurs de risque. De plus, enc collaboration avec les Pays-Bas, la France a porté un projet de résolution visant à éliminer les violences faites aux femmes et aux filles dans l'environnement numérique[50].

Par ailleurs, la France est à l'origine de plusieurs initiatives pour promouvoir et protéger les droits des enfants dans l'environnement numérique. Elle adapte notamment ses lois comme par exemple l'adoption d'une loi visant à garantir le respect du droit à l'image des enfants (*Loi n°2024-120 du 19 février 2024 parue au JO n°42 du 20 février 2024*), qui définit expressément la situation du droit à l'image des mineurs ou encore une loi visant à encadrer l'exploitation commerciale de l'image d'enfants de moins de seize ans sur les plateformes en ligne (*Loi n° 2020-1266 du 19 octobre 2020 parue le 20 octobre 2020*).

Le Comité des droits de l'enfant encourage toutefois la France à renforcer l'effectivité du droit à l'oubli numérique, à mieux encadrer l'exploitation de l'image des enfants en ligne, à intégrer l'éducation numérique dans les programmes scolaires et à veiller à ce que le contrôle parental respecte pleinement la vie privée des enfants :

> *« Tout en notant que la loi no 2016-1321 du 7 octobre 2016 pour une République numérique consacre le droit des enfants à l'oubli numérique,* ***le Comité recommande à l'État partie de sensibiliser le public, en particulier les enfants, à ce droit sur Internet et d'en contrôler le respect****. Il prend note de l'adoption de la loi no 2020-1266 du 19 octobre 2020 visant à encadrer l'exploitation commerciale de l'image d'enfants de moins de 16 ans sur les plateformes en ligne et recommande à l'État partie de* ***renforcer l'application de cette loi et l'éducation numérique à l'école****, en les intégrant aux programmes scolaires et en formant les enseignants à l'utilisation des nouvelles technologies. Il lui recommande également de veiller à ce que l'application de la loi no 2022-300 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à Internet respecte totalement le droit des enfants à la*

[50] *Adoption de la résolution franco-néerlandaise sur les violences faites aux femmes et aux filles, Déclarations de la France à l'ONU, Intervention de M. Nicolas DE RIVIERE, Représentant permanent de la France auprès des Nations Unies à l'Assemblée générale des Nations Unies*, 14 novembre 2024. Lien : https://onu.delegfrance.org/adoption-a-l-agnu-de-la-resolution-franco-neerlandaise-visant-a-lutter-contre

protection de leur vie privée.[51] »

Enfin, dans sa candidature au CDH pour le mandat 2021-2023, de façon spécifique, la France n'avait pas mis l'accent sur la protection des droits des enfants à l'ère du numérique. Les droits des enfants dans le numérique, ne sont pas encore pleinement intégrés comme axes structurants de sa stratégie au sein du CDH. Néanmoins, la France a démontré son engagement sur ces questions dans d'autres forums, et met en avant dans sa candidature la *Déclaration sur les droits de l'enfant dans l'environnement numérique*[52] et la création d'un laboratoire pour la protection de l'enfance en ligne :

> *« Elle a lancé une Déclaration sur les droits de l'enfant dans l'environnement numérique, qui appelle à renforcer l'éducation au numérique et à développer des outils numériques adaptés aux enfants, ainsi qu'à mieux protéger les enfants des menaces en ligne. A cet effet, la France a mis en place un laboratoire international pour la protection de l'enfance contre les dangers auxquels ils sont confrontés sur Internet.*[53] »

Chapitre II. La France dans la diplomatie numérique européenne

Au niveau régional, le droit encadre les technologies numériques et les droits fondamentaux. A travers les institutions de l'Union européenne et du Conseil de l'Europe, deux ensembles politiques et juridiques européens, ces derniers contribuent à la protection des droits de l'Homme dans l'environnement numérique par la création de normes contraignantes ou d'instruments politiques et programmatiques. Un cadre juridique dense et riche s'impose aux Etats Membres (I). Ces outils juridiques et politiques mettent en lumière la cohérence et la complémentarités des ces différents organismes dans leur capacité à répondre aux défis actuels du numérique. La France, en tant qu'Etat membre de l'Union européenne et du Conseil de l'Europe, s'insère pleinement dans cette architecture normative (II).

---

[51] *Observations finales concernant le rapport de la France valant sixième et septième rapports périodiques CRC/C/FRA/CO/6-7,* Comité des droits de l'enfant, 4 décembre 2023

[52] *Déclaration conjointe sur les droits de l'enfant dans l'environnement numérique*, MEAE, 11 mars 2022. Lien ::https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/societe-civile-et-volontariat/evenements-incluant-la-societe-civile/forum-de-paris-sur-la-paix/4e-edition-du-forum-de-paris-sur-la-paix/article/la-france-appelle-a-defendre-les-droits-de-l-enfant-dans-l-environnement#sommaire_2

[53] *Candidature de la France au Conseil des droits de l'Homme pour la période 2024-2026, Engagements pris volontairement en application de la résolution 60/251 de l'Assemblée générale,* Représentation permanente de la France auprès des Nations Unies à New York, Lien : https://onu.delegfrance.org/candidature-de-la-france-au-conseil-des-droits-de-l-homme-2024-2026

I. Le cadre juridique européen

Après avoir présenté le socle juridique européen, il convient de s'intéresser à un cadre européen plus spécifique à certaines mutations numériques notamment celui relatif, à la protection des données personnelles (A), au domaine de l'IA (B), à la cybercriminalité (C), à la lutte contre la désinformation et la liberté des médias (D) et à la protection des droits de l'enfants (E).

Sur le cadre juridique européen global

En tant qu'Etat membre de l'Union européenne, la France est tenue de respecter et de mettre en œuvre le droit européen, notamment les règlements et directives relatifs à la protection des droits fondamentaux, à la régulation des technologies numériques et à la gouvernance de l'intelligence artificielle, dans le respect des principes de subsidiarité et de proportionnalité qui régissent l'action de l'Union. A ce titre, elle doit veiller à garantir les droits énoncés par la *Charte des droits fondamentaux de l'Union européenne*, notamment le respect de la vie privée, la protection des données personnelles, la non-discrimination et la dignité humaine.

Les Conclusions du Conseil des affaires étrangères du 18 juillet 2022, s'inscrivant dans la stratégie « Global Gateway », affirment une volonté de l'UE d'orienter la transformation numérique selon *« une approche centrée sur l'humain »*[54]. L'adoption du *Digital Services Act (DSA)*[55] et du *Digital Markets Act (DMA)*[56] s'inscrit dans cette logique, en dotant l'UE d'un cadre normatif plus robuste visant à encadrer les pratiques des grandes plateformes numériques tout en garantissant la protection des utilisateurs. L'UE entend renforcer cette dynamique par une coordination accrue entre ses institutions et ses États membres, en lien avec les enceintes multilatérales telles que l'ONU, l'OSCE, le Conseil de l'Europe ou encore le G7. L'UE souhaite fonder sa diplomatie numérique sur le respect et la promotion des droits de l'Homme, des libertés fondamentales et du principe démocratique. Le Conseil de l'UE invite par ailleurs les Etats membres à lutter contre les campagnes de désinformation et contre les ingérences étrangères, notamment par la Russie, en approuvant la mise en place de mesures contre les « acteurs de manipulation de l'information ». L'ouverture d'un bureau diplomatique à San Francisco en 2022 illustre concrètement cette stratégie d'influence

[54] *Conclusions du Conseil 11406/22 du 18 juillet 2022 sur la diplomatie numérique de l'UE*
[55] *Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (Digital Services Act)*
[56] *Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 sur les marchés contestables et équitables dans le secteur numérique (Digital Markets Act)*

normative, visant à dialoguer directement avec les grandes entreprises technologiques américaines et à défendre le modèle de gouvernance numérique européen à l'échelle internationale.

L'Union européenne est fermement engagée à garantir un environnement numérique sûr et ouvert, en luttant contre la cybercriminalité, notamment le terrorisme en ligne, et en garantissant la liberté d'expression et un environnement sûr pour les médias.

A) Une Europe forte sur la législation de la protection des données personnelles

Une donnée est la représentation conventionnelle d'une information en vue de son traitement informatique. En langage binaire, elle est représentée par une suite de 0 et de 1. Une donnée est dite « personnelle » lorsqu'elle contient une information se rapportant à une personne physique qui pourrait permettre de l'identifier directement ou indirectement. Le nom, l'identifiant, l'adresse électronique ou des données de localisation sont des exemples de données personnelles. Le *règlement général sur la protection des données personnelles (RGPD)*[57] vient définir la donnée à caractère personnel comme *« toute information se rapportant à une personne physique identifiée ou identifiable* ». Une « personne physique identifiable » est une personne qui peut être distincte des autres non seulement « *par référence à un identifiant »* mais aussi par *« un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».* En matière de protection de données personnelles et des droits de l'Homme, la diplomatie numérique de la France s'appuie fermement sur le cadre juridique européen. Le RGPD, entré en vigueur en 2018, établit un standard élevé et contraignant pour la collecte, le traitement et la sécurisation des données personnelles, affirmant la primauté des droits individuels à la vie privée et à la protection des données dans l'Union. La France est aussi signataire de la *Convention 108+ sur la protection des données personnelles*[58].

Le cadre juridique de l'Union européenne n'est pas aussi respectueux des droits de l'Homme qu'il prétend l'être. La décision d'adéquation adoptée par la Commission européenne le 10

[57] *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 (RGPD)*
[58] *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108)*, 1981

juillet 2023[59] doit simplifier la législation sur le transfert des données entre les Etats-Unis et les Etats membres de l'Union. Toutefois, la Cour de justice de l'Union au travers de l'arrêt Schrems I[60] a invalidé la première décision dénommée *Safe Harbor*, accord conclu entre la Commission européenne et les États-Unis qui permettait aux entreprises américaines s'y soumettant de transférer les données personnelles des ressortissants de l'Union vers leur territoire. Par la suite, fut conclu le 2 février 2016 le controversé « *Privacy shield* »[61] destiné à maintenir les accords commerciaux tout en se conformant aux exigences de la Cour de justice afin d'assurer un niveau de protection suffisant des données à caractère personnel transférées aux États-Unis. Par un arrêt Schrems II[62], la Cour de justice a invalidé ce deuxième accord au motif qu'il était contraire à l'article 45 du *RPGD.*

En vertu de l'article 45, paragraphe 3, du *RGPD*, la Commission a décidé par voie d'actes d'exécution que les Etats-Unis assurait désormais « un niveau de protection adéquat » des données à caractère personnel, c'est-à-dire substantiellement équivalent à celui garanti au sein de l'Union. Ces décisions constatant le caractère adéquat du niveau de protection, comme c'est le cas en espèce, ont pour effet de permettre le transfert libre de données à caractère personnel de l'Union, ainsi que de la Norvège, du Liechtenstein et de l'Islande vers un pays tiers sans autre obstacle. Dès lors, le transfert de données personnelles depuis l'UE vers certains organismes états-uniens de façon libre et sans encadrement spécifique par des «clauses contractuelles types » est désormais possible. Cependant, « l'existence de principes fondamentaux de protection des données et les droits individuels » semblent aussi avoir été négligés dans cette évaluation effectuée par les autorités européennes de protection des données. L'*avis du Comité européen à la protection des données*[63], rendu le 28 février 2022 sur le dernier projet de décision d'adéquation de la Commission européenne, exprime de nombreuses préoccupations à ce sujet. L'annexe I, I.5 du projet de décision d'adéquation

---

[59] *Décision d'exécution (UE) 2023/1795 de la Commission du 10 juillet 2023 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE - États-Unis*

[60] *Cour de justice de l'Union européenne, Maximillian Schrems/Data Protection Commissioner (Schrems I), 6 octobre 2015, C-362/14, EU:C:2015:650*

[61] *Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis*

[62] *Cour de justice de l'Union européenne, Data Protection Commissioner/Facebook Ireland Ltd et Maximillian Schrems (Schrems II),16 juillet 2020, C-311/18, EU:C:2020:559*

[63] *Avis 28/2022 sur les critères de certification Europrivacy en ce qui concerne leur approbation par le comité en tant que label européen de protection des données conformément à l'article 42, paragraphe 5 (RGPD),* Comité européen de la protection des données, 10 octobre 2022

prévoit que l'adhésion des organisations aux principes posés peut être limitée, notamment dans la mesure nécessaire pour se conformer à une décision de justice ou pour répondre à des exigences d'intérêt public, d'application de la loi ou de sécurité nationale mais elle peut également être limitée par une loi, une décision de justice ou une réglementation gouvernementale. En outre, la décision d'adéquation propose des exemptions au droit d'accès pourtant consacré à l'article 15 du *RGPD* stipulant que :

> « *La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel* ».

Le Comité relève aussi une exemption trop générale au droit d'accès qui concerne les informations accessibles au public et celles provenant des archives publiques. Quant au "recours effectif", ce dernier reste très controversé.

B) Vers une gouvernance européenne de l'IA : un positionnement tardif mais ambitieux

La Commission européenne souhaite favoriser une législation des services numériques qui *« protège les consommateurs et leurs droits fondamentaux »*[64] en ligne en établissant des règles claires et proportionnées. Dans le *Plan d'action en faveur des droits de l'Homme et de la démocratie 2020-2024* [65], il est clairement précisé que :

« L'utilisation abusive des nouvelles technologies, dont l'IA, a pour corollaire un risque d'augmentation de la surveillance, du contrôle et de la répression ».

Par ailleurs, le 13 juin 2024, le *règlement établissant des règles harmonisées concernant l'intelligence artificielle (IA Act)*[66] a été adopté. Ce texte constitue une avancée normative majeure dans le champ du numérique. Il s'agit du premier cadre législatif contraignant

---

[64] *Loi sur les services numériques : garantir un environnement en ligne sûr et responsable*, Commission européenne, 2022. Lien : https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_fr

[65] *Plan d'action en faveur des droits de l'homme et de la démocratie 2020-2024*, Commission européenne, mars 2020

[66] *Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) no 300/2008, (UE) no 167/2013, (UE) no 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)*

spécifiquement dédié à l'intelligence artificielle au sein de l'UE. Il s'inscrit dans une logique de sécurisation des usages de l'IA, tout en veillant à leur compatibilité avec l'acquis juridique de l'Union. De surcroît, il s'aligne sur les principes de la Charte et sur les dispositions du *RGPD.*

Au niveau du Conseil de l'Europe, une *Convention-cadre sur l'intelligence artificielle, les droits de l'homme, la démocratie et l'Etat de droit*[67] a été adoptée le 17 mai 2024. Cette dernière se base sur le guide HUDERIA[68] qui fournit une approche structurée de l'évaluation des risques et des impacts des systèmes d'IA.. Il constitue le premier instrument normatif contraignant en la matière, engageant les 46 États membres du Conseil de l'Europe à transposer dans leur droit interne des standards juridiques communs visant à encadrer l'usage de l'IA dans le strict respect des valeurs démocratiques et des droits fondamentaux. La France, en tant qu'État signataire, devra ainsi adapter ses normes internes à cette Convention, consolidant sa diplomatie numérique autour d'une approche éthique, humaniste et fondée sur l'État de droit.

Le cadre européen relatif au numérique repose aussi sur d'autres instruments fondamentaux, notamment la *directive code européen des communications*[69] du 11 décembre 2018. Cette dernière harmonise la réglementation des réseaux et services de communications électroniques au sein du marché intérieur. Si elle ne vise pas explicitement l'intelligence artificielle, elle s'applique aux prestataires automatisés et encadre leur responsabilité, en garantissant la liberté d'expression en ligne conformément à l'article 52 de la Charte des droits fondamentaux de l'Union européenne. De même, la *directive 2000/31/CE*[70] instaure des principes essentiels tels que la responsabilité des intermédiaires et la protection de la vie privée des utilisateurs, assurant un environnement numérique plus respectueux des libertés individuelles. Plus récemment, le *règlement portant sur la gouvernance européenne des données*[71]*,* dit *Data Governance Act*, du 30 mai 2022, est venue instituer un cadre sécurisé de gouvernance des données publiques et privées en facilitant leur réutilisation par les systèmes

---

[67] *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108)*, Conseil de l'Europe, 1981

[68] *HUDERIA – Évaluation des risques et des impacts des systèmes d'IA*, Conseil de l'Europe, 2024, Lien : https://www.coe.int/fr/web/artificial-intelligence/huderia-risk-and-impact-assessment-of-ai-systems

[69] *Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen* (refonte)

[70] *Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information (Directive sur le commerce électronique)*

[71] *Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724*

d'IA, tout en imposant des garanties strictes. Ces normes doivent garantir que l'essor technologique s'appuie sur des principes démocratiques.

C) Un cadre juridique européen exhaustif relatif à la cybercriminalité

L'Union européenne a développé un cadre juridique fort de lutte contre la cybercriminalité, dans un premier temps avec la création en 2013 du Centre européen de lutte contre la cybercriminalité (*European Cybercrime Centre* ou *EC3*), situé à La Haye, visant à lutter contre la cybercriminalité dans l'Union européenne, notamment les crimes possibles seulement via internet, l'exploitation sexuelle des enfants ainsi que les fraudes aux paiements. Ce centre offre notamment un soutien opérationnel, stratégique, analytique et médico-légal aux enquêtes menées par les États membres.

Par ailleurs, de nombreuses normes ont été adoptées par l'Union européenne concernant la cybercriminalité. Dans un premier temps, la *directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*, dite *directive SRI*[72], adoptée en 2016, constitue la première législation prise au niveau l'UE dans l'objectif d'intensifier la coopération entre les États membres dans le domaine de la cybercriminalité. Deux règlements ont par la suite été adoptés en 2019 : le *règlement sur la cybersécurité*[73], créant notamment l'agence de l'Union européenne pour la cybersécurité, qui aide les États membres, les institutions de l'Union européenne ainsi que d'autres acteurs à lutter contre les cyberattaques ainsi que le *règlement concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses Etats membres*[74], assorti d'une *décision*[75], qui constituent le cadre juridique permettant à l'Union européenne d'imposer des sanctions, des mesures restrictives aux personnes ou entités auteurs de cyberattaques ou de tentatives de cyberattaques.

---

[72] *Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (Directive SRI)*

[73] *Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité)*

[74] *Règlement (UE) 2019/796 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses Etats membres*

[75] *Décision (PESC) 2019/797 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres*

De plus, l'UE s'est dotée d'un cadre afin d'assurer une réponse diplomatique conjointe face aux actes de cyber-malveillance : la *« boîte à outils cyberdiplomatique »*[76], qui permet à l'UE et ses Etats membres de prendre toutes les mesures relevant de la politique étrangère et de sécurité commune, y compris des sanctions, pour empêcher, décourager, prévenir et contrer les actes de cyber-malveillance. Ce cadre a notamment été revu en 2023 avec l'adoption de *lignes directrices relatives à la mise en œuvre de la* « *boîte à outil cyberdiplomatique* »[77]. En vue de réagir et de contrer les actions déstabilisatrices menées par la Russie envers l'UE et ses Etats membres, notamment celles menaçant la cybersécurité (cyberattaques, campagnes de manipulation de l'information et d'ingérence), le Conseil s'est spécifiquement doté d'un nouveau cadre juridique de sanctions en 2024, composé du *règlement*[78] et d'une *décision concernant des mesures restrictives eu égard aux activités déstabilisatrices menées par la Russie*[79]. Les mesures restrictives, pouvant être prises à l'encontre de personnes physiques et morales, constituent en des interdictions d'entrée sur le territoire de l'UE, un gel des avoirs, ou encore une interdiction de mettre des fonds ou des ressources économiques à la disposition des personnes inscrites sur la liste.

En 2022, une *directive SRI 2*[80] a été adoptée, venant remplacer la *directive SRI 1* avec un champ d'application plus large, des règles plus claires et des outils plus solides pour garantir la cybersécurité au sein de l'Union européenne. Cette directive prend ainsi en compte de nouvelles menaces numériques, ayant notamment émergé au cours de la crise sanitaire. Plus récemment, en 2024, le *règlement sur la cyber-résilience*[81] a été adopté, dénotant de la volonté globale de l'UE de renforcer ses règles, déjà nombreuses, en matière de cybersécurité. Ce règlement vient imposer des exigences obligatoires aux fabricants et aux détaillants en matière de cybersécurité pour les produits comportant des éléments

---

[76] *Conclusions du Conseil 10474/17 du 19 juin 2017 relatives à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance ("boîte à outils cyberdiplomatique")*

[77] *Lignes directrices 10289/23 du Conseil du 8 juin 2023 relatives à la mise en œuvre de la boîte à outil cyberdiplomatique*

[78] *Règlement (UE) 2024/2642 du Conseil du 8 octobre 2024 concernant des mesures restrictives eu égard aux activités déstabilisatrices menées par la Russie*

[79] *Décision (PESC) 2024/3174 du Conseil du 16 décembre 2024 modifiant la décision (PESC) 2024/2643 concernant des mesures restrictives eu égard aux activités déstabilisatrices menées par la Russie*

[80] *Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)*

[81] *Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyber résilience)*

numériques, afin de garantir que ceux-ci ne comportent pas de cyberrisques pour les consommateurs de l'UE. Le Conseil européen a également adopté une *boussole stratégique en matière de sécurité et de défense*[82] en mars 2022, premier livre blanc de l'UE sur ce sujet, qui comprend des mesures fortes pour lutter contre la cybercriminalité, dont le renforcement de la résilience et la lutte contre les menaces hybrides, les cyberattaques et les activités de manipulation de l'information et d'ingérence menées depuis l'étranger.

Concernant plus spécifiquement le terrorisme, l'Union européenne a notamment pris des mesures pour lutter contre les contenus terroristes en ligne, au regard de la menace qu'ils représentent. En effet, les technologies numériques (réseaux sociaux, dark web) sont de plus en plus utilisées pour radicaliser, recruter, inciter à la violence et faciliter la commission d'attentats terroristes. Afin de contrer ce phénomène, l'Union européenne a adopté, le 29 avril 2021, le *règlement relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne*[83], qui définit les contenus terroristes en ligne comme « *les textes, images, documents audio ou vidéo utilisés pour inciter à la commission d'actes terroristes, donner des instructions sur la manière de commettre de tels actes ou solliciter la participation à des groupes terroristes* ». Ce règlement impose le retrait ou le blocage dans l'heure par les fournisseurs de service d'hébergement, lorsqu'ils reçoivent une injonction de retrait de l'autorité nationale compétente (désignée par chaque Etat membre), de contenus à caractère terroriste à la suite de leur identification en ligne. Il prévoit également des procédures de retrait transfrontalier des contenus (lorsque le fournisseur de service d'hébergement n'est pas situé dans le même État membre que l'autorité nationale qui émet l'ordre de retrait), des mesures spécifiques à prendre par les fournisseurs de service d'hébergement exposés à ces contenus ainsi que la conservation de ces contenus par les fournisseurs à des fins administratives et judiciaires. Il a également pour objectif de mettre en place des garanties solides pour le plein respect de la liberté d'expression et d'information, en imposant notamment des obligations de transparence pour les fournisseurs de service d'hébergement, la publication de rapports de transparence annuels par les autorités nationales compétentes et en prévoyant des voies de recours pour les fournisseurs de service d'hébergement et les

[82] *Boussole stratégique en matière de sécurité et de défense - Pour une Union européenne qui protège ses citoyens, ses valeurs et ses intérêts, et qui contribue à la paix et à la sécurité internationales*, Conseil de l'Union européenne, 21 mars 2022

[83] *Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne*

fournisseurs de contenu. Des sanctions envers les plateformes en ligne en cas de violations systématiques sont également prévues, pouvant aller jusqu'à 4% de leur chiffre d'affaires.

Par ailleurs, le Forum de l'Union européenne sur l'internet est une initiative lancée par la Commission européenne en décembre 2015, qui regroupe les pays de l'UE ainsi que les pays signataires de l'accord de libre échange européen, certaines institutions et agences européennes (Europol, Eurojust, l'Agence des droits fondamentaux, le SEAE et le coordinateur du Conseil pour la lutte contre le terrorisme) des acteurs de l'industrie de l'internet (notamment Amazon, MistralAl, Microsoft, Twitter, Tiktok, Telegram, Google …) et d'autres partenaires, notamment le Bureau des Nations Unies pour la lutte contre le terrorisme. Ce forum a pour objectif la collaboration entre ces différents acteurs et l'alignement des positions européennes en matière de cybersécurité, notamment en ce qui concerne l'utilisation abusive de l'internet à des fins terroristes, autour de deux actions principales : la réduction de l'accessibilité des contenus à caractère terroriste en ligne et l'augmentation du volume des récits alternatifs en ligne. Ce Forum a ainsi participé à l'élaboration de plusieurs initiatives pour lutter contre le terorrisme en ligne, notamment la création de l'Unité de l'Union européenne chargée du signalement des contenus à caractère terroriste sur l'internet (EU IRU) d'Europol en 2015 et l'élaboration d'une liste de groupes d'extrémisme de droite violente en ligne, de symboles et de manifestes pour soutenir la modération des contenus par les parties prenantes de l'industrie, qui n'a aucun d'effet contraignant.

D) <u>Cadre juridique de lutte contre la désinformation et la liberté des médias</u>

La désinformation est un enjeu majeur pour l'Union européenne, au regard de ses conséquences néfastes pour la démocratie, et plus spécifiquement pour la liberté d'expression, garantie notamment par l'*article 11 de la Charte des droits fondamentaux de l'Union européenne*, qui repose sur l'existence de médias libres et indépendants et sur l'accès par les citoyens à des informations fiables, diversifiées et de qualité. En raison des nouvelles technologies, cette désinformation a atteint un niveau sans précédent. Les campagnes de désinformation en ligne à grande échelle, qui sèment la méfiance et créent des tensions sociales, nécessitent donc une réponse coordonnée de la part des pays et des institutions de l'UE, des plateformes en ligne, des médias d'information mais également des citoyens.

Plusieurs initiatives ont ainsi été prises par la Commission européenne pour lutter contre la désinformation, afin de protéger l'Union européenne, ses institutions, ses citoyens, ses politiques. La *Communication "lutter contre la désinformation en ligne : une approche européenne"*[84] du 26 avril 2018 décrit la démarche globale qu'entend mener la Commission européenne pour lutter contre la désinformation en ligne, qui comprend plusieurs objectifs : améliorer la transparence concernant l'origine des informations, favoriser la diversité des informations, promouvoir la crédibilité de celles-ci et élaborer des solutions inclusives.

Par ailleurs un *Code de bonnes pratiques contre la désinformation*[85], adopté en 2018 et renforcé en 2022, regroupant divers acteurs, notamment les grandes plateformes du numérique (Google, Tiktok, Twitter s'étant retiré en 2023), des acteurs de la publicité, de la technologie de pointe ou encore de la société civile qui s'engagent à lutter contre la désinformation, en prévoyant des normes d'autorégulation. Il est notamment prévu que ce Code soit intégré en tant que *Code de bonnes pratiques volontaires contre la désinformation* au sein du cadre de la législation sur les services numériques à partir du 1er juillet 2025, et deviendra ainsi le cadre de référence pour déterminer si les plateformes sont en conformité avec le *règlement sur les services numériques* de 2022 (règlement DSA).

Une autre initiative de la Commission européenne a été l'adoption du *Plan d'action contre la désinformation*[86] en 2018, dans l'objectif de renforcer les capacités et la coopération de l'UE en matière de lutte contre la désinformation, notamment au regard des élections européennes de 2019. Ce *Plan d'action* décrit les mesures que la Commission et la Haute représentante, avec le soutien du Service européen pour l'action extérieure (SEAE), en coopération avec les Etats membres et le Conseil européen doivent prendre pour lutter contre la désinformation, comme la mise en place d'un système d'alerte rapide pour réagir aux campagnes de désinformation, en collaboration avec les réseaux existants, le Parlement européen, l'Organisation du traité de l'Atlantique Nord (OTAN) et le mécanisme d'intervention rapide du G7. Ce *Plan d'action* prévoit également la surveillance continue par la Commission de la

[84] *Lutter contre la désinformation en ligne : une approche européenne,* Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, 26 avril 2018, COM(2018) 236 final

[85] *Code de bonnes pratiques contre la désinformation,* Commission européenne, 2018

[86] *Plan d'action contre la désinformation***,** Communication conjointe au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions, 5 décembre 2018, JOIN(2018) 36 final

mise en oeuvre du *Code de bonnes pratiques contre la désinformation* ou encore du soutien par les États membres, en coopération avec la Commission, à la création d'équipes multidisciplinaires de vérificateurs de faits et de chercheurs indépendants afin de détecter et de dénoncer les campagnes de désinformation. D'autres mesures consignées dans ce *Plan d'action* visent à renforcer la sensibilisation de la population à la désinformation, notamment par des communications stratégiques dans le voisinage de l'UE.

Un *Plan d'action pour la démocratie européenne*[87] a également été adopté en 2020 dans le but de renforcer la résilience des démocraties au sein de l'UE, ce qui passe notamment par le renforcement de la cybersécurité, la lutte contre la désinformation et les cyberattaques. En vue de remplir cet objectif, les mesures prévues dans ce plan visent à promouvoir des élections libres et équitables, avec la mise en place notamment d'un nouveau mécanisme opérationnel conjoint pour la résilience électorale en vue de renforcer les capacités des États membres à faire face aux risques liés aux élections, en particulier en ce qui concerne la désinformation et les cybermenaces, en étroite coopération avec le groupe de coopération SRI. Par ailleurs, le plan entend renforcer la liberté et le pluralisme des médias, tout en intensifiant la lutte contre la désinformation. Cela inclut, par exemple, l'amélioration des instruments européens existants destinés à lutter contre l'ingérence étrangère, en particulier ceux permettant d'imposer des sanctions financières.

Plusieurs groupes de travail ont par ailleurs été créés au sein du SEAE, notamment le groupe de travail East Stratcom en 2015, qui a trois domaines d'action : la communication et la promotion efficaces des politiques de l'UE e à l'égard du voisinage oriental ; le renforcement de l'environnement médiatique global dans le voisinage oriental et les États membres, englobant un soutien à la liberté des médias et un renforcement des médias indépendants et l'amélioration des capacités de l'UE de prévoir, de s'attaquet et de répondre aux activités de désinformation menées par la Russie. Le SEAE a par la suite mis en place deux groupes de travail supplémentaires : la *task force* « Balkans occidentaux » et la *task force* « Sud » pour les pays du Proche-Orient, d'Afrique du Nord et de la région du Golfe.

[87] *Plan d'action pour la démocratie européenne*, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, 3 décembre 2020, COM(2020) 790 final

L'Union européenne est venue également encadrer la question des « *deep fakes* », manipulation de l'information qui constitue un enjeu majeur pour les démocraties à l'ère de l'intelligence artificielle. Ces enregistrements vidéos ou audios réalisés ou modifiés grâce à l'IA ou ces contenus faux rendus profondément crédibles par l'IA sont ainsi encadrés par le *règlement sur l'intelligence artificielle*[88] du 13 janvier 2024, première législation au monde visant à encadrer le développement, la mise sur le marché et l'utilisation de l'IA. Ce règlement impose ainsi, dans son préambule, que *"les déployeurs qui se servent d'un système d'IA pour générer ou manipuler des images ou des contenus audio ou vidéo présentant une ressemblance sensible avec des personnes, des objets, des lieux, des entités ou des événements existants et pouvant être perçu à tort par une personne comme authentiques ou véridiques (hypertrucages), devraient aussi déclarer de manière claire et reconnaissable que le contenu a été créé ou manipulé par une IA en étiquetant les sorties d'IA en conséquence et en mentionnant son origine artificielle"*.

Le *DSA* est venu également s'attaquer à la désinformation, en imposant des mesures aux très grandes plateformes et très grands moteurs de recherche, proportionnées aux risques sociétaux que représentent la diffusion de contenus préjudiciables.

L'UE s'est également fixée comme priorité de renforcer l'indépendance, la transparence et le pluralisme des médias et des journalistes notamment avec l'adoption du *règlement établissant un cadre commun pour les services de médias dans le marché intérieur* du 11 avril 2024, dit *règlement européen sur la liberté des médias*[89]. Ce règlement, qui s'inscrit dans le *plan d'action de la Commission pour la démocratie européenne*[90], suit les objectifs de ce dernier : lutter contre la montée des extrémismes et le risque d'ingérence étrangère dans les scrutins électoraux européens, en imposant notamment la publication de la liste des propriétaires de médias ; en demandant aux autorités nationales de procéder à une évaluation des concentrations des médias privés et de leur impact sur le pluralisme des médias et l'indépendance éditoriale dans leur État ; en interdisant l'utilisation de logiciels espions et d'outils de surveillance contre les médias, les journalistes et leurs familles ainsi qu'en protégeant la liberté éditoriale face aux ingérences politiques ou économiques.

---

[88] *Op. cit.* n°66, p. 36

[89] *Règlement (UE) 2024/1083 du Parlement européen et du Conseil du 11 avril 2024 établissant un cadre commun pour les services de médias dans le marché intérieur et modifiant la directive 2010/13/UE (règlement européen sur la liberté des médias)*

[90] *Op. cit.* n°88, p. 44

D’autres actions sont également menées par l’UE pour garantir la liberté et le pluralisme des médias, notamment la mise en place d’un système de surveillance de la propriété des médias visant à constituer une base de données par pays contenant des informations sur la propriété des médias. L’UE accorde par ailleurs des subventions pour soutenir l’innovation des médias locaux et régionaux et stimuler le pluralisme. Un instrument de surveillance du pluralisme des médias a été également mis en place pour repérer les risques potentiels pesant sur l’indépendance ou la diversité du secteur, ainsi qu’une plateforme pour la liberté des médias afin de soutenir les médias indépendants russes et biélorusses opérant sur le territoire de l’Union européenne.

Par ailleurs, l’UE dispose d’un Observatoire européen des médias numériques (EDMO), organisme indépendant réunissant des vérificateurs de faits, des chercheurs universitaires et d’autres parties prenantes ayant une expertise dans le domaine de la désinformation en ligne. Cet observatoire a pour mission de cartographier et soutenir les organisations de vérification des faits ; de cartographier, soutenir et coordonner également les activités de recherche sur la désinformation au niveau européen et de concevoir un cadre garantissant un accès sécurisé et respectueux de la vie privée aux données des plateformes pour les chercheurs universitaires. L’EDMO assiste également les autorités publiques dans le suivi des politiques mises en place par les plateformes numériques afin de limiter la diffusion et l’impact de la désinformation. Un portail public a également été créé afin de fournir aux professionnels des médias, aux enseignants et aux citoyens des informations et du matériel afin de renforcer la sensibilisation et la résilience face à la désinformation en ligne, tout en soutenant les campagnes d’éducation aux médias.

E) <u>Protection des droits de l’enfant</u>

Tout d'abord, l'UE a développé des instruments juridiques importants pour sécuriser les traitements de données personnelles des mineurs et prohiber le profilage. En outre, le RGPD encadre le traitement des données personnelles et prévoit des dispositions spécifiques aux mineurs.

Le DSA, règlement de l’UE entré en vigueur le 25 août 2023, impose des mesures de protection spécifiques pour les mineurs sur les plateformes en ligne. Les fournisseurs de ces plateformes doivent garantir la sécurité des mineurs, et ne pas utiliser de publicités basées sur le profilage de ces derniers. Le DSA vise à créer un espace numérique plus sûr. Il tend à rendre illégal en ligne ce qui est illégal hors ligne. 25 entités sont listées par la Commission

européenne afin de respecter le règlement : initialement AliExpress, Amazon Store, Apple AppStore, Bing, Booking, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Wikipedia, X (anciennement Twitter), Youtube et Zalando; puis récemment Pornhub, Stripchat et XVideos Shein et Temu. En cas de non respect du règlement, des sanctions peuvent être prononcées, d'abord financières mais elles peuvent aller jusqu'à l'interdiction d'activités sur le marché européen.

Par ailleurs, le DSA prend spécifiquement en compte la protection des mineurs dans son article 28, en obligeant les fournisseurs de plateformes en ligne à garantir aux mineurs un niveau élevé de protection en mettant en place des mesures appropriées et proportionnées. L'UE agit de manière concrète. En effet, la Commission européenne a ouvert en novembre 2023 une enquête visant Meta et Snap pour protéger les mineurs[91]. Cette enquête fait suite à la mise en œuvre du DSA, afin de vérifier que ces groupes sont en accord avec les protections prévues par cette réglementation. En cas d'infractions, de lourdes sanctions financières sont prévues, allant jusqu'à 6% du chiffre mondial de la société mise en cause. D'autres groupes sont visés par des enquêtes, en application du DSA[92].

La nouvelle stratégie pour un meilleur Internet pour les enfants (BIK+)[93], adoptée le 11 mai 2022, vise à garantir que les enfants soient protégés, respectés et responsabilisés en ligne conformément aux Principes numériques européens[94]. Dans le cadre de BIK+, le portail « Better Internet for Kids » continuera de proposer de nombreuses ressources et bonnes pratiques qui s'adressent aux enfants, aux parents et aux enseignants. La stratégie prévoit également un code européen sur le design adapté à l'âge, le développement de normes pour l'assurance et la vérification de l'âge, un soutien à l'évaluation rapide des contenus illicites et

---

[91] Communiqué de presse, *La Commission envoie une demande d'informations à Meta au titre de la législation sur les services numériques*, Commission européenne, 1 décembre 2023. Lien : https://digital-strategy.ec.europa.eu/fr/news/commission-sends-request-information-meta-under-digital-services-act

[92] Communiqué de presse, *La Commission envoie des demandes d'informations à YouTube, Snapchat et TikTok sur les systèmes de recommandation au titre de la législation sur les services numériques*, Commission européenne, 2 octobre 2024. Lien : https://digital-strategy.ec.europa.eu/fr/news/commission-sends-requests-information-youtube-snapchat-and-tiktok-recommender-systems-under-digital

[93] *New Better Internet for Kids Strategy (BIK+) : compendium of EU formal texts concerning children in the digital world : 2024 edition*. Commission européenne, Office des publications de l'Union européenne. Lien : https://data.europa.eu/doi/10.2759/90437.

[94] *Déclaration européenne sur les droits et principes numériques pour la décennie numérique,* 26 janvier 2022, COM(2022) 28 final

nuisibles, ainsi que l'assurance que le numéro « 116 111 » offre une aide aux victimes de cyberharcèlement.

Le Conseil de l'Europe lui, a adopté la *Stratégie pour les droits de l'enfant (2022-2027)*[95] mettant l'accent sur les droits des enfants dans l'environnement numérique. Cette stratégie été renforcée par des lignes directrices recommandées par le Comité des Ministres aux Etats membres[96]. L'intérêt supérieur de l'enfant fait parti des principes défendus par ces recommandations :

> *« Dans toutes les actions concernant l'enfant dans l'environnement numérique, l'intérêt supérieur de l'enfant* ***doit être une considération primordiale****. Lorsqu'ils évaluent l'intérêt supérieur d'un enfant, les États devraient faire tout leur possible pour équilibrer et, dans la mesure du possible, concilier le droit de l'enfant à la protection avec d'autres droits.*[97] *»*

D'autre part, il est rappelé que l'accès inégal au numérique limite la capacité des enfants à exercer pleinement leurs droits fondamentaux :

> *« L'accessibilité et l'utilisation de l'environnement numérique sont importantes pour la réalisation des droits et des libertés fondamentales des enfants, pour leur inclusion, leur éducation, leur participation et le maintien de leurs relations familiales et sociales. Lorsque les enfants n'ont pas accès à l'environnement numérique ou que cet accès est limité en raison d'une mauvaise connectivité, leur capacité à exercer pleinement leurs droits humains peut être entravée.*[98] *»*

Un *Manuel pour les décideurs politiques*[99] est venu compléter ces lignes directrices, en donnant des conseils et en aidant à la formulation de cadres et de politiques nationales.

II. La position de la France dans la diplomatie numérique européenne

La France prend part aux discussions européennes relatives au numérique, avec l'objectif de contribuer à l'élaboration d'un cadre juridique commun. Elle s'attache à

[95] *Stratégie pour les droits de l'enfant (2022-2027)*, Conseil de l'Europe, mars 2022
[96] *Recommandation CM/Rec(2018)7 du Comité des Ministres sur les Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique,* Conseil de l'Europe, 2018
[97] *Ibidem* p.12
[98] *Ibidem* p.14
[99] *Manuel pour les décideurs politiques sur les droits de l'enfant dans l'environnement numérique*, Conseil de l'Europe, décembre 2020

promouvoir un équilibre entre développement technologique et protection des droits fondamentaux, notamment en ce qui concerne le respect du principe de non-discrimination, consacré par l'article 14 de la Convention européenne des droits de l'homme (A). En parallèle, la France participe aux initiatives européennes en matière de lutte contre la cybercriminalité, en soutenant une coopération renforcée entre les États membres (B).

Sur l'approche diplomatique française au niveau européen

En tant qu'Etat membre de l'UE, la France est tenue de respecter et de mettre en œuvre le droit européen, notamment les règlements et directives relatifs à la protection des droits fondamentaux, à la régulation des technologies numériques et à la protection des droits de l'enfant, dans le respect des principes de subsidiarité et de proportionnalité qui régissent l'action de l'Union. A ce titre, elle doit veiller à garantir les droits énoncés par la Charte des droits fondamentaux de l'UE.

Dans le cadre de la présidence française du Conseil de l'UE, le Président de la République, Emmanuel Macron, a prononcé un discours face au Parlement européen afin de décliner les priorités stratégiques de la Présidence française du Conseil de l'UE. Il a mis un point d'honneur sur un des défis du siècle : « celui de la révolution numérique »[100], accompagné d'une volonté affirmée de réduire les inégalités. Cette dynamique reste à nuancer puisque la France n'a jamais signé ni ratifié le Protocole n°12 à la Convention européenne des droits de l'homme sur l'interdiction générale de la discrimination. Lors d'une question posé à l'Assemblée nationale le 22 janvier 2018[101], la France estime que sa législation nationale et l'interprétation actuelle de l'art 14 de la CEDH suffisent à garantir ce principe. La France est également un État membre du Conseil de l'Europe et doit respecter ses recommandations.

Plusieurs autorités administratives indépendantes et organes français ont été identifiés comme compétents pour assurer le respect du règlement sur l'intelligence artificielle de 2024 récemment adopté. La Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) est notamment chargée de contrôler les pratiques commerciales et de prévenir les abus dans l'utilisation des systèmes d'IA à destination des

[100] *Discours du Président Emmanuel Macron devant le Parlement européen*, 19 janvier 2022. Lien : https://www.elysee.fr/emmanuel-macron/2022/01/19/discours-du-president-emmanuel-macron-devant-le-parlement-europeen

[101] LUQUET A., *Question écrite à l'Assemblée nationale sur l'intelligence artificielle et les droits fondamentaux*, 15e législature, Journal Officiel, question publiée le 14 novembre 2017, p. 5471 ; réponse publiée le 6 février 2018, p. 943. Question signalée le 22 janvier 2018

consommateurs. La Commission nationale de l'informatique et des libertés (CNIL) est également investie d'une mission centrale dans la régulation des traitements algorithmiques impliquant des données personnelles et le défenseur des droits, autorité constitutionnelle indépendante, veille à la protection des droits et libertés, notamment face aux risques de discrimination engendrés par les biais algorithmiques.

A) La France dans les discussions européennes en matière d'IA et les potentielles violations du principe de non-discrimination (article 14 de la CEDH)

La France influence les législation dans les discussions européennes. Les travaux de Desmoulin-Canselier et Le Métayer ont inspiré ceux de l'UE sur la définition des systèmes IA[102]. Leur définition a inspiré celle de l'*IA Act* qui précise qu'un système d'IA est « *un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie* » et qui « *déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels* ».

Les outils numériques, fondés sur des algorithmes ou des systèmes d'intelligence artificielle, présentent des risques non négligeables en matière de discrimination. Les recherches récentes ont mis en lumière l'ampleur des biais pouvant survenir dès leur conception ou leur déploiement, exposant ainsi à des potentielles violations inquiétantes de l'article 14 de la CEDH. En 2019, le Conseil d'EQUINET avait déjà constaté « *l'absence d'étude européenne* »[103] sur les avantages et les risques que l'intelligence artificielle pouvait représenter au sujet du principe d'égalité, en particulier du point de vue des organes chargés de veiller à son application. En septembre 2023, lors d'une conférence de presse, la Défenseure des droits a rappelé l'urgence de « *replacer le principe de non-discrimination au cœur de tout projet sur l'IA* »[104]. Elle avait insisté sur la nécessité de garantir ce droit fondamental dans les discussions européennes et dans le *règlement européen sur l'intelligence artificielle*. Déjà

---

[102] DESMOULIN-CANSELIER S., LE MÉTAYER D., *Décider avec les algorithmes*, Dalloz

[103] « *In 2019, the Board of Equinet, the European Network of Equality Bodies, noted the lack of any European study on the benefits and risks to the principle of equality caused by automated decision making, and, more generally, by Artificial Intelligence (AI).*» EQUINET – European Network of Equality Bodies, *Regulating for an Equal AI: A New Role for Equality Bodies*, juin 2020. Lien: https://equineteurope.org/wp-content/uploads/2020/06/ai_report_digital.pdf

[104] Communiqué de presse, *« Intelligence artificielle : la Défenseure des droits appelle à garantir le droit de la non-discrimination »,* Défenseur des droits, 17 avril 2024. Lien : https://www.defenseurdesdrots.fr/intelligence-artificielle-la-defenseure-des-droits-appelle-garantir-le-droit-de-la-non-376

dans son rapport de 2020 consacré aux algorithmes, le Défenseur des droits avait souligné que les risques étaient « *considérables* »[105] et alertait sur la « *fausse neutralité des algorithmes* »[106]. Malgré ces préventions face aux dérives discriminatoires, un constat demeure : « *la prise de conscience tarde à émerger en France* »[107]. De même, le rapport de 2021 sur les technologies biométriques[108] pointait les risques de leur utilisation sur les droits fondamentaux et notamment sur le principe de non-discrimination.

Dans son rapport dédié à l'IA[109], l'*European Network of Equality Bodies* (EQUINET) avait mis l'accent sur l'importance de garantir le rôle et les pouvoirs des organismes de promotion de l'égalité dans les nouvelles mesures de contrôle visant à faire appliquer la loi et à permettre aux individus d'obtenir réparation dans le contexte des systèmes d'IA. EQUINET précise que, « par leur nature même »[110], les systèmes d'IA possèdent des biais d'exclusion et de différenciation en violation des droits de l'Homme.

B) <u>Une diplomatie française proactive au sein de l'Union européenne concernant la cybercriminalité</u>

La France, au sein de l'UE, recherche une coopération renforcée entre les Etats membres sur les questions de sécurité du cyberespace pour mieux les appréhender et défendre les intérêts communs. Sur le plan opérationnel, le but de l'action française est d'atteindre le plus haut niveau possible d'autonomie stratégique en matière technologique, réglementaire et capacitaire.

La France est particulièrement investie dans les initiatives européennes en matière de cybersécurité, en œuvrant notamment à la promotion d'une coopération accrue entre les vingt-sept États membres en cas de crise cyber. Elle a été également investie dans la préparation de l'agenda numérique européen de la nouvelle Commission, avec la volonté que la position européenne soit compatible avec les intérêts nationaux concernant notamment le marché intérieur, la coopération en matière policière et judiciaire, les relations extérieures, la sécurité et la défense, la protection des institutions européennes contre d'éventuelles attaques

[105] *Rapport - Algorithmes : prévenir l'automatisation des discriminations*, Défenseur des droits, mai 2020
[106] *ibidem*.
[107] *ibidem*
[108] *Rapport - Technologies d'identification biométrique à distance dans l'espace public : enjeux et recommandations*, Défenseur des droits, février 2022
[109] *Op., cit.*, n° 103, p. 49.
[110] *ibid.* n°109, p. 49

informatiques entre autres. Concernant la « *boîte à outil cyberdiplomatique* »[111] de l'UE qui prévoit des sanctions en cas d'actes de cyber-malveillance, la France a agi en faveur de son adoption par l'ensemble des Etats membres, et pour sa mise en œuvre.

La France œuvre par ailleurs à renforcer le dialogue avec les acteurs du secteur privé et de la société civile en matière de cybersécurité, notamment avec l'organisation du Forum *InCyber Europe* (auparavant Forum international de la cybersécurité), événement majeur européen dans ce domaine. La France participe également au Forum de l'Union européenne sur l'Internet, dont l'objectif est d'aligner les positions européennes en matière de cybersécurité.

La France est également particulièrement active sur les questions de lutte contre le terrorisme au niveau de l'UE. Elle a été notamment engagée dans les discussions relatives à l'élaboration du *règlement européen relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne*[112], et participe activement au Forum de l'Union européenne sur l'internet, qui réunit les États membres, les entreprises technologiques et la société civile pour échanger sur les bonnes pratiques et renforcer la coopération dans la lutte contre la radicalisation en ligne.

[111] *Op. cit.* n°76, p. 38
[112] *Op. cit.* n°83 p. 40

PARTIE II. ILLUSTRATIONS DE THÉMATIQUES SPÉCIFIQUES DANS LA DIPLOMATIE NUMÉRIQUE DE LA FRANCE

La diplomatie française, en matière de régulation de l'internet et de droits fondamentaux, doit être analysée en comparaison avec celles exercées par les autres pays à l'échelle internationale. Afin d'illustrer la position de la France, notre étude s'articule autour de plusieurs axes clés, reconnus comme des thématiques stratégiques dans le domaine du numérique. L'intelligence artificielle est un point stratégique pour l'avenir qui soulève de nombreux défis éthiques. La France entend répondre à ces enjeux en incarnant un modèle qui tend vers un respect des principes juridiques fondamentaux en matière d'IA et de données personnelles (Chapitre I). La protection de certaines catégories de personnes, notamment des populations vulnérables, face aux risques spécifiques induits par le numérique représente une priorité majeure qui devra s'inscrire dans un effort international visant à définir des normes adaptées à ces risques particuliers (Chapitre II). Enfin, l'engagement de la France à garantir la sécurité de l'espace numérique, à en assurer l'ouverture, ainsi qu'à promouvoir la liberté d'expression en ligne sont des éléments fondamentaux au cœur des débats diplomatiques (Chapitre III).

Chapitre I. Les enjeux liés à l'intelligence artificielle

La France opte pour une position intermédiaire et nuancée. Elle souhaite utiliser une IA respectueuse des droits de l'Homme dans la course mondiale à l'acquisition d'une intelligence artificielle toujours plus performante mais tend parfois à sous-estimer les questions de biais algorithmique et d'éthique qui en résultent. Son approche met en lumière les avantages et les défis de l'IA dans les systèmes du service publics (I) ainsi que les difficultés liées à la protection des données personnelles (II).

I. La position de la France sur les droits de l'homme dans la course mondiale à l'acquisition d'une Intelligence Artificielle toujours plus performante

Par nature, l'intelligence artificielle est devenue un outil stratégique de diplomatie à travers le monde (A). La France, pour sa part, mobilise cette IA au service de son service

public, notamment à travers son intégration dans les dispositifs de vidéosurveillance, de sécurité intérieure et de lutte contre le terrorisme. Cette utilisation soulève toutefois des enjeux juridiques et éthiques importants, notamment en matière de respect des droits fondamentaux (B).

A) Intelligence artificielle : un outil diplomatique

Si la France ambitionne de prendre part à la course mondiale à l'intelligence artificielle, elle continue néanmoins de s'interroger sur les réelles possibilités de développement et sur les moyens suffisants pour concevoir une IA de confiance (1). Ses actions dans ce domaine traduisent une volonté d'allier performance technologique, souveraineté numérique et respect des valeurs fondamentales (2).

1. L'ambition de la France pour l'IA et la définition d'une IA « digne de confiance »

La France a pour ambition de jouer un rôle de premier plan dans la compétition mondiale autour de l'IA, comme en témoigne l'organisation du Sommet International sur l'IA du 10 au 11 février 2025 à l'initiative du président de la République et dans la continuité des Sommets de Bletchley Park de novembre 2023 au Royaume-Uni et de Séoul de mai 2024 en Corée du Sud. Ce sommet avait pour ambition de valoriser le savoir-faire des acteurs de l'IA en Europe, promouvoir une utilisation de cette technologie au service de l'intérêt général et de rassembler, sous une co-présidence franco-indienne, de nombreux partenaires internationaux autour de cette vision commune. Le Sommet pour l'action sur l'IA a pu aborder cinq thématiques de travail : l'IA au service de l'intérêt public, l'innovation et la culture, l'IA de confiance, la gouvernance mondiale de l'IA et l'avenir du travail.

Concernant le thème de l'IA au service de l'intérêt public, une Fondation globale pour l'IA sera mise en place, rassemblant 6 pays fondateurs. La fondation financera et apportera son soutien à des projets portant sur l'IA au service de l'intérêt public. Dans cette course aux technologies, les droits de l'Homme occupent-ils réellement une place centrale dans les débats, ou sont-ils relégués au second plan ? Le dimanche 9 février, lors de l'émission

« 20h30 le dimanche »[113] sur France 2 à la veille de l'ouverture du Sommet international, le président de la République s'est exprimé sur les enjeux de l'intelligence artificielle : « *C'est à nous de mettre cette IA au service de l'humain et nous avons tout pour réussir* ». Face à l'évolution rapide de l'IA, de nombreuses inquiétudes émergent sur la liberté de pensée et de conscience, l'émergence d'une politique de désinformation, les violations des droits d'auteur ou du droit de la propriété intellectuelle notamment. Le président a insisté sur la nécessité d'« *une régulation mondiale* [et] *des partenariats entre les acteurs privés et publiques afin que les bon comportements émergent* ». Dans cette perspective, une « déclaration sur une intelligence artificielle inclusive et durable pour les peuples et la planète » a été signée par 63 pays ainsi que l'Union européenne lors du sommet. Le second paragraphe de cette déclaration appelle à « *une approche inclusive ouverte et multipartite qui permettra à l'IA d'être éthique, sûre, sécurisée, digne de confiance et axée sur les droits de l'Homme et sur l'humain* ». Enfin, les Etats reconnaissent au quatrième alinéa la nécessité d'un dialogue pluripartite inclusif mené dans le respect de « *la protection des droits de l'Homme* ». Ainsi la France confirme-t-elle son engagement en matière d'IA et participera au Sommet de Kigali, le 3e Forum mondial sur l'éthique de l'IA qui sera organisé par la Thaïlande et l'UNESCO, ainsi qu'à la Conférence mondiale sur l'IA en 2025 et le Sommet mondial de 2025 sur l'IA au service du bien social.

Le groupe d'experts de haut niveau sur l'intelligence artificielle (GEHN IA) a publié des *lignes directrices en matière d'éthique pour une IA digne de confiance*[114]. Une IA "digne de confiance" présente les trois caractéristiques : être licite, éthique et robuste. Elle doit assurer le respect des législations et réglementations applicables, l'adhésion à des principes et valeurs éthiques et garantir une fiabilité tant technique que sociale. En effet, même avec de bonnes intentions, les systèmes d'IA peuvent causer des préjudices involontaires. En France, l'ambassadeur du numérique s'interroge sur la question de l'existence d'une réelle IA digne de confiance et s'appuie sur les écrits de la philosophe Anne Alombert pour étayer ses propos. Cette dernière a pu écrire dans son ouvrage « La crise de l'esprit, à l'ère des nouvelles technologie » que :

[113] MACRON E., *Discours d'ouverture du sommet sur l'intelligence artificielle à Paris*, YouTube, 21 mai 2024. Lien : https://www.youtube.com/watch?v=YSfAwQDQuHQ

[114] *Lignes directrices en matière d'éthique pour une IA digne de confiance,* Groupe d'experts indépendants de haut niveau sur l'intelligence artificielle, Commission européenne, juin 2018

> « *les "progrès" des machines apprenantes ou intelligentes semblent ainsi coïncider avec la destruction progressive des facultés de penser, par une industrie numérique qui fait des énergies psychiques sa première source de profit économique* »[115].

Cette réflexion soulève une interrogation essentielle quant à la place des droits de l'Homme dans l'action publique. Est-il possible d'inscrire la diplomatie numérique française en matière d'intelligence artificielle dans une approche pleinement respectueuse des droits fondamentaux, tant sur le plan national qu'international ?

2. Les actions de la France dans le domaine de l'IA

La France participe activement aux travaux du Conseil de l'Europe au sein du Comité ad hoc sur l'intelligence artificielle (CAHAI), afin de contribuer à l'élaboration d'un dispositif juridique conforme aux principes de l'État de droit.

Sur le plan onusien, la France codirige avec la Finlande les réflexions en cours sur la gouvernance numérique, en particulier dans la perspective de recommandations concrètes à l'échelle globale. En effet, dans la ligne du rapport final du groupe de haut niveau des Nations Unies sur la coopération numérique, la France et la Finlande ont été désignées comme « co-champions » et pilotent les consultations thématiques en cours en vue de recommandations concrètes sur la recommandation 3C (IA) de 2020[116]. A ce sujet, la France a rendu des *recommandations de sécurité pour un système d'IA générative*[117] produite par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Sa première recommandation est d'intégrer la sécurité dans le système d'IA afin de prévenir les risques de violation des droits, notamment du droit à la vie privée.

Enfin, un dialogue constant avec les principaux acteurs du numérique vient compléter cette diplomatie, notamment sur les enjeux liés à la régulation des contenus, à la désinformation et à la protection des données personnelles. La CNIL a réuni 60 partenaires issus de secteurs

---

[115] ALOMBERT, A., *Schizophrénie numérique : La crise de l'esprit, à l'ère des nouvelles technologies*, Editions Allia, 2024

[116] *Recommandation 3C – Promouvoir une gouvernance éthique de l'intelligence artificielle au sein du système des Nations Unies*, Groupe de haut niveau sur la coopération numérique, *L'ère de l'interdépendance numérique* (rapport présenté par le Secrétaire général de l'ONU), 2020

[117] *Recommandations de sécurité pour un système d'IA générative*, ANSSI, 2024. Lien : Recommandations_de_sécurité_pour_un_système_d_IA_générative.pdf

variés afin d'engager une réflexion sur l'éthique des algorithmes et de l'intelligence artificielle. Ils ont organisé 45 évènements entre mars et octobre 2017, en France et à l'étranger réunissant près de 3000 participants. La CNIL a coordonné cette démarche afin de favoriser une réflexion collective, pluraliste et accessible, inscrite dans une dynamique civique et démocratique. Cette étude a conduit à l'élaboration d'un rapport qui présente que si 83% des français[118] ont déjà entendu parler des algorithmes, plus de la moitié affirme ne pas savoir précisément de quoi il s'agit.

Le président Emmanuel Macron a annoncé 109 milliards d'euros d'investissements « *privés français et étrangers* »[119] en matière d'IA « *pour les prochaines années* »[120]. A l'image des Emirats-Arabes-Unis, qui prévoient la construction d'un centre de données géant pour un montant estimé entre 30 et 50 milliard d'euros[121], en France, l'entreprise Mistral AI prévoit d'investir à hauteur de plusieurs milliards d'euros dans la création d'un data center dans le département de l'Essonne. Or, ces infrastructures nécessitent d'énormes quantités d'énergie et de ressources, alimentant une empreinte carbone considérable et une consommation en eau massive. À cette pression écologique s'ajoute le risque de violations indirectes des droits de l'homme, notamment en lien avec les populations affectées par l'exploitation des ressources, le déplacement des communautés ou les effets du dérèglement climatique aggravés par ces projets.

La France n'est pas le seul pays à décider d'investir massivement dans l'IA. Lors d'une conférence de presse à Pékin, le 6 mars 2025, le président de la Commission nationale chinoise du développement et de la réforme a annoncé que le « fonds d'orientation du capital-risque d'Etat » allait se concentrer sur des domaines de pointe tels que l'IA. Ce fonds devrait s'élever à près de 138 milliards de dollars de capitaux sur 20 ans[122] de la part des gouvernements locaux et du secteur privé. La Chine considère que l'IA est essentielle afin de stimuler la croissance économique et moderniser l'industrie manufacturière. Par ailleurs,

---

[118] *Garder la main : rapport sur la maîtrise des algorithmes et de l'intelligence artificielle*, CNIL, 2023. Lien : https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_rapport_garder_la_main_web.pdf

[119] *« Intelligence artificielle : Emmanuel Macron annonce des investissements en France de 109 milliards d'euros dans les prochaines années »* , Le Monde, 9 février 2025, Lien : Lien : https://www.lemonde.fr/pixels/article/2025/02/09/intelligence-artificielle-emmanuel-macron-annonce-des-investissements-en-france-de-109-milliards-d-euros-dans-les-prochaines-annees_6539115_4408996.html

[120] *Ibidem*

[121] *« Sommet de l'IA à Paris : d'où proviendront les 1,09 milliard d'euros promis par Emmanuel Macron ? »,* Europe 1, 21 mai 2024, Lien : https://www.europe1.fr/technologies/sommet-de-lia-a-paris-dou-proviendront-les-109-milliards-deuros-promis-par-emmanuel-macron-302162

[122] GAN N., LIU J., *« China announces high-tech fund to grow AI, emerging industries »,*CNN, 10 mars 2025. Lien : https://edition.cnn.com/2025/03/06/tech/china-state-venture-capital-guidance-fund-intl-hnk/index.html

l'Australie a publié son plan d'action sur l'IA, qui définit quatre domaines d'intervention dont le fait de veiller à l'utilisation de technologies d'IA responsable, inclusives et qui reflètent les valeurs australiennes. Il s'agit d'un plan voulant faire de l'Australie avant tout un leader mondial dans le développement des systèmes d'IA. L'Australie investit 24,2 millions de dollars[123] prévu sur un durée de 4 à 6 ans dans le développement de l'IA visant par exemple à soutenir des partenariats public-privé pilotant des projets IA à impact économique et social ou à financer un programme de formation de spécialistes locaux en IA.

Lancé en octobre 2021 par le gouvernement français, le programme *France2030* constitue le principal levier politique d'investissement stratégique de l'Etat dans les secteurs technologiques et scientifiques d'avenir. Doté d'une enveloppe globale de 54 milliards d'euros, ce programme ambitionne de répondre aux défis contemporains majeurs. Dans ce cadre, 3 milliards d'euros sont spécifiquement affectés à 43 programmes et équipements de recherche prioritaires (PEPR). Il s'agit de construire ou consolider l'excellence française dans des domaines scientifiques prioritaires au niveau national ou européen, et notamment l'intelligence artificielle et le numérique[124]. Le 16 juin 2023, le plan français de souveraineté numérique a par ailleurs alloué un budget public de 1,5 milliard[125], accompagné de 506 millions de cofinancements privés, pour une stratégie IA sur cinq ans. Ce montant doit aussi permettre l'émergence d'une IA de confiance : *« répondant à des normes de transparence et de confidentialité* ». La France cherche à consolider la présence d'au moins trois de ses établissements dans le Top 50 mondial des universités dans le champ de l'IA.

B) L'IA au service du service public et son utilisation dans la vidéosurveillance et la lutte contre le terrorisme

L'investissement de la France dans l'intelligence artificielle, ainsi que son plan d'action pour son déploiement au sein des services publics, traduisent une orientation stratégique de sa diplomatie (1). L'usage de l'IA et d'autres systèmes algorithmiques dans la prise de décision administrative reflète une volonté de moderniser l'action publique (2). Cela

---

[123] An action plan for artificial intelligence in Australia", Australian Government, 18 juin 2021. Lien : An action plan for artificial intelligence in Australia | Department of Industry Science and Resources

[124] *« Intelligence artificielle et numérique »*, Ministère de l'enseignement supérieur et de la recherche, 17 janvier 2023. Lien : https://www.enseignementsup-recherche.gouv.fr/fr/intelligence-artificielle-et-numerique-97624

[125] *« Souveraineté numérique : des moyens inédits pour soutenir les acteurs de l'IA »*, Ministère de l'économie, des finances et de la souveraineté industrielle et numérique, 16 juin 2023. Lien : https://www.economie.gouv.fr/souverainete-numerique-moyens-inedits-soutien-acteurs-IA

se manifeste notamment par le recours à la vidéosurveillance augmentée lors des Jeux olympiques et paralympiques de 2024, ou encore par diverses mesures de lutte contre le terrorisme appuyées par des technologies d'IA. Toutefois, cette dynamique soulève des inquiétudes croissantes quant aux risques de dérives sécuritaires, à l'opacité des algorithmes et aux potentielles atteintes aux droits fondamentaux (3).

1. L'investissement et le plan d'action de l'utilisation de l'IA par la France au sein des services publics : éléments révélateurs de la diplomatie française

Le 5 mars 2024, la Commission de l'intelligence artificiel a remis son *rapport « Notre ambition pour la France »*[126]. Elle a présenté un plan d'action structuré autour de six axes et comprenant 25 recommandations dont la première est de « *créer les conditions d'une appropriation collective de l'IA et de ses enjeux* ». Elle prévoit un nouvel investissement public annuel de 5 milliards d'euros pendant cinq ans pour financer le secteur de l'IA. Ce plan souligne les risques d'utilisation malveillante ou systémique de l'IA et formule des propositions axées principalement sur la protection des droits d'auteur et de propriété intellectuelle.

En 2022, à la demande du Premier ministre, le Conseil d'Etat a publié une étude plaidant en faveur d'une stratégie de l'IA « de confiance » au service des services publics. Cette démarche s'inscrit pleinement en continuité des lignes directrices proposées par la Commission européenne. Cette dernière repose sur sept principes : « *la primauté humaine, la performance, l'équité et la non-discrimination, la transparence, la sûreté (cybersécurité), la soutenabilité environnementale et l'autonomie stratégique* »[127]. La France tient à adopter toutes les mesures nécessaires pour assurer une protection optimale des droits et libertés des citoyens à l'ère numérique.

[126] *Rapport - IA : notre ambition pour la France*, Commission de l'intelligence artificielle, mars 2024. Lien : https://www.info.gouv.fr/upload/media/content/0001/09/4d3cc456dd2f5b9d79ee75feea63b47f10d75158.pdf

[127] *Intelligence artificielle et action publique : construire la confiance, servir la performance*, Conseil d'État, 2022. Lien : https://www.conseil-etat.fr/publications-colloques/etudes/intelligence-artificielle-et-action-publique-construire-la-confiance-servir-la-performance

Enfin, le *plan France Relance*[128] dédie 908 millions d'euros[129] à la transformation numérique. Si 570 millions d'euros ont été investis seulement pour la généralisation de la fibre, seulement 250 millions se concentrent sur l'inclusion numérique et 88 millions à la modernisation des services publics des collectivités territoriales, une part de ce budget

prendra notamment la forme d'un « *recours croissant à l'IA* »[130].

L'IA s'immisce aussi dans le domaine de la santé. Si nous ne pourrons pas développer l'ensemble des préoccupations et l'application de la diplomatie française à ce sujet, il reste intéressant de noter que la France a participé aux débats de l'I-DAIR (International Digital health & AI Research collaborative) consacré à l'ouverture de données concernant la santé le 13 octobre 2020. De même, la France est présente auprès de la Commission d'étude 16, consacrée au multimédia et aux technologies numériques associées. Elle a achevé ses travaux et donné naissance à un Groupe spécialisé sur l'intelligence artificielle au service de la santé (FG-AI4H). Ce Groupe a été mis en place dans le cadre d'un partenariat entre l'UIT et l'Organisation mondiale de la santé (OMS). Son objectif principal est d'établir un cadre d'évaluation normalisé pour l'évaluation des méthodes fondées sur l'intelligence artificielle au service de la santé, du diagnostic, du triage ou des décisions relatives au traitement ; incluant des considérations sur les droits des personnes en situation de handicap.

2. <u>L'utilisation de l'IA et d'autres systèmes algorithmiques en matière de prise de décision administrative</u>

Les algorithmes sont largement utilisés en France et le Défenseur des droits a indiqué qu'un débat public était en cours sur l'utilisation des algorithmes dans le recrutement, le système judiciaire et le secteur de la santé. En France, les algorithmes sont utilisés pour lutter contre la fraude fiscale. Ils peuvent analyser diverses données, y compris des informations librement partagées par les individus sur les réseaux sociaux. Le Conseil constitutionnel a jugé conforme à la Constitution l'usage de ces algorithmes pour lutter contre la fraude fiscale, à condition que les données utilisées ne révèlent aucune information interdite, telle que

---

[128] *Plan de relance : les actions du ministère*, Ministère du Travail, du Plein emploi et de l'Insertion, 2024. Lien : https://travail-emploi.gouv.fr/le-ministere-en-action/relance-activite/

[129] *« IA : quel potentiel et quels risques dans les services publics ? »,* Vie publique, 2024. Lien : https://www.vie-publique.fr/parole-dexpert/293547-ia-quel-potentiel-et-quels-risques-dans-les-services-publics Vie Publique

[130] *ibid.* n°129, p.58

l'origine ethnique, le genre, l'orientation sexuelle, les opinions politiques ou religieuses, ou encore les informations génétiques et biométriques.

Par ailleurs, la France tente d'utiliser l'intelligence artificielle dans ses algorithmes notamment dans les systèmes ADM et IA qui désignent des outils technologiques capables d'émettre ou de soutenir des décisions relevant normalement de l'autorité humaine. Ces systèmes soulèvent des questions de transparence, de responsabilité et de respect des droits fondamentaux, notamment lorsque leurs décisions ont des effets juridiques ou individuels. Par décision du 30 décembre 2021, le Conseil d'Etat avait validé le décret relatif au projet *Datajust*, un modèle d'IA dont l'algorithme était destiné à exploiter les données issues des décisions juridictionnelles en matière d'indemnisation des préjudices corporels. La haute juridiction a jugé que ce dispositif ne portait atteinte ni à la loi n°78-7 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ni aux garanties fondamentales des libertés publiques. Le décret se limitait à encadrer une collecte de données juridictionnelles à des fins de recherche, sans effet normatif. L'objectif poursuivi, consistant à renforcer l'accessibilité, la lisibilité et la prévisibilité du droit par l'analyse jurisprudentielle, a été reconnu comme légitime et suffisamment encadré au regard de la finalité poursuivie. Toutefois, le ministère de la Justice a renoncé à ce projet. Si les difficultés techniques sont en cause, des résistances corporatistes surgissent. Ce projet naît sans aucune garantie législative, sans discussion parlementaire et en pleine période de confinement lié à l'épidémie de COVID-19. Selon Vincent Rivollier, enseignant-chercheur en droit privé, cet abandon traduit avant tout "*un désengagement du ministère sur les questions numériques, l'intervention publique se limitant à la mise à disposition de données et à l'encouragement des initiatives privées*"[131]. En 2023, suite au décès du jeune Nahel de 17 ans, Ravina Shamdasani, porte-parole du Haut-commissaire aux droits de l'homme avec déclaré que la France devait « *s'attaquer sérieusement aux problèmes profonds du racisme et de la discrimination dans les forces de police* ». Cette problématique est aussi rappelée par le Comité des droits de l'homme. Au regard de ces constats, les inquiétudes qui naissent d'une future utilisation accrue de l'IA dans les décisions administratives françaises semblent justifiées et légitimes.

EQUINET rappelle dans son rapport qu'"*en France, le principe de non-discrimination, consacré à plusieurs reprises par la jurisprudence du Conseil constitutionnel et du Conseil*

[131]RIVOLLIER V., *Datajust. Histoire d'un échec,* Séminaire Nouvelles technologies et justice, Centre internet et société, Mars 2023, Lien : Datejust. Histoire d'un échec - Archive ouverte HAL

d'État[132]*, s'applique à toute décision administrative, et a fortiori aux décisions algorithmiques*"[133]. Parmi les garanties adoptées en France au moment de l'ouverture à la prise de décisions administratives individuelles entièrement automatisées, l'interdiction d'en prendre sur le fondement de traitement de données personnelles dites « sensibles » a été posée comme permettant en partie de lutter contre d'éventuelles discriminations[134].

L'approche mesurée du contrôle juridictionnel s'aligne sur l'équilibre défini par la diplomatie française, qui promeut un développement de l'intelligence artificielle compétitif tout en affirmant, sur la scène internationale, la nécessité d'un encadrement éthique. Dans sa décision du 18 juin 2020[135], le Conseil constitutionnel a affirmé qu'une décision administrative individuelle ne pouvait pas être prise exclusivement sur la base d'un traitement entièrement automatisé sans intervention humaine. Par ailleurs, une affaire importante a marqué l'évolution jurisprudentielle française en matière l'utilisation d'algorithmes mais cette dernière ne reposait pas sur de l'IA. Dans sa décision du 3 avril 2020, relative à une Question Prioritaire de Constitutionnalité (QPC), le Conseil constitutionnel a recommandé aux établissements universitaires de publier les critères en fonction desquels les dossiers de candidatures sont traités. Le Conseil a également précisé que rien n'impose la divulgation des paramètres exacts des algorithmes utilisés. La France n'est pas le seul pays à s'intéresser à ces nouvelles technologies.

Plusieurs pays européens commencent à utiliser ou envisage l'utilisation de l'intelligence artificielle dans le domaine judiciaire et pénal, parmi eux figurent l'Italie, les Pays-Bas, la Pologne, l'Espagne et le Royaume-Uni[136]. Dans le contexte de la prise de décision administrative, les systèmes de décision automatisée (ADM) et l'intelligence artificielle (IA) suscitent des réflexions juridiques inégales au sein des États membres. Alors que certains pays restent silencieux sur ces enjeux, d'autres reconnaissent l'existence de débats nationaux, mettant en lumière la diversité des approches et des préoccupations. En France, les développements liés à l'IA sont bien identifiés comme porteurs d'enjeux juridiques, notamment en matière de protection des données et de libertés publiques. Toutefois, aucun

[132] Conseil d'État (France) 22 mai 2013, n° 351183, Lien :https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2013-05-22/351183.

[133] *Étude comparative portant sur le droit administratif et l'utilisation de l'IA et d'autres systèmes algorithmiques en matière de prise de décision administrative dans les États membres du Conseil de l'Europe* (Point 5.5 du projet d'ordre du jour), Comité européen de coopération juridique (CDCJ), 99e réunion, 23-25 novembre 2022

[134] *Étude d'impact, Projet de loi relatif à la protection des données personnelles*, Assemblée nationale, 12 décembre 2017,p.64.

[135] Conseil constitutionnel, Décision n° 2020-840 QPC, 20 mai 2020

[136] *Op., cit.* n° 103, p. 49.

débat majeur n'a encore émergé quant à une éventuelle inadaptation du droit administratif aux spécificités de ces technologies, ce qui pourrait laisser penser que la prise de conscience des risques potentiels reste limitée dans ce domaine.

Concernant la stratégie étatique de l'Etat au sujet de l'intelligence artificielle, Ophélie COELHO, chercheuse et spécialiste de la géopolitique du numérique affirme qu'il faudrait « *revenir à la première couche de dépendance pour bâtir des logiciels d'intelligence artificielle qui soient maîtrisable*s»[137].

3. La vidéosurveillance augmentée lors des jeux olympiques et paralympiques de 2024 et les autres mesures de lutte anti-terroriste en lien avec l'IA

L'intelligence artificielle est aussi utilisée pour la reconnaissance faciale (FRT). Elle permet essentiellement d'analyser les images et la correspondances des visages avec des bases de données déjà existantes. En France, la FRT a été testée à titre expérimental dans deux lycées de la ville de Nice. Cette utilisation de la FRT a été examinée par la CNIL (Commission nationale de l'informatique et des libertés) qui a rendu un avis jugeant que ce système n'était ni nécessaire ni proportionné à cet objectif. Dans une partie essentielle de sa décision, la CNIL a conclu :

> « *...les dispositifs de reconnaissance faciale sont particulièrement intrusifs et présentent des risques majeurs d'atteinte à la vie privée et aux libertés individuelles des personnes concernées. Ils sont également susceptibles de créer un sentiment de surveillance accrue. Ces risques sont renforcés lorsqu'ils sont appliqués à des mineurs, qui font l'objet d'une protection particulière dans les textes nationaux et européens.* »

Un tel dispositif ne peut donc être légalement mis en œuvre. Il avait également été annoncé que la France comptait utiliser un système de reconnaissance faciale appelé « Alicem » afin de créer une identité numérique permettant aux citoyens d'accéder aux services publics en ligne. Cette annonce a suscité la controverse, menant à une déclaration du gouvernement français en octobre selon laquelle une révision de l'usage de la FRT était en cours[138].

---

[137] Séminaire Diplomatie numérique, Déclaration d'intervenant, CNCDH, Sous-commission D, 22 novembre 2024 (CONFIDENTIEL).
[138] *Op. cit.* n°86, p. 45

En matière de sécurité publique, la vidéosurveillance assistée par l'IA a été autorisée par le législateur dans le cadre de la loi sur les jeux olympiques et paralympique de 2024 afin de faciliter la détection des évènements anormaux dans l'espace public. Si le gouvernement avait annoncé que ce déploiement était exceptionnel et ne s'appliquerait que durant la période des jeux, la France a finalement décidé en 2025, en contradiction avec sa ligne diplomatique, de prolonger la vidéosurveillance jusqu'en 2027.

Or le simple déploiement de technologie biométrique d'identification et d'évaluation à distance sur la voie publique, va tout d'abord à l'encontre du droit des enfants, voire il représente un risque d'atteinte grave pour ces derniers. Ces technologies sont contraires à l'encadrement rigoureux des données personnelles des enfants par le RGPD et la loi informatique et Libertés. Ces violations concordent avec l'inquiétude des français. En effet, plus d'un tiers considère que les enjeux liés aux technologies biométriques sont mal pris en compte par les pouvoirs publics[139]. Dans une lettre du 14 février 2023, le président de la CNCDH alertait les parlementaires sur ces nouvelles mesures. Le caractère particulièrement intrusif de l'autorisation des scanners corporels suscitait de fortes inquiétudes et la CNCDH a pu conclure que cette expérimentation paraissait prématurée et trop aléatoire par rapport aux libertés fondamentales. En appui de ces constatations, la CNCDH avait publié un avis[140] comprenant plusieurs recommandations dont celle de renforcer le contrôle en amont de l'installation ainsi que sur le fonctionnement des dispositifs de vidéosurveillance. En outre, elle reprochait une absence d'information claire pour les citoyens et un manque de sensibilisation aux enjeux liés aux droits fondamentaux de l'usage de dispositifs de surveillance. En décembre 2020, des experts indépendants de l'ONU avaient demandé à la France de revoir le projet de *loi sur la sécurité globale*[141], estimant qu'il n'était pas conforme aux droits de l'homme. Ils ont notamment critiqué l'article 22, qui autorisait l'utilisation de drones de surveillance, craignant une extension de la surveillance, en particulier des manifestants, et une limitation du travail des médias. En effet, cette proposition de loi mettait en danger l'anonymat dans l'espace public en permettant une forme de surveillance généralisée qui avait été rappelée par le défenseur des droits dans son avis du 17 novembre 2020.

---

[139] *Enquête sur la perception du développement des technologies biométriques en France*, Défenseur des droits, octobre 2022

[140] *Avis sur l'usage de la vidéosurveillance et le respect des droits fondamentaux*, CNCDH, 20 juin 2023

[141] *Loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés*

La France n'est pas le seul Etat à utiliser la technologie de la reconnaissance faciale et d'autres formes d'identification biométrique. Elle est actuellement utilisée aussi par les autorités publiques d'Italie de Suède et du Royaume-Uni[142]. Le 12 juillet 2023, Volker TURK, Haut-Commissaire des Nations Unies aux droits de l'homme, alerte sur l'utilisation des systèmes de reconnaissance faciale et les systèmes d'IA utilisés dans le système de justice pénale. Il demande aux gouvernements et aux entreprises « *d'agir d'urgence* »[143]. Dans un rapport présenté à la 52e session du Conseil des droits de l'homme, la Rapporteuse spéciale des Nations Unies sur la promotion et la protection des droits de l'homme dans la lutte antiterroriste, Fionnuala Ní Aoláin, a mis en garde contre une « *augmentation alarmante de l'utilisation de technologies intrusives et à haut risque* »[144] et insiste sur l'idée qu'« *il faut faire une pause dans l'utilisation des technologies intrusives à haut risque jusqu'à ce que des garanties adéquates soient mises en place* ». Au même moment, l'ONU demande un moratoire sur certains systèmes d'IA. Michelle BACHELET déclare que « *Les technologies d'intelligence artificielle peuvent avoir des effets négatifs, voire catastrophiques si elles sont utilisées sans prendre suffisamment en compte la manière dont elles affectent les droits humains*»[145]. L'ONU recense déjà de nombreux cas de personnes « *traitées injustement à cause de l'IA*»[146].

Dans ses observations finales (*CCPR/C/FRA/CO/6*), le Comité des droits de l'homme des Nations unies exprime sa préoccupation concernant les mesures de police administrative visant à prévenir des actes terroristes introduites par la la *loi n° 2017-1510 du 30 octobre 2017*[147] dite « loi SILT » et pérennisées par la loi du 30 juillet 2021. Le Comité regrette que l'Etat ne recense pas dans ses statistiques les effets potentiels de ces mesures. Il souligne notamment le risque d'une application disproportionnée de ces mesures à l'encontre de personnes de confession musulmane ou perçues comme telles ou d'origine étrangère. Le

---

[142] *Op., cit.,* n°103, p. 49.
[143] TÜRK V., *« Artificial intelligence must be grounded in human rights, says High Commissioner »,* discours prononcé lors d'une manifestation parallèle à la cinquante-troisième session du Conseil des droits de l'homme, 12 juillet 2023. Lien : https://www.ohchr.org/fr/statements/2023/07/artificial-intelligence-must-be-grounded-human-rights-says-high-commissioner
[144] *« Une experte de l'ONU dénonce le détournement des technologies de surveillance antiterroristes »*, *ONU Info,* 3 mars 2023. Lien : https://news.un.org/fr/story/2023/03/1133232
[145] Communiqué de presse, « *L'intelligence artificielle menace la vie privée : Bachelet appelle à une réglementation urgente »*, Haut-Commissariat aux droits de l'Homme, 15 septembre 2021, Lien : https://www.ohchr.org/fr/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet
[146] *« L'ONU appelle à un encadrement plus strict des technologies numériques afin de protéger les droits humains »,* ONU Info, 15 septembre 2021. Lien : https://news.un.org/fr/story/2021/09/1103762
[147] *Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme*

Comité se dit également « *préoccupé* » [148] du fait que le recours au droit administratif et aux mécanismes de contrôle n'offre pas de garanties suffisantes aux suspects, y compris le droit à un procès équitable, en contradiction avec l'article 14 du *Pacte relatifs aux droits civils et politiques*. L'organisation non gouvernementale Human Rights Watch s'était indignée au sujet de la loi sur le renseignement proposée par la France. Cette dernière permettant de procéder à des opérations de surveillance numérique de grande envergure en violation du droit de la vie privée visé à l'article 17 de la CEDH[149]. Cette loi permettait au Premier ministre d'autoriser la surveillance pour des motifs très généraux, allant bien au-delà de ceux reconnus en droit international des droits de l'Homme, et ce sans aucune intervention des autorités judiciaires. En vertu de l'article 1 du projet de loi, ces motifs incluent la prévention du terrorisme ainsi que « *les intérêts économiques, industriels et scientifiques majeurs de la France* », la prévention des « *atteintes à la forme républicaine des institutions* » et les violences collectives de nature à porter atteinte à la sécurité nationale. L'article 20 entré en vigueur le 1er janvier 2015 de la *loi n° 2013-1168 relative à la programmation militaire*[150] pour les années 2014 à 2019, autorise la surveillance administrative des communications électroniques sans contrôle juridictionnel préalable. Cette disposition permet aux agents habilités de plusieurs ministères de requérir auprès des opérateurs de communications électroniques et hébergeurs l'accès à des données de connexion, sur des fondements larges tels que la sécurité nationale, la protection du potentiel scientifique et économique ou la lutte contre le terrorisme. L'absence de contrôle judiciaire et la portée extensive des motifs invoqués soulèvent des interrogations quant à la conformité de ce dispositif avec l'article 17 du Pacte international relatif aux droits civils et politiques, relatif à la protection contre les ingérences arbitraires dans la vie privée.

II. La gestion des données personnelles à l'ère du numérique

La France accorde une réelle importance à la protection des données personnelles, mais elle doit encore renforcer sa posture d'innovation pour répondre aux défis technologiques actuels (A). Or, dans un contexte où la surveillance numérique tend

[148] *Observations finales concernant le sixième rapport périodique de la France*, Comité des droits de l'Homme (ONU), CCPR/C/FRA/CO/6, 4 novembre 2024

[149] *« Préoccupations et recommandations de Human Rights Watch sur la France »,* Human Rights Watch, 22 juin 2015. Lien : https://www.hrw.org/fr/news/2015/06/22/preoccupations-et-recommandations-de-human-rights-watch-sur-la-france

[150] *Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*

inévitablement à empiéter sur le droit au respect de la vie privée, cette conciliation entre sécurité et libertés demeure particulièrement délicate (B).

A) La France accorde de l'importance au respect de la protection des données personnelles mais doit davantage s'inscrire dans une posture d'innovation

L'un des défis majeurs du XXIe siècle tient à la nature même des données d'entraînement qui « nourrissent » l'IA dans son apprentissage. Selon la Commission nationale consultative sur l'intelligence artificielle, la notion même de données personnelles, clé de voûte du règlement européen en la matière (RGPD), pose question, dans la mesure où l'IA utilise de façon croissante des données collectives. La commission souligne l'importance d'une approche plus moderne de la donnée « *en conjuguant mieux protection et innovation* », pour « *accroître l'effectivité de la garantie des droits de chacun* ». Dans son rapport « Notre ambition pour la France», la commission propose de réformer le mandat de la Commission nationale informatique et libertés (CNIL), pour l'orienter vers une posture plus proactive en matière d'innovation.[151]

Par ailleurs, la CNIL, autorité administrative indépendante joue un rôle central dans la régulation des données personnelles. Elle veille au respect des droits fondamentaux dans le traitement des données à caractère personnel et participe activement à l'élaboration des normes éthiques encadrant l'usage du numérique. Sur la scène internationale et européen, la CNIL représente la France au sein du Comité européen de la protection des données (EDPB) où elle contribue à l'interprétation du *Règlement général sur la protection des données* (RGPD). La CNIL collabore avec ses homologues dans le cadre de l'Assemblée mondiale pour la protection de la vie privée (*Global Privacy Assembly*) afin de promouvoir un cadre commun de protection des droits à l'ère du numérique. Cette assemblée, qui rassemble toutes les autorités de protection des données dont la CNIL, a décidé de se mobiliser pour renforcer les capacités de coopération internationale afin d'établir des principes pour encadrer la reconnaissance faciale. La CNIL traduit sur le plan opérationnel les engagements de la France en faveur d'un numérique respectueux des droits de l'homme, contribuant à faire rayonner ses principes dans la régulations.

---

[151] « *Intelligence artificielle : 25 propositions pour une stratégie française* », 2024. Vie publique, Lien : https://www.vie-publique.fr/en-bref/293421-intelligence-artificielle-25-propositions-pour-une-strategie-francaise

La diplomatie du numérique française doit s'inscrire dans une perspective plus large en s'alignant sur les principes de la *Déclaration de Toronto* et de l'Institut AI Now. Afin de sécuriser et de mieux protéger les données personnelles, des études d'impact doivent être menées régulièrement avant toute adjudication : « *pendant la phase de développement, puis à intervalles réguliers tout au long du déploiement et de l'utilisation afin d'identifier les sources potentielles de résultats discriminatoires ou portant atteinte aux droits fondamentaux* ». Ces études permettraient d'évaluer la conception des algorithmes, les processus de contrôle ou le traitement des données. L'institut AI Now a présenté un *cadre pratique pour l'évaluation de l'impact des algorithmes par les organismes publics*[152]. Ce cadre s'aligne avec l'article 35 du *règlement général sur la protection des données de l'UE*, qui prévoit l'obligation de mener une analyse d'impact relative à la protection des données, et l'article 25 qui exige l'intégration de la protection des données dès la conception et par défaut, tout au long du cycle de la vie du système. Ces exigences visent à prévenir les biais algorithmiques, souvent causés par des jeux de données obsolètes, partiels ou discriminants, et à garantir la transparence des décisions automatisées.

La France accorde une plus grande importance aux sujets de l'utilisation ADM/IA et aux questions de respect de la vie privée et de protection des données[153]. Cette dynamique est similaire à celle de la Suisse, mais se différencie de celle adoptée par la République Tchèque et la Lituanie. En effet, ces derniers s'intéressent à l'applicabilité des décisions administratives fondées sur l'IA. Selon la Commission de l'intelligence artificielle, certaines règles et pratiques françaises sont plus contraignantes et plus protectrices que le cadre européen en matière de traitement de données personnelles. Cependant, en mars 2025, le député Emmanuel Maurel dénonçait à l'Assemblée nationale la décision de la CNIL d'autoriser le transfert massif de données de santé vers des serveurs Microsoft dans le cadre du projet européen Darwin EU, soulevant des inquiétudes légitimes sur la souveraineté numérique et la sécurité des données sensibles :

> *« le 11 mars dernier la CNIL, Commission Nationale de l'Informatique et des Libertés, a donné son feu vert pour un programme européen de recherche qui s'appelle Darwin EU qui prévoit de transférer les données de santé de 10 millions de français qui seront hébergées par l'entreprise américaine Microsoft. A l'heure où*

[152]DILLON R., SCHULTZ J., CRAWFORD K. et WHITTAKER M., A*lgorithmic Impact Assessments Report : A Practical Framework for Public Agency Accountability*, AI Now Institute, 9 avril 2018

[153] *Op., cit.*, n°126, p. 56

même la Commission européenne envisage des mesures de rétorsion commerciale à l'encontre des entreprises numériques américaines. Comment peut-on confier des informations aussi sensibles à Microsoft ? ».

Cette controverse illustre le paradoxe entre une régulation française a priori plus protectrice que le droit européen, et certaines pratiques institutionnelles qui paraissent la contredire. Tandis que la France peine à développer des base de données protectrice de la vie privée, en Inde la base indienne Aadhaar a permis l'inclusion bancaire et l'identité numérique de centaines de millions de citoyens de manière plus sécurisée que la base française TESS.

Enfin, la CNIL a publié un bilan portant sur cinq années de 2018 à 2023[154] sur les violations de données. Sur cette période, 17 483 notifications de violation de données ont été reçues par la Commission nationale de l'informatique et des libertés. Ce nombre est en perpétuel croissance. Les violations de données concernent pour la plupart des cas de piratages, d'autres proviennent d'erreurs humaines. Le secteur public regroupe un grand nombre de cas. En effet, les administrations publiques concentrent 18,1% du nombre de déclarations de violations. La CNIL révèle dans son bilan que :

« Le secteur privé est à l'origine d'environ deux tiers des déclarations de violations à la CNIL dont 39% de PME. Le secteur public représente quant à lui 22% des notifications ».

B) Quand la surveillance numérique semble inévitablement mener à une violation de la vie privée (article 8 CEDH)

Le rapport du Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH)[155] a examiné les conséquences de la surveillance numérique généralisée des espaces publics, à la fois hors ligne et en ligne. Cette modernité n'est pas exempte de dérives et cette surveillance de masse peut conduire à compromettre les droits fondamentaux, notamment le droit à la vie privée mais aussi la liberté d'expression et la liberté de réunion. Dans son rapport, l'ONU décrit en détail comment des outils de surveillance tels que le logiciel «

[154] Commission nationale de l'informatique et des libertés (CNIL), *Infographies – Bilan 5 ans de violations de données*, Paris, CNIL, mars 2024 (mise en ligne 27 mars 2024), Lien : Infographies - Bilan 5 ans violations de données

[155] *Le droit à la vie privée à l'ère du numérique, A/HRC/51/17, Assemblée générale, Conseil des droits de l'homme,* Haut-Commissariat des Nations Unies aux droits de l'homme, 51e session 12 septembre–7 octobre 2022, Lien : https://undocs.org/fr/A/HRC/51/17

Pegasus » peuvent transformer la plupart des smartphones en « *dispositifs de surveillance 24 heures sur 24* ». De tels outils permettent ainsi à un individu mal intentionné d'accéder non seulement à tout ce qui se trouve sur les mobiles, mais aussi de prendre le contrôle de ces appareils pour espionner la vie de son utilisateur. Le rapport indique :

> « *Alors qu'ils sont prétendument déployés pour lutter contre le terrorisme et la criminalité, ces logiciels espions ont souvent été utilisés pour des raisons illégitimes, notamment pour réprimer les opinions critiques ou dissidentes et ceux qui les expriment, y compris les journalistes, les personnalités politiques de l'opposition et les défenseurs des droits de l'homme* ».

La France condamne fermement toute utilisation abusive des outils de surveillance numérique, en particulier lorsqu'ils portent atteinte aux droits fondamentaux. Par ailleurs, la CNCDH a alerté sur l'utilisation de logiciels espions comme Pegasus et Predator, soulignant les risques pour la vie privée et les libertés fondamentales. Si c'est logiciels sont utilisé par les Etats européens en 2021, ces derniers sont qualifiés d'« *extrêmement invasifs* » par une étude commandée par le département thématique des droits des citoyens et des affaires constitutionnelles du Parlement européen : « *Selon le Contrôleur européen de la protection des données, ces capacités 'ne sont vraisemblablement pas conformes aux exigences de proportionnalité» définies par la CJUE et la CEDH'* »[156]. Les autorités françaises ont elles aussi souligné ces dangers. Toute utilisation de ce type de logiciels doit faire l'objet d'une autorisation judiciaire préalable.

L'ONU alerte également sur l'extension préoccupante de la surveillance croissante dans les espaces publics eu égard à l'automatisation des traitements de données. En effet, « *la collecte et l'analyse automatisées des données à grande échelle* » surpasse les limites matérielles des anciennes pratiques. Si l'intrusion des Etats dans la sphère privée des individus était auparavant restreinte, les nouveaux systèmes d'identité numérisés et les vastes bases de données biométriques font peser un risque systémique sur les libertés individuelles dans un cadre de surveillance de plus en plus opaque et difficilement contrôlable.

Les nouvelles technologies ont également permis la surveillance systématique des publications en ligne, notamment par la collecte et l'analyse des messages sur les médias

---

[156] Parlement européen, Direction générale des politiques internes, *Synthèse exécutive – Étude pour la commission PEGA : Utilisation de Pegasus et de logiciels espions de surveillance équivalents. Cadre juridique des États membres en matière d'acquisition et d'utilisation de Pegasus et de logiciels espions de surveillance équivalents*, Bruxelles, Parlement européen, 2022, Lien : Utilisation de Pegasus et de logiciels espions de surveillance équivalents - Cadre juridique des États membres en matière d'acquisition et d'utilisation

sociaux. L'ONU dénonce le manque d'informations des gouvernements, dont la France, au sujet de leurs activités de surveillance : « *Même lorsque les outils de surveillance sont initialement mis en place à des fins légitimes, ils peuvent facilement être réaffectés, souvent à des fins pour lesquelles ils n'étaient pas initialement prévus* ». Dans ces conditions, l'ONU estime que les États devraient « *limiter les mesures de surveillance publique* » à celles qui sont « *strictement nécessaires et proportionnée*s »[157]. Par exemple, il est suggéré aux États de cibler avec précision les contextes géographiques et temporels dans lesquels les dispositifs de surveillance sont déployés. De plus, la conservation des données ne devrait s'étendre que sur une période strictement nécessaire. Enfin, l'ONU insiste sur une réduction immédiate du recours aux technologies de reconnaissance biométrique dans les lieux accessibles au public.

Dans ce contexte, alors même que la diplomatie française s'affiche activement dans les enceintes multilatérales comme promotrice d'un usage éthique et encadré des technologies de surveillance, certaines décisions internes traduisent un écart croissant entre la position internationale affichée et la réalité des politiques nationales en matière de sécurité. Ce décalage interroge la cohérence de la position française sur la scène mondiale, notamment dans sa capacité à conjuguer exigence de sécurité et respect des droits fondamentaux.

Chapitre II. Les enjeux liés à la protection de certaines catégories de personnes

Si la protection des droits de l'enfant est cruciale pour assurer l'intérêt supérieur de l'enfant dans l'environnement du numérique (I), l'accessibilité au numérique doit également être garantie (II).

I. La promotion et la protection primordiale de l'intérêt supérieur de l'enfant dans l'environnement numérique

[157] *Logiciels espions et surveillance : l'ONU met en garde contre les menaces croissantes pour la vie privée,* ONU Info, 16 septembre 2022. Lien : https://news.un.org/fr/story/2022/09/1127181

Les enfants sont des personnes vulnérables qui doivent être protégées des effets potentiellement néfastes des technologies (A), notamment par le biais des initiatives françaises (B).

A) Une protection nécessaire des enfants vulnérables face aux défis du numérique

Le principe de l'intérêt supérieur de l'enfant constitue une norme essentielle en droit international comme en droit interne. Il impose que toute décision concernant un enfant - qu'elle touche à sa vie familiale, à sa protection ou à son éducation - soit guidée en priorité par la recherche de son bien-être, de son épanouissement global et du respect de ses droits fondamentaux.

Ce concept trouve son origine dans le droit international, notamment dans la *CIDE*, adoptée en 1989. Son article 3 dispose que :

> *« Dans toutes les décisions, qu'elles soient prises par des institutions publiques ou privées, relatives aux enfants, l'intérêt supérieur de l'enfant doit être une considération primordiale.*[158] *»*

Ce principe a été repris et renforcé dans d'autres instruments internationaux, comme dans l'article 24§2 de la *Charte des droits fondamentaux de l'UE*, et il est désormais intégré dans les législations nationales de nombreux États, y compris la France. En France, bien que le Code civil ne définit pas explicitement l'expression « intérêt supérieur de l'enfant », il en reconnaît la primauté dans diverses situations juridiques. Ce principe est notamment utilisé par les juges aux affaires familiales pour guider leurs décisions, qu'elles concernent la garde des enfants, les mesures de protection ou l'adoption.

L'impact des technologies numériques sur les enfants est ambivalent : il offre à la fois des opportunités d'apprentissage et d'échange, tout en les exposant à des dangers et notamment du fait de leur vulnérabilité. En effet, à l'ère du numérique, il est essentiel de garantir les droits des enfants afin de les protéger des risques accrus liés aux nouvelles technologies.

[158] Nations Unies. (1989). *Convention relative aux droits de l'enfant,* article 3

Comme le souligne un rapport de l'UNICEF[159], l'interactivité et la technologie numériques peuvent exposer les enfants à des menaces amplifiées, telles que le cyberharcèlement, le *grooming* ou encore l'exploitation en ligne. L'impact des technologies numériques sur les enfants devient alors une question de santé publique. Il est donc primordial d'assurer leur droit à la protection contre les abus numériques et les violences en ligne, mais aussi de leur garantir un accès à une information adaptée, inclusive et sécurisée. Par ailleurs, la prévention des contenus illégaux, tels que la pornographie, la traite ou la radicalisation, doit être une priorité afin de préserver leur bien-être et leur développement. Le Comité des droits de l'enfant des Nations Unies a adopté une *observation* visant à s'assurer que les droits de chaque enfant - protégés par la CIDE - soient respectés, protégés et mis en œuvre dans l'environnement numérique[160]. Le texte soutient que l'environnement numérique contient certaines informations qui véhiculent *« des stéréotypes de genre, des informations discriminatoires, racistes, violentes, pornographiques ou abusives »*[161]. Les États devraient alors chercher à protéger *« les enfants contre les contenus nocifs et veiller à ce que les entreprises [...] et les autres fournisseurs [..] élaborent et appliquent des directives permettant aux enfants d'accéder en toute sécurité à des contenus diversifiés tout en protégeant ces mêmes enfants contre les matériels nocifs conformément à leurs droits et au développement de leurs capacités ».*

Ainsi, face à l'impact grandissant du numérique sur les enfants, il est impératif de mettre en place des mesures renforcées pour encadrer leur usage des technologies et assurer leur sécurité dans cet environnement en constante évolution.

Souvent en partenariat avec l'UNICEF, la France lance et soutient des initiatives afin de promouvoir et protéger les droits de l'enfant à l'ère du numérique. La France met en avant l'éducation comme un outil important de défense de l'intérêt supérieur de l'enfant et de lutte contre les inégalités. En éduquant au numérique ou à la réflexion éthique sur la conception d'outils technologiques, les droits des enfants seraient mieux respectés. L'OMS dans un

[159] *Rapport - la situation des enfants dans le monde 2017 - les enfants dans un monde numérique*, UNICEF, 2017, p.6
[160] *Observation n° 25 sur les droits de l'enfant en relation avec l'environnement numérique,* Comité des droits de l'enfant, CRC/C/GC/25, 2 mars 2021, par. 4
[161] *Ibidem* par. 54

rapport de 2022[162] souligne en effet l'importance de mettre en place des programmes éducatifs pour les enfants et les parents.

B) Les initiatives diplomatiques françaises

1. Partenariat mondial : Conférence ministérielle mondiale sur l'élimination de la violence à l'égard des enfants, Bogota, 2024

Une Conférence ministérielle mondiale pour mettre fin à la violence contre les enfants s'est tenue les 7 et 8 novembre 2024 à Bogota, en Colombie. Cette première conférence a été convoquée par le gouvernement colombien, avec le soutien du gouvernement suédois, de l'UNICEF, du Représentant spécial du Secrétaire général des Nations Unies sur la violence à l'égard des enfants et de l'OMS. Elle avait pour objectif d'impulser un changement de politique, de mobiliser des ressources et de mettre l'accent sur la prévention de la violence. Les délégations ministérielles, aux côtés des enfants et des acteurs de la société civile, se sont rassemblées autour d'une vision commune et ambitieuse visant à éradiquer toutes les formes de violence contre les enfants.

44 gouvernements ont pris des engagements significatifs pour offrir des environnements sûrs et favorables à l'apprentissage d'ici 2030. La France a pris 5 engagements, dont deux concernant la protection des enfants dans l'environnement du numérique. Le premier engagement, intitulé *« Accompagner les parents face aux impacts et aux risques liés à l'exposition aux écrans et aux usages numériques, en particulier la violence en ligne »*[163], fait part de la mobilisation de la France concernant la sensibilisation des parents aux risques auxquels les enfants sont confrontés dans leur utilisation des outils numériques. Les risques sont notamment l'exposition à des contenus violents ou inappropriés et le harcèlement en ligne. La France met à cet effet en avant sa plateforme gouvernementale « jeprotegemonenfant.gouv.fr », en ligne depuis 2022. Plus de 200 000 bénéficiaires sont ciblés, étant principalement les parents, bien qu'elle reste accessible à tous. Cette plateforme sert à aider les parents à encadrer l'usage du numérique, prévenir les risques et réagir face aux situations de violence en ligne. Elle centralise des informations, propose des outils de

[162] *Rapport sur la prévention des violences en ligne contre les enfants, "What works to prevent violence against children online?",* OMS, 24 novembre 2022

[163] *Conférence de Bogota - L'engagement transformateur de la France, Soutenir les parents dans la gestion des risques liés aux usages numériques, en particulier la violence en ligne*

protection comme le contrôle parental, et informe également sur les dispositifs d'alerte et d'accompagnement des victimes dans la lutte contre le cyberharcèlement ou la suppression des contenus haineux. Toutefois, la plateforme a été financée exclusivement par des acteurs privés (moteurs de recherche, réseaux sociaux, chaînes de télévision, fournisseurs d'accès à Internet…) et une association (Union Nationale des Associations Familiales). L'engagement financier de l'État français se limite à l'hébergement et à la maintenance du site, pour un coût annuel s'élevant à seulement 6 200 euros en 2024.

Le deuxième engagement de la France, intitulé *« Lutter contre les violences faites aux enfants dans l'environnement numérique* »[164], fait part de la mobilisation de la France dans le renforcement de l'éducation numérique, en particulier pour les enfants vulnérables et en situation de handicap. La France souligne son engagement à travers la présentation, conjointement avec les Pays-Bas, d'une résolution biennale depuis 2006 devant l'Assemblée Générale des Nations Unies visant à intensifier la lutte contre toutes les formes de violence faites aux femmes. Pour la 79e session de l'Assemblée générale des Nations Unies, cette démarche s'est traduite par une focalisation sur la violence numérique à l'égard des femmes et des filles[165], enjeu encore peu abordé dans les débats onusiens. De plus, elle met en avant sa déclaration politique initiée en collaboration avec l'UNICEF, sur *Les droits des enfants dans le monde numérique*[166], adoptée le 17 mars 2022 par neuf pays (Argentine, Belgique, Bulgarie, Estonie, France, Italie, Jordanie, Luxembourg et Maroc), ainsi que par l'UNICEF et la Représentante spéciale du Secrétaire général des Nations Unies pour la violence contre les enfants. La France fait part de sa volonté d'engagement futur dans une campagne afin d'élargir le nombre de signataires de cette déclaration conjointe. Enfin, la France met en avant le *Laboratoire pour la protection de l'enfance en ligne*, lancé en novembre 2022, visant à promouvoir la création d'outils numériques adaptés aux enfants dès leur conception. La France s'engage à continuer de soutenir les travaux du Laboratoire et à renforcer les solutions innovantes pour protéger les enfants en ligne.

[164] *Conférence de Bogotá - L'engagement transformateur de la France, Violence contre les enfants dans l'environnement numérique*
[165] *Op. cit* n°50, p. 31
[166] *Op. cit.* n°52, p. 32

2. Sur le Forum de Paris sur la Paix et l'Appel à l'action pour défendre les droits de l'enfant dans l'environnement numérique

Le Forum de Paris sur la Paix, créé le 9 mars 2018, est une manifestation internationale tenue chaque année à Paris. Réunissant les Etats, des acteurs publics et privés et la société civile, il vise à agir face aux défis mondiaux en développant une gouvernance mondiale concrète.

Lors du 4ème Forum de Paris sur la Paix en novembre 2021, la France, en partenariat avec l'UNICEF, a lancé un *Appel à l'action visant à défendre les droits de l'enfant dans l'environnement numérique*[167]. Cette initiative reconnaît à la fois les opportunités offertes par le numérique pour l'éducation et l'expression des enfants, et les risques tels que le cyberharcèlement ou l'exposition à des contenus inappropriés. Les signataires de cet Appel, incluant plusieurs États, grandes plateformes numériques et ONG, se sont engagés à faciliter l'accès des enfants aux technologies et à l'alphabétisation numérique, tout en garantissant leur protection en ligne. Ils ont également adopté une politique de tolérance zéro envers les abus numériques ciblant les mineurs.

a) Déclaration sur les droits de l'enfant dans l'environnement numérique du 17 mars 2022

En 2021, la France a initié, avec l'UNICEF, une déclaration politique sur les droits des enfants dans l'environnement numérique, adoptée le 17 mars 2022 par neuf États (Argentine, Belgique, Bulgarie, Estonie, France, Italie, Jordanie, Luxembourg et Maroc), ainsi que par l'UNICEF et la Représentante spéciale du Secrétaire général des Nations Unies sur la violence contre les enfants.

Cette déclaration a été soutenue par plusieurs États, mais aussi par des grandes plateformes numériques et des organisations non gouvernementales. Elle s'inscrit donc dans une démarche multilatérale et multi-acteurs, visant à créer un environnement numérique sûr et bénéfique pour les enfants. Elle vise à garantir que les enfants puissent bénéficier des opportunités

[167] *Appel à l'action : défendre les droits de l'enfant dans l'environnement numérique,* Elysée, 11 novembre 2021, Lien : https://www.elysee.fr/emmanuel-macron/2021/11/11/communique-de-presse-conjoint-entre-la-presidence-de-la-republique-et-le-fonds-des-nations-unies-pour-lenfance

offertes par le numérique tout en étant protégés contre ses dangers. Aujourd'hui, 23 États soutiennent cette déclaration et s'engagent à la mettre en œuvre aux niveaux national, régional et international. La France lance de nouvelles campagnes pour élargir le nombre de signataires, afin de garantir la promotion et le respect des principes de cette déclaration.

La déclaration conjointe souligne l'importance fondamentale de permettre aux enfants de participer activement aux décisions qui les concernent. Elle reconnaît ainsi les enfants comme acteurs à part entière de leurs droits, en leur donnant une voix dans la création d'un environnement numérique qui les concerne directement.

> *« Rappelant le droit des enfants à participer aux décisions qui les concernent, consacré par la Convention relative aux droits de l'enfant, et réaffirmant combien il est important que tous les enfants prennent effectivement part à la conception et à la mise en œuvre des mesures, produits et services touchant à l'exercice de leurs droits dans l'environnement numérique; [168]»*

b) *Sommet pour l'action sur l'IA : coalition, coordonnée par le Forum de Paris sur la Paix et everyone.ai*

Parmi leurs nombreuses initiatives politiques, le Forum de Paris sur la Paix promeut la coopération mondiale dans le secteur des technologies innovantes. Ainsi, il existe une coalition multipartite pour une IA bénéfique au développement de l'enfant pour protéger les enfants des dangers numériques tout en leur offrant un accès bénéfique à la technologie. Cette coalition internationale place la protection de l'intérêt supérieur de l'enfant au cœur de son action, en réunissant plusieurs acteurs différents tels que les gouvernements, les entreprises technologiques, les chercheurs, les éducateurs, les ONG mais aussi les familles.

Cette initiative, soutenue par le ministre français des Partenariats internationaux et de nombreux États et organisations internationales comme l'UNICEF et l'UNESCO, promeut une IA centrée sur l'enfant, conçue de manière éthique, inclusive, adaptée à l'âge, respectueuse de la vie privée et pensée en lien avec les familles. Guidée par la *CIDE,* elle vise à anticiper les risques, combler les inégalités et garantir un environnement numérique où chaque enfant peut se développer en toute sécurité et pleinement exercer ses droits.

[168] *Op. cit.* n°52, p. 32

La coalition s'est fixée cinq objectifs principaux. Le premier est d'établir des lignes directrices communes, évolutives et inclusives pour encadrer l'usage de l'IA destinée aux enfants, en mettant l'accent sur leur sécurité et leur bien-être. Le deuxième consiste à s'appuyer sur des données scientifiques pour évaluer les effets de l'IA sur le développement des enfants et encourager la recherche à long terme. Le troisième vise à créer un réseau d'experts pour orienter les décisions et garantir que les solutions d'IA respectent les droits de l'enfant, et le quatrième à renforcer la coopération internationale et interdisciplinaire entre toutes les parties prenantes. Enfin, le cinquième objectif vise à renforcer l'éducation à l'IA en développant des lignes directrices, des outils pédagogiques et des programmes adaptés pour que les enfants, leurs familles et les éducateurs puissent utiliser l'IA de façon sûre et responsable.

c) Laboratoire pour la protection de l'enfance en ligne

Le *Laboratoire pour la protection de l'enfance en ligne* a été lancé par la France en novembre 2022 par le Président de la République à l'Élysée, lors de la 5ème édition du Forum. Cette initiative fait suite au lancement de l'*Appel à l'action pour défendre les droits de l'enfant dans l'environnement numérique* en novembre 2021[169], et de la *Déclaration sur les droits de l'enfant dans l'environnement numérique*[170] adoptée en mars 2022.

Cette initiative s'inspire de l'*Appel de Christchurch*[171], contre l'extrémisme violent en ligne, lancé conjointement par la Nouvelle-Zélande et la France à la suite de l'attentat de 2019 qui avait causé la mort de 51 personnes dans deux mosquées de cette ville néo-zélandaise. Elle vise à regrouper gouvernements, entreprises technologiques et du numérique, experts universitaires ainsi que acteurs de la société civile tels que des ONG afin de partager les expertises, les meilleures pratiques, et tester des solutions innovantes pour mieux protéger les enfants en ligne. En effet, le Laboratoire bénéficie du soutien du Royaume-Uni et du Centre National pour les Enfants Manquants et Exploités (National Center for Missing & Exploited Children – NCMEC – organisme américain).

[169] *Op. cit.* n°167 p. 74
[170] *Op., cit., n*°156, p. 68
[171] *« Appel de Christchurch, une initiative ambitieuse au service d'un internet ouvert, libre et sûr »* , MEAE. Lien : https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/article/l-appel-de-christchurch-une-initiative-ambitieuse-au-service-d-un-internet

Il vise à encourager la conception d'outils numériques adaptés aux enfants dès leur conception. L'objectif est de développer des cadres normatifs, des bonnes pratiques industrielles et des principes de conception axés sur la sécurité et la confidentialité. La *Charte du Laboratoire*[172] affirme dès son quatrième paragraphe que les droits de l'Homme, notamment la protection de la vie privée, doivent être au centre des initiatives visant à améliorer l'environnement numérique.

Le Laboratoire a également permis la création d'une base de données internationale pour supprimer les images intimes partagées sans consentement et l'expérimentation de la vérification d'âge sur les sites pornographiques. De plus, il a été annoncé l'engagement de nouveaux soutiens et objectifs pour 2024 afin de mettre en place des actions concrètes visant à lutter contre les violences envers les enfants sur Internet et à garantir leur sécurité dans l'espace numérique. Cet engagement a été pris par le ministre de l'Europe et des Affaires étrangères Jean-Noël Barrot et Charlotte Caubel, magistrate et ancienne secrétaire d'État chargée de la protection de l'enfance, en lien avec le MEAE et l'Ambassadeur pour le numérique, Henri VERDIER.

Jean-Noël BARROT a déclaré :

> *« La protection des mineurs dans l'espace numérique est un combat du Gouvernement, que nous devons également mener au niveau européen et mondial. Nos enfants sont confrontés de plus en plus jeunes aux dangers d'internet : c'est notre devoir collectif de proposer des solutions concrètes aux entreprises du numérique, à la société et aux parents pour les préserver. À travers le Laboratoire et ses objectifs ambitieux pour 2024, notre force de frappe est amplifiée en faveur de la protection des enfants.*[173] »

---

[172] *Charte du Laboratoire pour la protection de l'enfance en ligne*, Elysée, 8 novembre 2023, Lien : https://www.elysee.fr/emmanuel-macron/2023/11/08/charte-du-laboratoire-pour-la-protection-de-lenfance-en-ligne

[173] Communiqué de presse, *Bilan et orientations du Laboratoire pour la protection de l'enfance en ligne*, Ministère de l'économie, des finances et la souveraineté industrielle et numérique, n°1328. Lien : https://presse.economie.gouv.fr/09112023-cp-bilan-et-orientations-du-laboratoire-pour-la-protection-de-lenfance-en-ligne/

En mobilisant pour la première fois de nombreux gouvernements étrangers, des organisations internationales et les principaux acteurs du numérique, le Laboratoire reflète une approche multipartite de la diplomatie numérique française. La France met notamment en avant le Laboratoire comme un pilier central de sa diplomatie numérique, illustrant son engagement en faveur d'un Internet plus sûr pour les enfants, qui s'inscrit plus globalement dans sa stratégie de diplomatie numérique visant à promouvoir un cyberespace ouvert, sûr et respectueux des droits fondamentaux.

3. Appel à un accord futur

Le 11 mai 2025, la ministre du numérique et de l'IA a déclaré vouloir aboutir au bout de trois mois à un accord européen en mobilisant « ses partenaires », contraignant les réseaux sociaux à vérifier l'âge des adolescents les utilisant.[174] L'objectif de cette accord est d'aller plus loin que la législation européenne en vigueur :

> *« À l'échelle européenne, nous avons un cadre d'action de référence : le règlement sur les services numériques, le Digital Services Act, (...) Mais il faut aller plus loin pour renforcer sa portée, afin qu'il contraigne les réseaux sociaux à ne pas accepter la création de comptes sans vérification d'âge. »*

Ainsi, en coalition avec l'Espagne et la Grèce, un document a été envoyé à la Commission européenne[175], appelant à une action collective européenne pour répondre à la responsabilité intergénérationnelle que représente la protection des mineurs face aux risques numériques. Tout en reconnaissant les bénéfices de la technologie, ils alertent sur les déséquilibres engendrés par les plateformes numériques. Ils soulignent les progrès des législations européennes telles que le RGPD, le DSA et la stratégie BIK+, mais identifient encore des défis majeurs :

- établir une majorité numérique européenne pour l'accès aux réseaux sociaux ;

---

[174] *Pour la ministre chargée de l'IA et du Numérique Clara Chappaz : « Les réseaux sociaux avant 15 ans, c'est non »,* La Tribune Dimanche, 11 mai 2025. Lien : https://www.latribune.fr/la-tribune-dimanche/dimanche-eco/pour-la-ministre-chargee-de-l-ia-et-du-numerique-clara-chappaz-les-reseaux-sociaux-avant-15-ans-c-est-non-1024669.html

[175] Document politique de la France, l'Espagne et la Grèce envoyé à la Commission européenne : *"Protecting Minors from Online harms and risks: Age verification, age- appropriate design and a pan-European digital age of majority"*, mai 2025. Lien : https://www.euractiv.fr/wp-content/uploads/sites/3/2025/05/Euractiv-1-2-1.pdf

- imposer des mécanismes robustes de vérification de l'âge à l'échelle européenne ;
- adopter un cadre réglementaire contraignant pour garantir des interfaces sûres, non addictives, et respectueuses de la vie privée dès la conception.

Les trois Etats signataires appellent également à créer d'autres normes européennes afin d'imposer des designs adaptés aux enfants.

II. Les inégalités : l'accessibilité au numérique et les inégalités de genre et structurelles

Il existe une réelle fracture numérique qui se manifeste par une accessibilité inégale selon plusieurs critères (A), contre laquelle la France tente de lutter à travers ses initiatives (B).

A) État de la situation d'une fracture numérique persistante

L'accès à Internet comporte deux volets : d'une part, la possibilité de consulter librement des contenus en ligne, sauf dans certains cas strictement encadrés par le droit international des droits de l'Homme ; d'autre part, la disponibilité des infrastructures et des technologies nécessaires - tels que câbles, modems, ordinateurs ou logiciels - permettant la connexion au réseau. La liberté d'Internet, quant à elle, désigne « l'exercice, la protection et

la jouissance des droits de l'homme et des libertés fondamentales en ligne »[176], conformément aux instruments internationaux en matière de droits de l'Homme.

Dans un secteur marqué par des inégalités de genre, il convient de garantir l'égalité d'accès aux technologies et promouvoir la parité numérique. De manière générale, il s'agit d'assurer une accessibilité équitable entre les genres mais aussi entre tous, quel que soit le statut social ou les sources de revenus.

En effet, il existe des fractures numériques importantes, particulièrement visibles surtout chez les enfants. Tout d'abord selon un rapport de l'UNICEF de 2022[177], 346 millions de personnes ne sont pas connectés, les enfants, personnes vulnérables, étant particulièrement touchés par ce manque de connectivité. Par ailleurs, selon le même rapport, Internet accroît la vulnérabilité des enfants aux risques et dangers.

Le rapport fait état de plusieurs défis :

- Les jeunes constituent la tranche d'âge la plus connectée. À l'échelle mondiale, 71 % d'entre eux utilisent Internet contre 48 % pour la population totale ;
- Les jeunes Africains sont les moins connectés : environ trois jeunes sur cinq n'utilisent pas Internet, contre seulement un sur 25 en Europe ;
- 56 % des sites Internet sont en anglais, ce qui empêche beaucoup d'enfants d'accéder à des contenus qu'ils comprennent ou qui sont en rapport avec leur culture ;
- Cinq pays hébergent à eux seuls plus de 9 sites pédopornographiques sur 10 confirmés à l'échelle mondiale : le Canada, les États-Unis, la France, la Fédération de Russie, et les Pays-Bas.

B) Les initiatives françaises dans la lutte contre la fracture numérique

1. Inégalités d'accès entre Etats

Lors du Forum de Paris sur la Paix de 2022, l'un des projets acceptés dans le cadre des candidatures est la thématique intitulée « Mettre l'Intelligence Artificielle (IA) au service du

[176] *Recommandation CM/Rec(2016)5[1] du Comité des Ministres du Conseil de l'Europe aux États membres sur la liberté d'Internet*, 13 avril 2016
[177] *Rapport sur les enfants à l'ère numérique, Mieux protéger les enfants dans un monde numérique tout en améliorant l'accès à Internet des plus défavorisés*, UNICEF, 11 décembre 2017

développement économique dans le Sud Global »[178]. Cette thématique illustre la diplomatie française en action sur la scène internationale. En effet, par ce thème, la France mobilise son *leadership* pour promouvoir une coopération numérique mondiale qui favorise le développement durable, l'innovation et la résilience économique dans les États du Sud. En valorisant les technologies de l'IA comme outils de transformation socio-économique et non de fracture technologique, elle affirme une vision diplomatique inclusive et solidaire, concernée par la réduction des inégalités globales et la construction d'un multilatéralisme tourné vers l'avenir.

2. Inégalités de genre

Un projet de résolution franco-néerlandaise à l'Assemblée générale de l'ONU[179] met en avant la diplomatie féministe de la France en ciblant directement les inéquités de genre dans l'environnement numérique. En tant que cadre normatif, elle appelle les États et les plateformes à prévenir et éliminer les violences en ligne - qu'il s'agisse de harcèlement, de discours haineux, de diffusion non consentie d'images ou de *deepfakes* - et propose d'agir à la source en réduisant la fracture numérique entre les sexes et en corrigeant les biais algorithmiques. Par ce texte, la France affirme que le numérique peut être un levier d'émancipation, en favorisant la participation des femmes dans les processus décisionnels, l'accès à l'éducation et à la santé, tout en renforçant la responsabilité des États et des acteurs privés en matière de modération et de lutte contre l'impunité.

De plus, la France a adopté une *Stratégie internationale de la France pour une diplomatie féministe (2025-2030)*[180]. Sur le site officiel du MEAE, la France définit des objectifs de protection et de promotion des droits des femmes et des filles, tant à l'international qu'au niveau européen. Parmi ces objectifs, le numérique figure parmi les sujets à défendre. De plus, la France vise à lutter contre les violences faites aux femmes et aux filles dans plusieurs espaces, dont l'environnement numérique. Ainsi, la quatrième des cinq priorités tend à *«*

[178] Forum de Paris sur la Paix - Appel à solutions 2022, *Représentation permanente de la France auprès des Nations Unies à New York*, 13 janvier 2023, Lien : https://onu.delegfrance.org/forum-de-paris-sur-la-paix-appel-a-solutions-2022
[179] *Op. cit* n°50, p. 31
[180] *Stratégie internationale de la France pour une diplomatie féministe (2025-2030),* MEAE. Lien : https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-feministe/strategie-internationale-de-la-france-pour-une-diplomatie-feministe-2025-2030/

défendre les droits des femmes dans l'environnement numérique et l'intelligence artificielle et à mobiliser la diplomatie économique et commerciale en faveur de l'égalité. ».

Dans cette Stratégie, l'objectif est d'élargir la portée du Laboratoire pour les droits des femmes en ligne[181]. Ce laboratoire a été lancé en 2024 et est une plateforme visant à lutter contre les violences fondées sur le genre, commises en ligne. À cet effet, 5 millions d'euros sont prévus pour ce programme.

Chapitre III. L'engagement de la France à garantir la sécurité de l'espace numérique, son ouverture et promouvoir la liberté d'expression en ligne

Aujourd'hui, le numérique doit être régulé en raison de nombreux enjeux : les menaces dans le cyberespace qui entraînent une instabilité et une insécurité, notamment l'usage d'internet à des fins criminelles et plus spécifiquement terroristes, la remise en cause de l'ouverture d'internet, de la liberté d'expression par la volonté de contrôle des réseaux par les Etats autoritaires ou encore l'ingérence numérique étrangère à des fins de déstabilisation. Le rôle des grandes entreprises du numérique, notamment au regard de leur position dominante et de l'engagement de leur responsabilité, soulève également des problématiques.

Par la publication de sa *Stratégie internationale pour le numérique* le 15 décembre 2017[182], la France a fait du numérique un enjeu de premier ordre pour sa politique étrangère, et plus globalement pour son action publique. La diplomatie numérique qu'entend mener la France, notamment autour de trois des objectifs consacrés dans cette stratégie (garantir la sécurité internationale du cyberespace, à travers le renforcement de l'autonomie stratégique européenne et la promotion de la stabilité du cyberespace dans les instances internationales et la régulation des contenus diffusés sur l'internet ainsi que la régulation des plateformes ; contribuer à la gouvernance de l'Internet en renforçant son caractère ouvert et diversifié, tout en renforçant la confiance dans son utilisation ; promouvoir les droits de l'Homme, les

[181] *Le laboratoire pour les droits des femmes en ligne*, MEAE, juillet 2024. Lien : https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-feministe/le-laboratoire-pour-les-droits-des-femmes-en-ligne/
[182] *Op. cit.* n°44, p. 27

valeurs démocratiques et la langue française dans le monde numérique), dénotent ainsi sa volonté de garantir la sécurité et l'ouverture de l'espace numérique (I) ainsi qu'à promouvoir et protéger la liberté d'expression en ligne (II).

I. Garantir la sécurité de l'espace numérique

Au regard de l'intensification de la cybercriminalité, la France a renforcé la résilience de ses infrastructures et développé une culture de la cybersécurité, tant dans le secteur privé que public. La France, outre son engagement au niveau de l'Union européenne, est active au sein des instances internationales et via des initiatives bilatérales et multilatérales en vue de garantir la sécurité de l'espace numérique, en promouvant les principes de liberté, d'ouverture, de neutralité, de sûreté et d'unification afin de favoriser la paix et la sécurité internationale (A), et est particulièrement engagée dans la lutte contre le terrorisme en ligne en ce sens (B).

A) Les initiatives diplomatiques françaises en matière de cybersécurité

La France joue également un rôle moteur au sein des instances internationales et par des initiatives bilatérales et multilatérales face à la menace croissante que représente la cybercriminalité, et promeut le développement d'un cadre de coopération efficace, respectueux de la vie privée et protecteur des libertés fondamentales.

1. L'Appel de Paris pour la confiance et la sécurité dans le cyberespace du 12 novembre 2018

L'*Appel de Paris pour la confiance et la sécurité dans le cyberespace*[183], lancé par le Président Emmanuel Macron le 12 novembre 2018 à l'occasion de la réunion du Forum sur la gouvernance de l'internet et du Forum de Paris sur la Paix à l'UNESCO, est aujourd'hui la plus grande initiative multi-acteurs en matière de cybersécurité, soutenu par 81 Etats, 36 organismes publics et administrations territoriales, 390 organisations et membres de la société civile, et plus de 700 entreprises et entités du secteur privé. Cet Appel invite notamment tous

[183] MACRON E., *Appel de Paris pour la confiance et la sécurité dans le cyberespace*, 11 novembre 2018, Lien : https://pariscall.international/fr/call

les acteurs à réagir ensemble face aux nouvelles menaces qui mettent en danger les citoyens et les infrastructures, les soutiens s'engageant ainsi à travailler ensemble afin de mettre en œuvre ses principes et à adopter des comportements responsables dans le cyberspace. Cette Appel affirme la volonté française de garantir un cyberespace ouvert, sûr, stable, accessible et pacifique, condamne les cyberactivités malveillantes en temps de paix, vise à promouvoir une vaste coopération dans le domaine du numérique et des efforts pour renforcer les capacités des différents acteurs et encourage les initiatives qui permettent d'accroître la résilience et les compétences des utilisateurs.

Cet *Appel de Paris* repose ainsi sur neufs principes communs qui visent à guider l'action de la France et des soutiens de l'Appel en vue de sécuriser le cyberespace. Ces principes sont : la protection des individus et des infrastructures ; la protection d'internet ; la défense des processus électoraux (en développant la capacité de prévention des interférences d'acteurs étrangers visant à déstabiliser des processus électoraux au moyen de cyber-activités malveillantes, avec la mise en place par exemple de la *Transatlantic Commission on Election Integrity*) ; la défense de la propriété intellectuelle (en empêchant le vol de la propriété intellectuelle à l'aide des technologies de l'information et de communication, notamment des secrets industriels ou autres informations commerciales confidentielles, dans l'intention de procurer des avantages concurrentiels à des entreprises ou à un secteur commercial), la non-prolifération (en empêchant la prolifération des logiciels malveillants et des pratiques informatiques destinés à nuire) ; la sécurité de tout le cycle de vie des processus, produits et services numériques ; l'hygiène informatique ; la non-cyber-riposte privée (en empêchant les acteurs non étatiques, y compris le secteur privé, de répondre par des actions cyber offensives à une attaque dont ils seraient victimes) ; l'acceptation et la mise en oeuvre des normes internationales de comportement responsable.

2. Initiatives françaises sein des organisations internationales

Au niveau onusien, la France, avec 54 autres Etats et l'Union européenne, a milité pour l'adoption d'un programme d'action des Nations Unies sur la cybersécurité, en vue de contribuer concrètement à l'élévation du niveau global de cybersécurité, passant par la promotion d'un comportement étatique responsable dans l'utilisation des technologies, le renforcement des capacités des Etats ainsi que la collaboration avec le secteur privé, la

société civile, les milieux universitaires et la communauté technique. Cette initiative a abouti à l'adoption, par l'Assemblée générale des Nations Unies le 24 octobre 2023, de la *résolution A/C.1/78/L.60/Rev.1*[184] portée par la France, la Colombie et les Etats Unis.

L'engagement de la France en matière de cybersécurité se manifeste également dans d'autres instances internationales, notamment au sein du G7. Le 6 avril 2019, les ministres des Affaires étrangères des pays membres ont adopté la *Déclaration de Dinard sur l'initiative pour des normes dans le cyberespace*[185]. Dans la continuité de l'*Appel de Paris*, cette déclaration promeut l'établissement de normes internationales encadrant le comportement responsable des États dans le cyberespace, encourage la coopération entre États pour prévenir les cyberattaques, lutter contre les activités malveillantes, garantir un espace numérique libre, ouvert, sûr et stable et synthétise les leçons tirées ainsi que les bonnes pratiques identifiées.

Au G20, la France a porté auprès de la présidence japonaise la question de la responsabilité des acteurs privés. Résultat de cette initiative, la *déclaration d'Osaka*[186] lors du Sommet du G20 de 2019 reconnaît l'importance de promouvoir la sécurité dans l'économie numérique et de combler certaines des lacunes et vulnérabilités existantes en matière de cybersécurité.

Un Forum mondial sur la sécurité numérique pour la prospérité économique se tient également depuis 2018 à l'OCDE, sous impulsion française. Ce Forum est un cadre multilatéral international, permettant un dialogue entre experts et décideurs politiques afin de partager leurs expériences et d'influencer l'élaboration des politiques publiques en matière de sécurité numérique. Il offre l'opportunité de faire progresser les positions défendues par la France sur la question de la responsabilité des acteurs privés dans la sécurité et la stabilité du cyberespace.

A l'Organisation pour la sécurité et la coopération en Europe (OSCE), organisation régionale de référence pour la définition et la mise en œuvre des mesures de confiance appliquées au cyberespace, un groupe de travail informel a été mis en place depuis 2012, réunissant les experts des États participants. La France, au sein de cette organisation, promeut un agenda

---

[184] *Résolution A/C.1/78/L.60/Rev.1, Programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale*, Assemblée générale des Nations Unies, 24 octobre 2023

[185] *Déclaration de Dinard sur l'initiative pour des normes dans le cyberespace*, G7, 5 avril 2019. Lien : https://www.elysee.fr/admin/upload/default/0001/04/1aa18fff8ca04e2f0bb984a29612368e0c9063c4.pdf

[186] *Déclaration des chefs d'Etats et du gouvernement,* Sommet du G20 d'Osaka, 2019. Lien : https://www.elysee.fr/admin/upload/default/0001/04/1aa18fff8ca04e2f0bb984a29612368e0c9063c4.pdf

ambitieux d'opérationnalisation de ces mesures afin de renforcer la transparence, la coopération et la confiance entre les pays membres de l'organisation.

La France est également fortement engagée au sein de l'Organisation du traité de l'Atlantique Nord (OTAN) sur les questions de cybersécurité. Elle a joué un rôle moteur dans l'adoption, par les 28 États membres, d'un « *Engagement pour la cyberdéfense* » (*"Cyber Defence Pledge"*)[187] lors du Sommet de Varsovie en juin 2016. Cet engagement souligne la priorité donnée au renforcement et à l'amélioration des capacités de cyberdéfense des infrastructures et réseaux nationaux. En mai 2018, la France a d'ailleurs accueilli la première conférence internationale consacrée à la mise en œuvre de cet engagement.

3. Initiatives bilatérales

La France mène également des dialogues stratégiques bilatéraux de cybersécurité (2020 : conduite de trois dialogues avec les Etats-Unis, le Royaume Uni et la Russie), dont le but est d'identifier des points de convergence à mettre en avant dans le cadre d'enceintes multilatérales et, plus globalement, de construire une relation de confiance. Ces dialogues ont également pour objectif la mise en œuvre de coopérations au niveau technique. Des coopérations bilatérales pilotées par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) avec certains partenaires étrangers (Maroc et Vietnam notamment), avec pour objectif de permettre un partage d'expérience et des bonnes pratiques sur des sujets techniques (méthodes d'analyse des menaces, certifications informatiques, résolutions d'incidents, protection des infrastructures critiques ou sécurisation de grands événements) ont également lieu. Pour finir, le Ministère de la Justice et le Ministère de l'Intérieur développent des coopérations bilatérales entre services d'enquêtes ou judiciaires pour lutter contre la cybercriminalité.

La France entend aujourd'hui mener une réflexion, avec ses partenaires étatiques mais aussi du secteur privé et de la société civile, sur le rôle et les responsabilités spécifiques des acteurs privés dans le renforcement de la stabilité et de la sécurité internationale du cyberespace.

B) La lutte contre le terrorisme en ligne, priorité française

[187] Communiqué de presse, *Engagement en faveur de la cyberdéfense*, OTAN, 8 juillet 2016. Lien : https://www.nato.int/cps/en/natohq/official_texts_133177.htm?selectedLocale=fr

La France est ainsi particulièrement engagée dans la lutte contre l'utilisation d'internet à des fins terroristes, avec des initiatives au niveau de l'Union européenne, des instances internationales ainsi qu'avec ses partenaires internationaux. L'action de la France dans ce domaine passe notamment par un renforcement de la coopération internationale dans le domaine de la prévention de la radicalisation.

La France est à l'origine, aux côtés de la Nouvelle-Zélande, de l'*Appel de Christchurch*[188],

lancé le 15 mai 2019 en réponse aux attentats perpétrés à Christchurch (Nouvelle-Zélande) le 15 mars 2019, dont les images ont été diffusées en direct sur les réseaux sociaux par l'auteur. Cet événement a notamment mis en lumière les insuffisances des dispositifs existants pour prévenir la diffusion de contenus terroristes en ligne. Cet Appel, soutenu par 52 États, la Commission européenne, l'UNESCO, le Conseil de l'Europe, de grandes plateformes numériques (Amazon, DailyMotion, Facebook, Google, Microsoft, Qwant, Twitter, YouTube, entre autres) ainsi que des représentants de la société civile, vise à renforcer la coopération entre gouvernements, entreprises et acteurs du numérique pour éliminer les contenus terroristes et extrémistes violents en ligne.

Différents engagements gouvernementaux ont été pris dans cet Appel, notamment la lutte contre les facteurs de terrorisme et d'extrêmisme violent, en renforçant la résilience et l'inclusion de nos sociétés pour leur permettre de résister aux idéologies terorristes et extrêmistes violentes (notamment par l'éducation) ; l'application des lois en vigueur qui interdisent la production ou la diffusion de contenus terroristes et extrémiste violents ; le fait d'encourager les médias à appliquer des normes éthiques lorsqu'ils décrivent en ligne des événements terroristes ; le soutien à la mise en place de cadre, par exemple des normes sectorielles, pour s'assurer que la communication sur les attentats n'augmente pas l'écho de ces contenus et envisager des mesures adaptées afin de prévenir l'utilisation des services en ligne pour diffuser des contenus terroristes et extrêmistes violents, notamment des mesures concertées (des actions de sensibilisation et de renforcement des capacités destinées aux petits fournisseurs de service en ligne, des normes sectorielles ou de cadres volontaires, des mesures réglementaires ou politiques compatibles avec un Internet libre, ouvert et sûr et conformes au droit international des droits de l'Homme).

[188] MACRON E., ARDERN J., *Appel de Christchurch*, 15 mai 2019, Lien : :https://www.christchurchcall.org/content/files/2024/06/Appel-de-Christchurch-texte-complet-francais-1.pdf

Par ailleurs, les fournisseurs de service, par cet Appel, s'engagent à prendre des mesures particulières et transparentes permettant de prévenir le téléchargement de contenus terroristes et extrémistes violents, mais aussi leur diffusion sur les réseaux sociaux et les services analogues de partage de contenus, incluant notamment leur retrait immédiat et permanent ; à faire preuve de plus de transparence dans la mise en place de normes collectives ou de conditions de services ; à appliquer ces normes collectives ou ces conditions de service dans le respect des droits de l'Homme et des libertés fondamentales (en privilégiant la modération des contenus terroristes et extrémistes violents, tout en les identifiant, en fermant des comptes lorsque c'est nécessaire, en mettant en place des procédures efficaces de réclamation et d'appel pour les personnes qui souhaitent contester le retrait de leur contenu ou contester une décision de refus de téléchargement de leur contenu) ; à mettre en œuvre des mesures efficaces et immédiates visant à atténuer les risques particuliers de diffusion de contenus terroristes et extrémistes violents dans le cadre de flux en direct (notamment l'identification de contenus à des fins d'examen en temps réel) ; à effectuer des rapports publics, réguliers et transparents, quantitatifs sur la quantité et la nature de contenus terroristes et extrémistes violents détectés et retirés ; à examiner les formules des algorithmes et les autres processus pouvant orienter les utilisateurs vers des contenus terroristes et extrémistes violents et/ou amplifier ces contenus ; à agir ensemble pour faire en sorte que les efforts intersectoriels soient coordonnées et solides.

La mise en œuvre de ses engagements constitue une part importante de l'action française en matière de sécurité numérique et de régulation des plateformes numériques, qui passe par plusieurs initiatives : la mise en place d'un réseau consultatif composé d'organisations de la société civile ; le suivi de la mise en oeuvre des engagements de l'Appel par les entreprises ; le suivi de la mise en place des protocoles des entreprises de l'Internet et d'Europol pour une réponse rapide et coordonnée à la diffusion de contenus terroristes suite à une attaque ; le lancement d'une consultation inédite des soutiens pour évaluer l'efficacité et le respect des engagements de l'Appel ainsi que pour définir ses futures priorités ou encore la préparation du deuxième anniversaire de l'Appel.

II. La promotion et la protection de la liberté d'expression en ligne

La France vise à créer ses propres outils pour lutter contre la création et la diffusion

de ces fausses informations, tout en appelant à une plus grande responsabilisation des plateformes numériques, qui jouent un rôle majeur dans la diffusion et l'amplification de ces contenus. À travers ces efforts, la France défend les principes d'un internet libre, ouvert, neutre et unique, qu'elle promeut activement au sein des institutions et instances de l'UE et auprès de ses partenaires internationaux. L'Ambassadeur du numérique mène également des actions transversales pour défendre les valeurs défendues par la France au regard d'internet, et participe ainsi à des initiatives multipartites et multilatérales pour renforcer l'indépendance stratégique de la France vis-à-vis des grands acteurs étatiques ou privés (A).

L'action et les iniatives françaises dans le domaine du numérique visent également à soutenir les mouvements démocratiques, la liberté d'expression et les droits de l'Homme dans les pays où ces libertés et droits sont menacés et à lutter contre l'ingérence étrangère, qui peut être définie comme un « *agissement commis directement ou indirectement à la demande ou pour le compte d'une puissance étrangère et ayant pour objet ou pour effet, par tout moyen, y compris par la communication d'informations fausses ou inexactes, de porter atteinte aux intérêts fondamentaux de la Nation, au fonctionnement ou à l'intégrité de ses infrastructures essentielles ou au fonctionnement régulier de ses institutions démocratique* »[189]. Ces actes d'ingérence étrangère, qui constitue une véritable menace pour nos démocraties, se sont particulièrement multipliés ces dernières années en raison de l'expansion de l'usage d'internet et des réseaux sociaux, ainsi que l'apparition des nouvelles technologies numériques (B).

A) L'appui à l'environnement des médias et la lutte contre la désinformation, priorités françaises

La France est particulièrement engagée en faveur d'un accès universel à une information de qualité, libre, diversifiée et fiable. Face aux menaces croissantes qui pèsent sur l'écosystème médiatique – qu'il s'agisse de la fragilité économique des médias dans de nombreux pays ou de la prolifération des contenus trompeurs, souvent favorisée par l'absence de modération sur les réseaux sociaux – la France mène une action de premier plan. Cette action s'appuie sur plusieurs leviers : des initiatives politiques, un soutien concret aux acteurs des médias, ainsi qu'une lutte active contre la désinformation et les manipulations de l'information.

[189] Définition issue de la loi 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France

1. Le soutien à l'environnement des médias

Une *feuille de route médias et développement pour la période 2023-2027*[190] a notamment été adoptée par le gouvernement français, présentant les axes de l'action du ministère de l'Europe et des affaires étrangères concernant le développement des médias à l'étranger. Dans un premier temps, la France entend améliorer l'environnement autour des médias, qui passe par une aide aux pays aux écosystèmes vulnérables afin de renforcer leur résilience face aux déstabilisations des systèmes médiatiques, soutenue par les Fonds équipes pays France (FEF), comme par exemple le projet *Medialogue* (programme axé sur la mise en réseau et renforcement des compétences des journalistes du Kirghizistan, du Kazakhstan, d'Ouzbékistan, et du Tadjikistan) ou le projet *Expressions balkaniques* (qui vise à développer l'éducation aux médias et sensibiliser aux manipulations de l'information dans les Balkans occidentaux), qui sont des programmes mis en place par Canal France international (CFI), opérateur de l'Etat en charge du développement des médias. La France agit également en faveur de la régulation de l'activité des plateformes numériques et du recours à l'IA, en promouvant de nouveaux cadres de régulation en faveur de l'intégrité de l'information, de la protection de la profession journalistique et de l'accès à une information fiable, vérifiée, indépendante et de qualité. L'appui à la production et à la diffusion de contenus fiables, l'intensification de la lutte contre la désinformation fait également partie des axes d'action du Ministère de l'Europe et des affaires étrangères, en veillant notamment à approfondir le soutien aux journalistes et à la société civile afin d'échanger avec eux concernant les outils, les avancées techniques et les bonnes pratiques pour lutter contre la désinformation. En ce sens, plusieurs objectifs sont poursuivis par la France : le renforcement des capacités des médias et de leurs personnels, en particulier des fact-checkeurs ; le renforcement des capacités techniques des médias ; la facilitation de la mise en réseau des fact-checkeurs ; le renforcement de la capacité de la société civile et des médias à développer l'éducation aux médias et à la citoyenneté civile. La France soutient ainsi plusieurs initiatives de la société civile, notamment l'Initiative pour la confiance dans le journalisme (label indépendant et transparent initié par Reporter sans frontières, certifiant l'engagement d'un média en faveur de l'intégrité de l'information). L'audiovisuel public extérieur français contribue également

[190] *Feuille de route Médias et développement*, MEAE, 2 novembre 2023. Lien ; https://www.diplomatie.gouv.fr/IMG/pdf/a4_feuille_route_medias_et_dev_2023-27_v8_bd_cle8d6286.pdf

activement à la poursuite de cet objectif, notamment avec le groupe France Médias Monde, à travers la diffusion de contenus de proximité en français et en langues locales.

La promotion de la liberté d'informer par la France passe également par la négociation de textes ambitieux au sein des organisations et enceintes internationales, ainsi que la protection des journalistes. Pour finir, l'action française afin d'assurer un environnement des médias ouvert et sûr passe également par l'éducation aux médias et à l'information.

Les initiatives françaises sont nombreuses en matière d'appui à l'environnement médiatique afin de promouvoir et de protéger la liberté d'expression à l'international. À l'occasion du Forum de Paris sur la Paix en 2022, la ministre de l'Europe et des Affaires étrangères de l'époque, Catherine Colona, a notamment annoncé l'installation à Paris du *Fonds international pour les médias d'intérêt public (IFPIM)* et de la contribution française à ce dernier à hauteur de 13 millions d'euros pour la période 2023-2024, auxquels s'ajoute un million d'euro via l'Organisation internationale de la francophonie. Ce fonds a pour objectif de financer des médias d'intérêt public fragiles dans des pays à revenus faibles et intermédiaires.

Canal France international (CFI) a également mis en place, depuis 2019, des *programmes* « *Désinfox* », financés par la Direction générale de la Mondialisation du développement (DGM) et des partenariats et le Centre de crise et de soutien (CDCS) du Ministère de l'Europe et des affaires étrangères, qui recouvrent différents projets d'appui à la résilience des écosystèmes médiatiques (journalistes, fact-checkeurs, blogueurs, étudiants, activistes) face aux manipulations informationelles. Les actions menées dans dix pays d'Afrique francophones (Togo, Bénin, Côte d'Ivoire, République centrafricaine, Sénégal, Cameroun, Tchad, Niger, Burkina Faso, Mali) visent à renforcer les compétences des journalistes et médias traditionnels aux techniques de vérification des faits, d'accompagner les médias et rédactions dédiés à ces pratiques spécifiques, de structurer ces initiatives à l'échelle francophone et régionale et de vulgariser ces outils auprès des jeunesses du continent et d'une audience élargie. La Plateforme africaine des fact-checkeurs francophones (PAFF) a également été lancée en avril 2024, avec le soutien de la DGM. Pour la période 2019-2023, le budget dédié à ces programmes était de trois millions d'euros, reconduit à hauteur de 2,85 millions d'euros jusqu'en 2027, avec un accent mis sur l'éducation aux médias et la structuration d'un réseau francophone de vérificateurs de faits.

Plus globalement, dans le cadre de sa politique de développement des médias, 40,2 millions d'euros ont notamment été investis en 2022 dans des projets de soutien aux médias à travers le monde. La DGM a investi 30 millions d'euros en 2023 pour la coopération en faveur des médias et la lutte contre la désinformation. De plus, 2,5 millions d'euros ont été investis par le Centre de crise et de soutien du Ministère de l'Europe et des affaires étrangères dans le domaine des médias en 2023, afin de nouer des partenariats avec CFI et des organisations non gouvernementales françaises locales et internationales.

2. Une action globale en faveur de la protection de la liberté d'expression en ligne

La France entend également renforcer la mobilisation européenne et internationale sur les enjeux de lutte contre les manipulations de l'information. A l'échelle européenne, la France promeut le renforcement de la souveraineté numérique européenne et le rapprochement des positions des Etats membres dans les négociations internationales sur ces sujets, par la co-construction et l'animation du réseau des ambassadeurs européens pour le numérique et la cybersécurité notamment. Cette initiative joue ainsi un rôle clé dans la promotion d'une approche coordonnée et stratégique de l'UE face aux défis numériques et cybernétiques mondiaux. La France échange également informellement et régulièrement avec le SEAE sur les bonnes pratiques et les outils de la diplomatie numérique française en termes de lutte contre les manipulations d'information afin de s'accorder sur la conceptualisation du phénomène et sur les réponses à y apporter.

Au niveau multilatéral, la France promouvoit également sa vision d'un espace numérique sûr et ouvert, et a notamment porté, avec plusieurs autres pays, la *résolution 47/16 sur la promotion, la protection et l'exercice des droits de l'Homme sur internet*[191] au Conseil des droits de l'Homme en 2021, qui encourage « *tous les États à prendre les mesures nécessaires et appropriées pour promouvoir un accès libre, ouvert, interopérable, fiable et sécurisé à Internet et, selon des modalités qui soient conformes à leurs obligations internationales relatives aux droits de l'homme, à s'attaquer à la désinformation et à l'apologie de la haine*

[191] *Résolution 47/16, La promotion, la protection et l'exercice des droits de l'Homme sur internet,* Conseil des droits de l'homme, 13 juillet 2021

qui constituent une incitation à la discrimination, à l'hostilité ou à la violence, afin de garantir la pleine jouissance des droits de l'homme ».

La France fait partie des pays à l'origine du *Partenariat international pour l'information et la démocratie*[192], lancé le 26 septembre 2019 et signé par 52 États. Ce partenariat international a pour objectif de répondre aux nouveaux défis posés par la révolution numérique en matière de liberté d'expression, tels que la désinformation massive en ligne, l'influence grandissante des acteurs privés, l'affaiblissement du journalisme professionnel ou encore le contrôle politique des médias, en posant des principes et des objectifs pour garantir l'accès à une information fiable, tant pour les États participants que pour les entreprises. Afin de mettre en œuvre les principes du Partenariat, un Forum sur l'information et la démocratie a notamment été mis en place en 2019 par Reporters sans frontières et plusieurs organisations indépendantes de la société civile.

B) Politique de protection des droits de l'Homme de la France face aux régimes autoritaires et lutte contre l'ingérence étrangère en ligne

1. La promotion des droits de l'Homme dans l'environnement numérique

En termes de promotion des droits de l'Homme en ligne, notamment de la liberté d'expression à l'échelle internationale, la France milite contre la censure numérique, les coupures d'Internet imposées par certains régimes, et les lois liberticides. En effet, ces restrictions numériques imposées par des régimes autoritaires afin de restreindre l'accès l'information ont pu être observées dans plusieurs pays, notamment au Burkina Faso lors des manifestations de l'opposition en 2021 qui ont mené à une coupure d'internet suivie d'une restriction d'accès à Facebook ou encore au Sri Lanka en 2022, avec une coupure de l'accès à toutes les plateformes à la suite des protestations contre la mise en place d'un état d'urgence.

La France promeut cette vision d'un internet libre et ouvert notamment du Conseil des droits de l'Homme, avec l'adoption de la *résolution 47/16 sur la promotion, la protection et*

[192] *Partenariat international pour l'information et la démocratie,* 26 septembre 2019. Lien : https://www.diplomatie.gouv.fr/IMG/pdf/partenariat_international_pour_l_information_et_la_democratie_vf_cle898723.pdf

l'exercice des droits de l'Homme sur internet[193] qui « *condamne sans équivoque les mesures qui, en violation du droit international des droits de l'homme, empêchent une personne de rechercher, de recevoir ou de répandre des informations en ligne ou qui compromettent sa capacité à le faire, notamment les coupures de l'accès à Internet et la censure en ligne, engage tous les États à mettre un terme à de telles mesures et à s'abstenir d'en prendre* ». La résolution demandait également au Haut-Commissariat des Nations Unies aux droits de l'homme de présenter une étude sur la tendance consistant à couper l'accès à Internet, en analysant les causes de ces coupures, leurs implications juridiques et leurs conséquences sur les droits de l'Homme.

La France est également engagée dans la lutte contre la répression numérique, en soutenant les activistes numériques, journalistes et organisations non gouvernementales confrontés à la surveillance ou à la censure, particulièrement dans des régimes répressifs. Elle applique notamment les *Orientations de l'UE sur les défenseurs des droits de l'Homme*[194] de 2004, révisées en 2008, qui visent à protéger les défenseurs des droits de l'Homme dans les pays tiers et englobent les défenseurs des droits numériques. La France participe également à des coalitions européennes ou internationales contre la surveillance de masse, la désinformation, ou la propagande d'État. La France finance par ailleurs des programmes d'appui à la société civile dans des pays autoritaires, notamment via l'Agence française de développement (AFD) et le Fonds de solidarité pour les projets innovants (FSPI) du ministère des Affaires étrangères.

2. La lutte active contre l'ingérence étrangère en ligne

En matière de lutte contre l'ingérence étrangère, la France dispose d'un Service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM), créé en 2021 et rattaché au secrétariat général de la défense et de la sécurité nationale (SGDSN), dont la mission principale est de préserver le débat public des manipulations de l'information provenant de l'étranger et visant à porter atteinte aux intérêts fondamentaux de la nation sur les plateformes numériques, via des investigations en sources ouvertes.

[193] *Op. cit.* n°191, p. 93
[194] *Orientations de l'UE concernant les défenseurs des droits de l'Homme*, Parlement européen, 2004, révisées en 2008. Lien : https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739386/EPRS_ATA(2023)739386_FR.pdf

Le 13 juin 2023, Catherine Colonna, ancienne Ministre de l'Europe et des affaires étrangères, a notamment dénoncé une *« campagne numérique de manipulation de l'information contre la France impliquant des acteurs russes et à laquelle des entités étatiques ou affiliées à l'État russe ont participé en amplifiant de fausses informations »*. Cette campagne de désinformation visant à affaiblir et inverser le soutien de la population européenne à l'Ukraine, baptisée « RRN », en raison du rôle joué par le média russe *Reliable Recent News*, a notamment touché plusieurs pays européens, dont la France. Elle a été suivie pendant plus d'un an par VIGINUM et a mené à la publication d'un *rapport technique*[195] en juin 2023, décrivant les différentes phases de cette campagne et mettant en évidence les marqueurs d'implication d'acteurs russes, notamment étatiques. Le rapport met en avant que cette campagne a consisté en la diffusion de contenus pro-russes liés à la guerre en Ukraine ; à l'usurpation de l'identité de médias européens et d'institutions gouvernementales pour y publier des contenus prorusses ; en la création de sites web d'actualités francophones partageant des contenus polémiques ainsi qu'en la mise en oeuvre de moyens inauthentiques combinés, tels que des faux-sites ou des faux compte sur les réseaux sociaux permettant de relayer les contenus. VIGINUM a notamment détecté que sur les 355 noms de domaine usurpant l'identité de médias, quatre ciblaient spécifiquement le public francophone et reprenaient l'identité graphique de quotidiens français (20 Minutes, le Monde, le Parisien, et le Figaro). De plus, l'identité du site web du Ministère de l'Europe et des affaires étrangères a été usurpée en mai 2023 dans le cadre de cette campagne de manipulation de l'information menée par la Russie. Le Ministère de l'Europe et des affaires étrangères, sur la base des investigations de VIGINUM, a ainsi constitué un dossier de sanctions européennes contre les individus et les sociétés impliqués dans la campagne RRN.

Plus globalement, la France, l'Allemagne et la Pologne, par une *déclaration conjointe*[196] du 12 février 2024 prononcée dans le cadre d'une réunion des pays du Triangle de Weimar en France, ont mis en avant leur volonté d'intensifier leur coordination à l'égard de la lutte contre la désinformation, les cyberattaques et les ingérences politiques de la Russie dans le

[195] *Rapport - RRN : une campagne de l'information complexe et persistance,* VIGINUM, Secrétariat de la défense et de la sécurité nationale, 13 juin 2023. Lien : https://www.sgdsn.gouv.fr/files/files/13062023_RRN_une%20campagne%20num%C3%A9rique%20de%20manipulation%20de%20l%27information%20complexe%20et%20persistante.pdf

[196] *Déclaration conjointe des ministères des affaires étrangères de France, d'Allemagne et de Pologne*, Réunion des pays du Triangle de Weimar, 12 février 2024. Lien : https://www.diplomatie.gouv.fr/fr/dossiers-pays/allemagne/le-triangle-de-weimar/article/reunion-des-pays-du-triangle-de-weimar-declaration-conjointe-des-ministres-des

contexte de la guerre avec l'Ukraine et maintenir un haut niveau d'exigence afin de protéger les citoyens. Les trois Etats ont annoncé, via cette déclaration, la mise en place d'un programme commun d'alerte et de réaction sur les manipulations de l'information et les ingérences étrangères, et ont mis en avant la nécessité que les plateformes prennent des mesures plus efficaces afin de combattre celles-ci.

VIGINUM a par ailleurs publié un *rapport* intitulé *« Manipulation d'algorithmes et instrumentalisation d'influenceurs ; enseignements de l'élection présidentielle en Roumanie & risques pour la France »*[197] portant sur les manipulations de l'information ayant ciblé les élections présidentielles roumaines de 2024, annulées a posteriori par la Cour constitutionnelle roumaine. Ce rapport analyse les modes opératoires observés essentiellement sur Tiktok, destinés à promouvoir artificiellement certains contenus, ainsi que l'instrumentalisation d'influenceurs et évalue le risque de leur transposition en France. Par la publication de ce rapport, VIGINUM souhaite notamment alerter les internautes sur le risque de manipulation des systèmes de recommandation de contenus sur les plateformes, mais également sensibiliser les créateurs de contenus bénéficiant d'une communauté importante en ligne sur les risques d'instrumentalisation dont ils pourraient faire l'objet.

La France a par ailleurs soutenu les mesures prises par la Commission européenne à l'encontre de Tik Tok dans le cadre des élections roumaines, et a mis en avant son soutien à la Roumanie pour lutter contre les ingérences numériques étrangères ciblant les démocraties.

La France a par ailleurs renforcé son cadre légal en adoptant une *loi visant à prévenir les ingérences étrangères en France*[198] en 2024, qui met en place des mesures en matière de transparence (nouveau registre des activités d'influence étrangère) et de renseignement (utilisation des algorithmes, gel des avoirs), et renforce également les sanctions pénales. Un registre des activités d'influence étrangère a été mis en place par cette loi, qui recensera, après déclaration auprès de la Haute autorité pour la transparence de la vie publique (HATVP) les activités des personnes agissant pour le compte d'un mandat étranger : puissances ou entités étrangères ou parties ou groupes politiques étrangers hors Union

[197] *Rapport - Manipulation d'algorithmes et instrumentalisation d'influenceurs : enseignements de l'élection présidentielle en Roumanie & risques pour la France*, VIGINUM, Secrétariat général de la défense et de la sécurité nationale, 4 février 2025, Lien : https://www.sgdsn.gouv.fr/publications/manipulation-dalgorithmes-et-instrumentalisation-dinfluenceurs-enseignements-de

[198] *Loi n°2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France*

européenne. La création de ce registre s'inspire notamment des Etats Unis (*Foreign Agents Registration Act*) et du Royaume Uni (*Foreign Influence Registration Scheme*). Les sanctions en cas de refus de transmission à la HATVP des informations (sur leur identité, leurs actions d'influence, les personnes approchées) sont de trois ans de prison et de 45 000 euros d'amende pour les personnes physiques, et peuvent aller jusqu'à 225 000 euros d'amende ou une interdiction de percevoir une aide publique pour les personnes morales.

Par ailleurs, la procédure de gel des avoirs financiers, autorisée en matière de terrorisme, est étendue aux affaires d'ingérences étrangères. Les personnes se livrant à de tels actes, les incitant ou les finançant pourront ainsi voir leurs fonds et ressources gelés en France.

CONCLUSION

Internet est un espace réputé sans frontières qui a donc nécessairement une dimension internationale, notamment au regard de la problématique du transfert des données. Le cyberespace est un espace international nouveau, dit transnational et sa nature appelle à une gouvernance mondiale protectrice des droits de l'Homme. Le droit international, et plus spécifiquement le droit international des droits de l'Homme, qui vise à lutter contre la discrimination, les inégalités et protéger de nombreux droits inhérents à l'être humain, a pour ambition de faire respecter les droits qui s'appliquent hors ligne en ligne. Cette analogie est nécessaire afin de pouvoir suivre les avancées technologiques dans un monde de plus en plus digital.

Toutefois, le cadre juridique est fragmenté, ce qui diminue l'impact de promotion et de protection des droits de l'Homme. En plus d'être fragmenté, il existe un écart entre les standards internationaux qui sont moins protecteurs que les standards européens. L'UE essaye en effet de s'imposer dans le domaine du numérique en régulant cet espace. Cependant, depuis 2002, les Etats-Unis incarnent le leader mondial de la diplomatie numérique. Cette position dominante rend difficile l'application de la réglementation européenne aux acteurs extraterritoriaux, et par conséquent l'application des standards en matière de droits de l'Homme à l'espace numérique[199].

Concernant plus spécifiquement le domaine de l'IA, la France semble privilégier une dynamique de compétitivité internationale, en s'efforçant de maintenir son rang dans la gouvernance mondial de l'IA, parfois au détriment d'une réflexion plus approfondie sur les garanties effectives des droits fondamentaux. Dans ce contexte, la France tente de s'imposer face aux Etats Unis et ses géants du web. En multipliant des partenariats stratégiques, notamment avec l'Inde, la France réussit à promouvoir une vision plus éthique de l'utilisation de l'IA. Si l'intégration constante de l'IA dans les services publics témoigne d'une volonté d'efficacité et de modernisation de l'action publique, elle continue de susciter des interrogations quant à la protection des droits de l'Homme. Enfin, il convient de souligner les efforts notables déployés par cette dernière en matière de protection des données personnelles.

---

[199] GOMART T., "*DE LA DIPLOMATIE NUMÉRIQUE.",* Revue Des Deux Mondes, 2013, 131–41. Lien : http://www.jstor.org/stable/44194679

En outre, au delà du sujet de cette étude, la France s'impose aussi en diplomatie numérique par son utilisation des nouvelles plateformes numériques de communication :

> *« l'Allemagne et la France ont su prendre le virage du numérique et s'avèrent être les premiers États à institutionnaliser une diplomatie publique transnationale »*[200].

Ainsi, les technologies numériques modifient les rapports de forces géopolitiques et jouent un rôle majeur dans les relations internationales. L'importance des technologies est telle qu'est née une « guerre de l'information » :

> « *Si l'ensemble des conflits ont une composante informationnelle, la guerre en Ukraine – comme la résurgence du conflit israélo-palestinien depuis octobre 2023 – se distingue par la circulation démesurée, sur les réseaux sociaux notamment, de données en provenance du terrain, produites le plus souvent en temps réel. Ces flux informationnels, qui pour la plupart ne sont plus filtrés par les contrôleurs d'accès (gatekeepers) médiatiques traditionnels, alimentent massivement et quotidiennement la « guerre de l'information » qui s'entremêle dans la guerre conventionnelle* »[201].

En matière de lutte contre la cybercriminalité, la France s'impose comme un acteur central de la gouvernance mondiale du cyberespace, en promouvant un numérique à la fois sûr, libre et respectueux des droits fondamentaux. Par ses initiatives telles que l'*Appel de Paris* ou l'*Appel de Christchurch*, elle encourage une coopération internationale renforcée entre États, secteur privé et société civile. Son action s'inscrit dans une volonté de répondre efficacement aux menaces croissantes que représentent la cybercriminalité et l'utilisation malveillante des technologies, tout en développant la résilience des infrastructures numériques. En articulant sécurité, liberté et responsabilité, la France entend ainsi contribuer à un cadre global qui garantisse la stabilité du cyberespace et la protection des citoyens à l'ère numérique.

La France défend également activement une vision d'un internet libre, ouvert et

---

[200] HOUGET A., JOSSET B., *« Vers une diplomatie numérique transnationale »*, Questions de communication, 44 | 2023, 155-182. Lien : https://journals.openedition.org/questionsdecommunication/pdf/33083

[201] LYUBAREVA I., NOCETTI J., *« La diplomatie numérique Évolution des stratégies diplomatiques et d'influence à l'ère (du) numérique »*. Réseaux, 2024, 2024/3 N° 245, p.11-35, Lien : https://shs.cairn.info/revue-reseaux-2024-3-page-11?lang=fr

sécurisé, en promouvant la liberté d'expression en ligne et en luttant contre la désinformation et les ingérences étrangères. Par une action diplomatique multilatérale, des soutiens financiers concrets aux médias indépendants et des initiatives éducatives, elle renforce la résilience des écosystèmes médiatiques face aux manipulations de l'information. Son engagement s'inscrit dans une volonté de protéger les droits fondamentaux, de soutenir les sociétés civiles et de faire face aux menaces numériques qui pèsent sur les démocraties. Cette diplomatie numérique s'appuie sur une coopération renforcée au niveau européen et international, pour répondre collectivement aux défis posés par l'environnement numérique globalisé.

Sur la protection des droits de l'enfant, la France mène ses négociations internationales autour de la protection de l'intérêt supérieur de l'enfant à l'ère du numérique en recherchant un équilibre entre la lutte contre les dangers en ligne - tels que l'exposition aux contenus violents ou le harcèlement - et la promotion des opportunités que le numérique peut offrir en matière d'éducation, de participation et de développement. L'éducation est ainsi au cœur de son approche, considérée comme un levier essentiel pour renforcer la résilience des enfants face aux risques numériques. La France insiste également sur la nécessité de mobiliser une pluralité d'acteurs et de tirer parti de l'innovation et des ressources du secteur privé. Ces ambitions se heurtent à deux limites majeures : un manque persistant de gouvernance coordonnée et un sous-financement des initiatives, notamment dans les pays les plus vulnérables. Pour traduire ses engagements en résultats concrets, la France devrait donc transformer ses principes diplomatiques en actions durables, inclusives et suffisamment dotées de moyens.

Concernant la diplomatie française sur le numérique, l'étude a montré qu'il existe parfois un écart entre le cadre juridique, l'engagement international et les initiatives *in fine*. Cet écart est d'autant plus accentué par le manque de transparence.

C'est pourquoi l'étude a permis de formuler les recommandations suivantes.

RECOMMANDATIONS

1. Les avancées technologiques ne sauraient se faire au détriment des droits de l'Homme. Une approche davantage préventive, axée sur l'anticipation des atteintes potentielles, devrait être privilégiée par la France.
2. Toute collecte ou utilisation de données de communication doit être autorisée par une autorité judiciaire et doit être strictement proportionnée à l'accomplissement des objectifs légitimes reconnus en vertu du droit international sur les droits de l'Homme, comme la protection de la sécurité nationale et de la sûreté publique.
3. Dans le cadre de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (« loi SILT ») et la loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, la France doit limiter le recours aux mesures administratives fondées sur des informations secrètes. Elle doit privilégier les poursuites pénales dans le respect des garanties du procès équitable et doit garantir un droit effectif à un recours juridictionnel.
4. La France doit rendre public les données précises et désagrégées sur l'usage des mesures concernant l'utilisation d'un modèle d'IA dans l'algorithme concernant l'utilisation de mesures de police administrative visant à prévenir des actes de tettorisme.
5. Dans la régulation des technologies émergentes, la France doit anticiper et influencer sur les technologies pour évoluer sur le long terme, comme précisé dans le Pacte mondial sur le numérique qui se veut intemporel. Il convient de ne pas rester dans la position réactive de réponse aux crises. En effet, quand les crises liées aux technologies touchent la santé mentale des mineurs, elles ont déjà des conséquences importantes sur le développement psychique des enfants qu'il est compliqué d'effacer par la suite.
6. Concernant l'encadrement des deep fakes, aucun cadre juridique international contraignant concernant spécifiquement cette question n'existe à ce jour. La France doit donc être à l'initiative de normes contraignantes en la matière.
7. La France doit également inciter en faveur de l'adoption d'un texte international afin d'encadrer les activités terroristes en ligne.
8. Sur la question spécifique de la protection des défenseurs des droits de l'Homme, comprenant les défenseurs des droits du numérique, il est nécessaire que la France se dote d'un cadre juridique permettant de les protéger au niveau national.

9. La France fait régulièrement participer la société civile dans ses initiatives internationales. Toutefois, pour les projets concernant les enfants, la France devrait insister davantage sur l'importance de placer les enfants au centre des politiques publiques.
10. L’éducation est un levier important dans la lutte contre les violations des droits des enfants dans l'environnement numérique. En plus de vouloir éduquer les enfants, sensibiliser et responsabiliser les parents, la France devrait davantage éduquer les groupes aux législations, conformément à ce que fait déjà l’UE qui va jusqu'à les sanctionner.
11. Investir davantage de financement dans des initiatives internationales.

BIBLIOGRAPHIE

I. DOCTRINE

A) Ouvrages

- ALOMBERT A., *Schizophrénie numérique: La crise de l'esprit, à l'ère des nouvelles technologies*, Editions Allia, 2024, 96p.
- BARBÉ V., MAUCLAIR S., *Intelligence Artificielle & Droits Fondamentaux*. 2022. Print. Collection L'Unité Du Droit Volume XXXII, 140p.
- BARRAUX B., *Humanisme et Intelligence Artificielle: Théorie Des Droits de L'Homme Numérique*. L'Harmattan, 2022. Print. Le Droit Aujourd'Hui, 646p.
- BIAD A. et PARISOT V. (Dir.), *La Charte des droits fondamentaux de l'Union européenne*, Anthemis, Collection Droit & Justice, 2018, 586 p.
- LOCHAK D., *Les droits de l'homme*, La Découverte, Collection Repères, 2024, 5ème éd., 128 p.

B) Articles

- DESMOULIN-CANSELIER S., LE MÉTAYER D., *Décider avec les algorithmes*, Dalloz.
- GOMART T.. *« DE LA DIPLOMATIE NUMÉRIQUE. »*, Revue Des Deux Mondes, 2013, 131–41, Lien : http://www.jstor.org/stable/44194679
- HUTTNER L., *« Le Contrôle de L'Accès Des Mineurs Aux Sites Pornographiques »*, Dalloz IP/IT : droit de la propriété intellectuelle et du numérique 7 (2024): Dalloz IP/IT : droit de la propriété intellectuelle et du numérique, 2024-07 (7). Print.
- HOUGUET A., JOSSET B., « *Vers une diplomatie numérique transnationale* », Questions de communication, 2023, 44, pp.155-182, Lien : https://journals.openedition.org/questionsdecommunication/pdf/33083
- JOLICOEUR M-P., *« Vérifier l'âge des internautes sur les sites pornographiques pour en limiter l'accès aux personnes mineures : une mesure novatrice et nécessaire pour le droit canadien »* dans Ledy Rivas Zannou, Eve Gaumond et Michael Lang (dir.), Rencontres. Regards croisés sur la justice, Lex Electronica(2023) 28-2, p. 79-121. Lien: https://www.lex-electronica.org/en/s/2852
- LYUBAREVA I., NOCETTI J., *« La diplomatie numérique Évolution des stratégies diplomatiques et d'influence à l'ère (du) numérique »*. Réseaux, 2024, 2024/3 N° 245, p.11-35, Lien : https://shs.cairn.info/revue-reseaux-2024-3-page-11?lang=fr
- RIVOLLIER V., *Datajust. Histoire d'un échec,* Séminaire Nouvelles technologies et justice, Centre internet et société, Mars 2023, Lien : Datejust. Histoire d'un échec - Archive ouverte HAL

II. DOCUMENTS OFFICIELS

A) Sources officielles internationales

1. Organisation des Nations Unies

a) Normes

- *Charte Africaine des Droits de l'Homme et des Peuples*, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), 27 juin 1981, entré en vigueur 21 octobre 1986
- Nations Unies. (1989). *Convention relative aux droits de l'enfant*
- *Convention des Nations Unies contre la cybercriminalité*, 24 décembre 2024
- Nations Unies. (1966). *Convention internationale sur l'élimination de toutes les formes de discrimination raciale*. Recueil des Traités, 660, 195
- *Déclaration universelle des droits de l'homme*, Nations Unies, 1948
- *Pacte international relatif aux droits civils et politiques*, Nations Unies, 1966
- *Pacte mondial de l'ONU*, 2000
- *Principes directeurs relatifs aux entreprises et aux droits de l'homme*, HCDH, 2011
- *Principes de l'OCDE sur l'intelligence artificielle*, 2019

b) Instruments et documents complémentaires des Comités, organes et agences des Nations Unies

i. Assemblée générale des Nations Unies

- *Recommandation 3C – Promouvoir une gouvernance éthique de l'intelligence artificielle au sein du système des Nations Unies*. Groupe de haut niveau sur la coopération numérique, *L'ère de l'interdépendance numérique* (rapport présenté par le Secrétaire général de l'ONU), 2020
- *Pacte pour l'avenir « Pacte numérique mondial », Projet de résolution* A/79/L.2, *déposé par le Président de l'Assemblée générale*, 20 septembre 2024
- *Rapport du Secrétaire général, Combattre la désinformation pour promouvoir et protéger les droits humains et les libertés fondamentales*, A/77/287, 12 août 2022
- *Rapport du Secrétaire général, Intensification de l'action menée pour éliminer toutes les formes de violence à l'égard des femmes et des filles : violence contre les femmes et les filles facilitée par les technologies*, A/79/500, 8 octobre 2024
- *Résolution A/C.1/78/L.60/Rev.1, Programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale*, 24 octobre 2023
- *Résolution A/RES/76/227, Combattre la désinformation pour promouvoir et protéger les droits humains et les libertés fondamentales*, 24 décembre 2021
- *Résolution A/RES/79/243*, *Convention des Nations Unies contre la cybercriminalité ; Renforcement de la coopération internationale pour la lutte contre certaines infractions commises au moyen de systèmes d'information et de communication et pour la communication de preuves sous forme électronique d'infractions graves,* 31 décembre 2024

ii. Conseil des droits de l'Homme

- *Compte rendu de séance, Le Conseil des droits de l'homme se penche sur les défis et opportunités pour le plein exercice par les enfants de leurs droits dans l'environnement numérique*, 10 mars 2023, Lien : https://www.ohchr.org/fr/news/2023/03/it-may-be-time-reinforce-universal-access-internet-human-right-not-just-privilege-high
- *Rapport A/79/520 de la Rapporteuse spéciale sur le droit à l'éducation,* 16 octobre 2024
- *Rapport A/HRC/48/31 du Haut-Commissariat sur l'intelligence artificielle, la vie privée et les droits de l'homme*, version préliminaire, 2021
- *Résolution 31/7, Les droits de l'enfant : les technologies de l'information et de la communication et l'exploitation sexuelle des enfants*, 23 mars 2016
- *Résolution 32/13, La promotion, la protection et l'exercice des droits de l'homme sur Internet*, 1er juillet 2016
- *Résolution 47/16, La promotion, la protection et l'exercice des droits de l'Homme sur internet,* 13 juillet 2021
- *Résolution 58/23, Défenseurs des droits humains et technologies nouvelles et émergentes : protéger les défenseurs et défenseuses des droits humains à l'ère numérique*, 28 mars 2025

iii. Haut-Commissariat aux droits de l'homme

- BACHELET M., *Les risques d'atteinte à la vie privée liés à l'intelligence artificielle nécessitent une action urgente*, 2021, Lien : Michelle Bachelet : les risques d'atteinte à la vie privée liés à l'intelligence artificielle nécessitent une action urgente | OHCHR
- *Haut-Commissaire : l'intelligence artificielle doit être ancrée dans les droits de l'homme*, 2023, Lien : https://www.ohchr.org/fr/statements/2023/07/artificial-intelligence-must-be-grounded-human-rights-says-high-commissioner
- *Le droit à la vie privée à l'ère du numérique, A/HRC/51/17, Assemblée générale, Conseil des droits de l'homme, 51e session 12 septembre–7 octobre 2022, Lien :* https://undocs.org/fr/A/HRC/51/17
- *Le HCDH et le droit à la vie privée à l'ère du numérique*, 2023, Lien : https://www.ohchr.org/fr/privacy-in-the-digital-age
- *Observation générale no 25 (2021) sur les droits de l'enfant en relation avec l'environnement numérique*, CRC/C/GC/25, 2 mars 2021
- *Projet B-Tech : technologies, droits de l'homme et entreprises*, 2021, Lien : https://www.ohchr.org/fr/business/b-tech-project
- TÜRK Volker, *« Human rights must be at the core of generative AI technologies »*, discours prononcé à l'Université de Stanford, 14 février 2024, Lien : https://www.ohchr.org/fr/statements-and-speeches/2024/02/human-rights-must-be-core-generative-ai-technologies-says-turk

iv. Comité des droits de l'enfant

- *Observations finales CRC/C/FRA/CO/6-7 concernant le rapport de la France valant sixième et septième rapports périodiques*, 4 décembre 2023
- *Observation générale n°25 CRC/C/GC/25, sur les droits de l'enfant en relation avec l'environnement numérique*, 02 mars 2021

v. UNICEF

- *Rapport - la situation des enfants dans le monde 2017 - les enfants dans un monde numérique*, 2017
- *Rapport sur les enfants à l'ère numérique, Mieux protéger les enfants dans un monde numérique tout en améliorant l'accès à Internet des plus défavorisés*, 11 décembre 2017

vi. UNESCO

- *Forum mondial sur l'éthique de l'intelligence artificielle*, février 2024, Lien : https://www.unesco.org/fr/articles/forum-mondial-sur-lethique-de-lintelligence-artificielle-2024
- *Le partenariat UNESCO/UE de lutte contre la désinformation et les discours de haine à l'échelle mondiale se développe,* 25 février 2025, Lien : https://www.unesco.org/fr/articles/le-partenariat-unesco/ue-de-lutte-contre-la-desinformation-et-les-discours-de-haine-lechelle
- *Recommandation sur l'éthique de l'intelligence artificielle*, 2021, Lien : https://www.unesco.org/fr/ethics-artificial-intelligence
- *Réseaux sociaux pour la paix,* 27 décembre 2022 (dernière mise à jour 16 novembre 2023), Lien : https://www.unesco.org/fr/articles/reseaux-sociaux-pour-la-paix

2. Autres organisations internationales et forums internationaux

- *Déclaration de Dinard sur l'initiative pour des normes dans le cyberespace*, G7, 5 avril 2019, Lien : https://www.elysee.fr/admin/upload/default/0001/04/1aa18fff8ca04e2f0bb984a29612368e0c9063c4.pdf
- *Déclaration des chefs d'Etats et du gouvernement,* Sommet du G20 d'Osaka, 2019, Lien : https://www.diplomatie.gouv.fr/IMG/pdf/19-2160-final_g20_osaka_leaders_declaration_fr_cle419f81.pdf
- Communiqué de presse, *Engagement en faveur de la cyberdéfense*, OTAN, 8 juillet 2016, Lien : https://www.nato.int/cps/en/natohq/official_texts_133177.htm?selectedLocale=fr

- *Livre Blanc « L'ONU, la cybersécurité et la lutte contre la cybercriminalité : le difficile consensus »,* Agora InCyber, 2024, Lien : https://europe.forum-incyber.com/wp-content/uploads/2024/11/AGORA_INCYBER_Livre_Blanc_ONU_NOV_2024.pdf
- *Rapport sur la prévention des violences en ligne contre les enfants, « What works to prevent violence against children online? »,* OMS, 24 novembre 2022

3. Déclarations, appels bilatéraux et multipartites

- MACRON E., ARDERN J., *Appel de Christchurch*, 15 mai 2019, Lien : https://www.christchurchcall.org/content/files/2024/06/Appel-de-Christchurch-texte-complet-francais-1.pdf
- MACRON E., *Appel de Paris pour la confiance et la sécurité dans le cyberespace*, 11 novembre 2018, Lien : https://pariscall.international/fr/call
- Gouvernements français, allemand et polonais, *Déclaration conjointe des ministères des affaires étrangères de France, d'Allemagne et de Pologne*, Réunion des pays du Triangle de Weimar, 12 février 2024, Lien : https://www.diplomatie.gouv.fr/fr/dossiers-pays/allemagne/le-triangle-de-weimar/article/reunion-des-pays-du-triangle-de-weimar-declaration-conjointe-des-ministres-des
- *Déclaration de Toronto sur la protection des droits à l'égalité et à la non-discrimination dans les systèmes d'apprentissage automatique*, 2018, Lien : https://www.torontodeclaration.org/wp-content/uploads/2019/12/Toronto_Declaration_French.pdf
- Gouvernements français, espagnol et grec, *Document politique de la France, l'Espagne et la Grèce envoyé à la Commission européenne, « Protecting Minors from Online harms and risks: Age verification, age - appropriate design and a pan-European digital age of majority »*, mai 2025, Lien : https://www.euractiv.fr/wp-content/uploads/sites/3/2025/05/Euractiv-1-2-1.pdf
- *Partenariat international pour l'information et la démocratie,* 26 septembre 2019, Lien : https://www.diplomatie.gouv.fr/IMG/pdf/partenariat_international_pour_l_information_et_la_democratie_vf_cle898723.pdf

B) Sources officielles régionales

1. Conseil de l'Europe

a) Conventions, protocoles et autres normes

- *Convention-cadre sur l'intelligence artificielle, les droits de l'homme, la démocratie et l'État de droit*, 2024
- *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108)*, 1981
- *Convention de Budapest sur la cybercriminalité*, 23 novembre 2001

- *Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques* (STCE n°224), 2023
- *Manuel pour les décideurs politiques sur les droits de l'enfant dans l'environnement numérique*, décembre 2020
- *Priorités pour sa coopération avec le Conseil de l'Europe 2020-2022*, 2020
- *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques* (STE N°289), 2003
- *Stratégie pour les droits de l'enfant (2022-2027)*, mars 2022

b) Décisions et recommandations

- *Recommandation CM/Rec(2018)7 du Comité des Ministres sur les Lignes directrices relatives au respect, à la protection et à la réalisation des droits de l'enfant dans l'environnement numérique,* 4 juillet 2018
- *Recommandation CM/Rec(2016)5[1] du Comité des Ministres du Conseil de l'Europe aux États membres sur la liberté d'Internet,* 13 avril 2016

c) Doctrine et manifestations scientifiques

- *Conférence : L'intelligence artificielle et les droits de l'homme – Nouveaux horizons dans la protection juridique européenne*, Palais des droits de l'homme, 24 avril 2025, Lien : https://www.echr.coe.int/fr/w/conference-artificial-intelligence-and-human-rights
- DAEMS R., *Conférence « Les droits de l'homme à l'ère de l'IA » - Intelligence artificielle*, allocution du Président de l'Assemblée parlementaire du Conseil de l'Europe, 20 janvier 2021, Lien : https://rm.coe.int/1680a05b58
- *Étude de faisabilité sur un cadre juridique pour l'intelligence artificielle fondé sur les normes du Conseil de l'Europe* CAHAI(2020)23-final, décembre 2020, Lien : https://rm.coe.int/cahai-2020-23-final-etude-de-faisabilite-fr-2787-2531-2514-v-1/1680a1160f
- *HUDERIA – Évaluation des risques et des impacts des systèmes d'IA*, 2024, Lien : https://www.coe.int/fr/web/artificial-intelligence/huderia-risk-and-impact-assessment-of-ai-systems
- *« Les droits humains à l'ère de l'intelligence artificielle »*, 2021, Lien : https://www.coe.int/fr/web/artificial-intelligence/human-rights-in-the-era-of-ai
- *Participation du président du CAI à la conférence de haut niveau des institutions de l'Ombudsperson et des INDH*, 2024, Lien : https://www.coe.int/fr/web/artificial-intelligence/-/cai-chair-participation-in-high-level-conference-for-ombudsperson-institutions-and-national-human-rights-institutions-nhri-

2. Union Européenne

a) Règlements et directives

- *Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (Directive SRI)*
- *Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information (Directive sur le commerce électronique)*
- *Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (refonte)*
- *Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)*
- *Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (AI Act)*, 2021
- *Règlement (UE) 2019/796 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses Etats membres*
- *Règlement (UE) 2024/2642 du Conseil du 8 octobre 2024 concernant des mesures restrictives eu égard aux activités déstabilisatrices menées par la Russie*
- *Règlement (UE) 2024/1083 du Parlement européen et du Conseil du 11 avril 2024 établissant un cadre commun pour les services de médias dans le marché intérieur et modifiant la directive 2010/13/UE (règlement européen sur la liberté des médias)*
- *Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724*
- *Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données)*
- *Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (Digital Services Act)*
- *Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 sur les marchés contestables et équitables dans le secteur numérique (Digital Markets Act)*
- *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 (RGPD)*
- *Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne*
- *Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la*

certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité)

- *Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) no 300/2008, (UE) no 167/2013, (UE) no 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)*
- *Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyber résilience)*

b) *Commission européenne*

- *Code de bonnes pratiques contre la désinformation,* 2018
- *Code renforcé de bonnes pratiques contre la désinformation,* 2022
- *Code des bonnes pratiques contre la désinformation 2022,* 13 février 2025, Lien : https://digital-strategy.ec.europa.eu/fr/policies/code-practice-disinformation
- Communiqué de presse, *« La Commission envoie une demande d'informations à Meta au titre de la législation sur les services numériques »*, Commission européenne, 1 décembre 2023, Lien : https://digital-strategy.ec.europa.eu/fr/news/commission-sends-request-information-meta-under-digital-services-act
- Communiqué de presse, *« La Commission envoie des demandes d'informations à YouTube, Snapchat et TikTok sur les systèmes de recommandation au titre de la législation sur les services numériques »*, Commission européenne, 2 octobre 2024, Lien : https://digital-strategy.ec.europa.eu/fr/news/commission-sends-requests-information-youtube-snapchat-and-tiktok-recommender-systems-under-digital
- *Contenus terroristes en ligne,* Lien : https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online_en?prefLang=fr&etrans=fr
- *Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis*
- *Décision d'exécution (UE) 2023/1795 de la Commission du 10 juillet 2023 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE - États-Unis*

- *Déclaration européenne sur les droits et principes numériques pour la décennie numérique,* 26 janvier 2022, COM(2022) 28 final
- *New Better Internet for Kids Strategy (BIK+) : compendium of EU formal texts concerning children in the digital world : 2024 edition*, Office des publications de l'Union européenne, 2024, Lien : https://data.europa.eu/doi/10.2759/90437
- *« Entrée en vigueur du règlement sur la cyber-résilience afin de rendre le cyberespace européen plus sûr et plus sécurisé »,* 10 décembre 2024, Lien : https://digital-strategy.ec.europa.eu/fr/news/cyber-resilience-act-enters-force-make-europes-cyberspace-safer-and-more-secure
- *Étude comparative portant sur le droit administratif et l'utilisation de l'IA et d'autres systèmes algorithmiques en matière de prise de décision administrative dans les États membres du Conseil de l'Europe* (Point 5.5 du projet d'ordre du jour), Comité européen de coopération juridique (CDCJ), 99e réunion, 23-25 novembre 2022
- *Forum Internet de l'Union européenne,* 20 mai 2025, Lien : https://home-affairs.ec.europa.eu/networks/european-union-internet-forum_en?prefLang=fr&etrans=fr
- *Le Code de conduite contre la désinformation,* 13 janvier 2025*,* Lien : https://digital-strategy.ec.europa.eu/fr/library/code-conduct-disinformation
- *Législation européenne sur la liberté des médias*, Lien : https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/european-media-freedom-act_fr
- *Lignes directrices en matière d'éthique pour une IA digne de confiance*, Groupe d'experts indépendants de haut niveau sur l'intelligence artificielle, Commission européenne, juin 2018
- *Lutte contre la désinformation en ligne*, 15 octobre 2024, Lien : https://digital-strategy.ec.europa.eu/fr/policies/online-disinformation
- *Lutter contre la désinformation en ligne : une approche européenne,* Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, 26 avril 2018, COM(2018) 236 final
- « *Loi sur les services numériques : garantir un environnement en ligne sûr et responsable* », 2022, Lien : https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_fr
- *Observatoire européen des médias numériques (EDMO)*, 16 octobre 2024, Lien : https://digital-strategy.ec.europa.eu/fr/policies/european-digital-media-observatory
- *Plan d'action en faveur des droits de l'homme et de la démocratie 2020-2024*, mars 2020
- *Plan d'action contre la désinformation***,** Communication conjointe au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions, 5 décembre 2018, JOIN(2018) 36 final
- *Plan d'action pour la démocratie européenne*, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, 3 décembre 2020, COM(2020) 790 final

c) *Conseil européen, Conseil de l'Union européenne*

- *Boussole stratégique en matière de sécurité et de défense - Pour une Union européenne qui protège ses citoyens, ses valeurs et ses intérêts, et qui contribue à la paix et à la sécurité internationales*, Conseil de l'Union européenne, 21 mars 2022
- *Conclusions du Conseil 10474/17 du 19 juin 2017 relatives à un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance ("boîte à outils cyberdiplomatique")*
- *Conclusions du Conseil 11406/2022 du 18 juillet 2022 sur la diplomatie numérique de l'UE*
- *Décision (PESC) 2024/3174 du Conseil du 16 décembre 2024 modifiant la décision (PESC) 2024/2643 concernant des mesures restrictives eu égard aux activités déstabilisatrices menées par la Russie*
- *Décision (PESC) 2019/797 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres*
- *Lignes directrices 10289/23 du Conseil du 8 juin 2023 relatives à la mise en œuvre de la boîte à outil cyberdiplomatique*
- *Lutter contre la diffusion de contenus à caractère terroriste en ligne,* Lien : https://www.consilium.europa.eu/fr/infographics/terrorist-content-online/
- *« Sanctions de l'UE à l'encontre de la Russie »*, 26 mai 2025, Lien : https://www.consilium.europa.eu/fr/policies/sanctions-against-russia/#hybrid
- *« Sanctions liées aux cyberattaques »,* 12 mai 2025, Lien : https://www.consilium.europa.eu/fr/policies/sanctions-against-cyber-attacks/

d) *Parlement européen*

- *Orientations de l'UE concernant les défenseurs des droits de l'Homme*, 2004, révisées en 2008, Lien : https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739386/EPRS_ATA(2023)739386_FR.pdf
- *Synthèse exécutive – Étude pour la commission PEGA : Utilisation de Pegasus et de logiciels espions de surveillance équivalents. Cadre juridique des États membres en matière d'acquisition et d'utilisation de Pegasus et de logiciels espions de surveillance équivalents*, Bruxelles, Parlement européen, 2022, Lien : Utilisation de Pegasus et de logiciels espions de surveillance équivalents - Cadre juridique des États membres en matière d'acquisition et d'utilisation

e) *Autres organes*

- *Avis 28/2022 sur les critères de certification Europrivacy en ce qui concerne leur approbation par le comité en tant que label européen de protection des données conformément à l'article 42, paragraphe 5 (RGPD),* Comité européen de la protection des données, 10 octobre 2022

- *« Les droits humains à l'ère de l'intelligence artificielle : Construire notre avenir numérique »*, Service européen pour l'action extérieure (SEAE), 2020, Lien : https://www.eeas.europa.eu/eeas/human-rights-age-artificial-intelligence-shaping-our-digital-future_en
- *Regulating for an Equal AI: A New Role for Equality Bodies*, juin 2020, European Network of Equality Bodies, Lien : https://equineteurope.org/wp-content/uploads/2020/06/ai_report_digital.pdf

f) Cour de Justice de l'Union européenne

- *Cour de justice de l'Union européenne, Maximillian Schrems/Data Protection Commissioner (Schrems I), 6 octobre 2015, C-362/14, EU:C:2015:650*
- *Cour de justice de l'Union européenne, Data Protection Commissioner/Facebook Ireland Ltd et Maximillian Schrems (Schrems II), 16 juillet 2020, C-311/18, EU:C:2020:559*

C) Sources officielles nationales

1. Dispositions législatives et réglementaires

- *Déclaration des droits de l'homme et du citoyen*, 1789
- *Loi n° 2023-380 du 19 mai 2023 relative aux Jeux Olympiques et Paralympiques de 2024*
- *Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.*
- *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, modifiée par le RGPD en 2018
- *Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.*
- *Loi n°2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France*

2. Institutions gouvernementales

a) Présidence

- *Appel à l'action : défendre les droits de l'enfant dans l'environnement numérique,* Elysée, 11 novembre 2021, Lien : https://www.elysee.fr/emmanuel-macron/2021/11/11/communique-de-presse-conjoint-entre-la-presidence-de-la-republique-et-le-fonds-des-nations-unies-pour-lenfance
- *Charte du Laboratoire pour la protection de l'enfance en ligne,* Elysée, 8 novembre 2023, Lien : https://www.elysee.fr/emmanuel-macron/2023/11/08/charte-du-laboratoire-pour-la-protection-de-lenfance-en-ligne

- *Conférence de presse d'Emmanuel Macron et Jacinda Ardern,* Elysée, 15 mai 2019, Lien : https://www.elysee.fr/front/pdf/elysee-module-3273-fr.pdf
- Communiqué de presse, *Bilan et orientations du Laboratoire pour la protection de l'enfance en ligne*, Ministère de l'économie, des finances et la souveraineté industrielle et numérique, n°1328, Lien : https://presse.economie.gouv.fr/09112023-cp-bilan-et-orientations-du-laboratoire-pour-la-protection-de-lenfance-en-ligne/

b) Ministères

- *« Appel de Christchurch, une initiative ambitieuse au service d'un internet ouvert, libre et sûr »*, MEAE, Lien : https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/article/l-appel-de-christchurch-une-initiative-ambitieuse-au-service-d-un-internet
- *Communiqué conjoint du ministère de l'Europe et des Affaires étrangères et du secrétariat d'État chargé de l'Enfance*, 9 mai 2023, Lien : https://solidarites.gouv.fr/nations-unies-comite-des-droits-de-lenfant-examen-du-respect-de-la-france-de-la-convention
- *Déclaration conjointe sur les droits de l'enfant dans l'environnement numérique*, MEAE, 11 mars 2022, Lien : https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/societe-civile-et-volontariat/evenements-incluant-la-societe-civile/forum-de-paris-sur-la-paix/4e-edition-du-forum-de-paris-sur-la-paix/article/la-france-appelle-a-defendre-les-droits-de-l-enfant-dans-l-environnement#sommaire_2
- *« Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne »*, VILLANI C, Rapport au Premier ministre, mars 2018
- *Feuille de route Médias et développement*, MEAE, 2 novembre 2023, Lien : https://www.diplomatie.gouv.fr/IMG/pdf/a4_feuille_route_medias_et_dev_2023-27_v8_bd_cle8d6286.pdf
- *« Garantir la cybersécurité »,* MEAE, janvier 2022, Lien : https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/garantir-la-cybersecurite/
- *Le laboratoire pour les droits des femmes en ligne*, juillet 2024, MEAE, Lien : https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-feministe/le-laboratoire-pour-les-droits-des-femmes-en-ligne/
- *« L'action internationale de la France en matière de lutte contre la cybercriminalité »*, MEAE, 9 janvier 2025, Lien : https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/actualites-et-evenements/article/l-action-internationale-de-la-france-en-matiere-de-lutte-contre-l
- *« La France et la cybersécurité »,* MEAE, janvier 2022, Lien :

https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/lutter-contre-la-criminalite-organisee/la-france-et-la-cybersecurite/

- *La France candidate au Conseil des droits de l'Homme 2021-2023*, MEAE, Lien : https://www.diplomatie.gouv.fr/IMG/pdf/candidature_cdh_fr_cle825da2.pdf
- *« La lutte contre la cybercriminalité, une priorité de l'Europe »,* Ministère de l'intérieur, 12 septembre 2023, Lien : https://www.gendarmerie.interieur.gouv.fr/gendinfo/actualites/2023/la-lutte-contre-la-cybercriminalite-une-priorite-pour-l-europe
- LE DRIAN J-Y., *Discours sur le cyberespace*, 11 novembre 2021, Lien : https://www.vie-publique.fr/discours/282457-jean-yves-le-drian-11112021-cyberespace
- *Le numérique et l'évaluation : définitions*, Réseau Canopé, Agence des usages TICE, Lien : https://www.reseau-canope.fr/fileadmin/user_upload/Projets/agence_des_usages/Evaluation_et_numerique/1_Le_numerique_et_l_evaluation__definitions.pdf
- *Lutte contre la désinformation - les mémos de la DGM n°3*, MEAE, 2024, Lien : https://www.diplomatie.gouv.fr/IMG/pdf/memo_dgm_n3-desinfo_web_cle85e19a.pdf
- *« Manipulation d'algorithmes et instrumentalisation d'influenceurs : enseignements de l'élection présidentielle en Roumanie & risques pour la France*, Secrétariat général de la défense et de la sécurité nationale *»* , 4 février 2025, Lien : https://www.sgdsn.gouv.fr/publications/manipulation-dalgorithmes-et-instrumentalisation-dinfluenceurs-enseignements-de
- *« Intelligence artificielle et numérique »,* Ministère de l'enseignement supérieur et de la recherche, 17 janvier 2023, Lien : https://www.enseignementsup-recherche.gouv.fr/fr/intelligence-artificielle-et-numerique-97624
- *Partenariat information et démocratie,* MEAE, 2023, Lien : https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/la-france-et-les-nations-unies/l-alliance-pour-le-multilateralisme/partenariat-information-et-democratie/
- *Plan de relance : les actions du ministère,* Ministère du Travail, du Plein emploi et de l'Insertion**,** 2024, Lien : https://travail-emploi.gouv.fr/le-ministere-en-action/relance-activite/
- *« Promouvoir les droits humains, les valeurs démocratiques et la langue française dans le monde numérique »*, MEAE, Lien : https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/les-domaines-d-action-de-la-diplomatie-numerique-francaise/promouvoir-les-droits-humains-les-valeurs-democratiques-et-la-langue-francaise/
- *« Quels sont les grands principes de la diplomatie numérique de la France ? », Diplomatie numérique*, MEAE, 2020, Lien : https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique

- *Rapport d'activité 2020,* Ambassadeur pour le numérique - MEAE, 6 octobre 2020, Lien : https://www.vie-publique.fr/files/rapport/pdf/281862.pdf
- *Rapport - RRN : une campagne de l'information complexe et persistance,* VIGINUM, Secrétariat de la défense et de la sécurité nationale, 13 juin 2023. Lien : https://www.sgdsn.gouv.fr/files/files/13062023_RRN_une%20campagne%20num%C3%A9rique%20de%20manipulation%20de%20l%27information%20complexe%20et%20persistante.pdf
- *« RRN : une campagne numérique de l'information complexe et persistante »,* Secrétariat général de la défense et de la sécurité nationale, 19 juin 2023, Lien : https://www.sgdsn.gouv.fr/publications/maj-19062023-rrn-une-campagne-numerique-de-manipulation-de-linformation-complexe-et
- *« Souveraineté numérique : des moyens inédits pour soutenir les acteurs de l'IA »*, Ministère de l'économie, des finances et de la souveraineté industrielle et numérique, 16 juin 2023, Lien : https://www.economie.gouv.fr/souverainete-numerique-moyens-inedits-soutien-acteurs-IA
- *Stratégie internationale de la France pour le numérique*, MEAE, 15 décembre 2017, Lien : https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf
- *Stratégie internationale de la France pour une diplomatie féministe* (2025-2030), MEAE, Lien : https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-feministe/strategie-internationale-de-la-france-pour-une-diplomatie-feministe-2025-2030
- *Stratégie nationale pour l'intelligence artificielle,* MEFSIN, 2018, mise à jour 2021, Lien : https://www.economie.gouv.fr/strategie-nationale-intelligence-artificielle

c) *Assemblée nationale*

- *Étude d'impact, Projet de loi relatif à la protection des données personnelles*, 12 décembre 2017, p.64.

d) *Défenseur des droits*

- Communiqué de presse, *« Intelligence artificielle : la Défenseure des droits appelle à garantir le droit de la non-discrimination »,* 17 avril 2024, Lien : https://www.defenseurdesdrots.fr/intelligence-artificielle-la-defenseure-des-droits-appelle-garantir-le-droit-de-la-non-376
- *Rapport - Algorithmes : prévenir l'automatisation des discriminations*, mai 2020, Lien : Algorithmes : prévenir l'automatisation des discriminations
- *Rapport - Algorithmes, systèmes d'IA et services publics : quels droits pour les usagers,* octobre 2024, Lien : Rapport algorithmes, systèmes d'IA et services publics : quels droits pour les usagers ? Points de vigilance et recommandations

- *Rapport - Technologies d'identification biométrique à distance dans l'espace public : enjeux et recommandations*, février 2022, Lien : ddd_rapport_technologies-biometriques_2021.pdf

e) Institutions publiques et agences gouvernementales

- *Avis sur la protection de l'intimité des jeunes en ligne,* CNCDH, A-2025-1, janvier 2025
- *Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux*, CNCDH, A-2022-6, 7 avril 2022
- DURIEUX B., LASCONJARIAS G., *L'année de la Défense nationale - Ruptures stratégiques*, Institut des hautes études de défense nationale, Documentation française, 2024, 204p.
- *Infographies – Bilan 5 ans de violations de données*, Paris, CNIL, mars 2024 (mise en ligne 27 mars 2024), Lien : Infographies - Bilan 5 ans violations de données
- *Intelligence artificielle et action publique : construire la confiance, servir la performance*, Conseil d'État, 31 août 2022, Lien : https://www.conseil-etat.fr/publications-colloques/etudes/intelligence-artificielle-et-action-publique-construire-la-confiance-servir-la-performance
- *Garder la main : rapport sur la maîtrise des algorithmes et de l'intelligence artificielle*, CNIL, 2023, Lien : https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_rapport_garder_la_main_web.pdf
- *Rapport - IA : notre ambition pour la France*, Commission de l'intelligence artificielle, mars 2024, Lien : https://www.info.gouv.fr/upload/media/content/0001/09/4d3cc456dd2f5b9d79ee75feea63b47f10d75158.pdf
- *Recommandations de sécurité pour un système d'IA générative* ANSSI, 2024, Lien : Recommandations_de_sécurité_pour_un_système_d_IA_générative.pdf
- Séminaire Diplomatie numérique, Déclaration d'intervenant, 22 novembre 2024, CNCDH, Sous-commission D, (CONFIDENTIEL)

3. Juridictions nationales

- Conseil d'État (France) 22 mai 2013, n° 351183, Lien : https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2013-05-22/351183.
- Conseil constitutionnel, Décision n° 2020-840 QPC, 20 mai 2020.
- LUQUET A., *Question écrite à l'Assemblée nationale sur l'intelligence artificielle et les droits fondamentaux*, 15e législature, Journal Officiel, question publiée le 14 novembre 2017, p. 5471 ; réponse publiée le 6 février 2018, p. 943. Question signalée le 22 janvier 2018

4. Institutions scientifiques

- DILLON R., SCHULTZ J., CRAWFORD K. et WHITTAKER M., A*lgorithmic Impact Assessments Report : A Practical Framework for Public Agency Accountability*, AI Now Institute, 9 avril 2018

5. Représentations françaises à l'international

- *Adoption de la résolution franco-néerlandaise sur les violences faites aux femmes et aux filles, Déclarations de la France à l'ONU, Intervention de M. Nicolas DE RIVIÈRE,* Représentant permanent de la France auprès des Nations Unies à l'Assemblée générale des Nations Unies, 14 novembre 2024, Lien : https://onu.delegfrance.org/adoption-a-l-agnu-de-la-resolution-franco-neerlandaise-visant-a-lutter-contre
- *Candidature de la France au Conseil des droits de l'Homme pour la période 2024-2026*, Engagements pris volontairement en application de la résolution 60/251 de l'Assemblée générale, Représentation permanente de la France auprès des Nations Unies à New York, Lien : https://onu.delegfrance.org/candidature-de-la-france-au-conseil-des-droits-de-l-homme-2024-2026
- *Conférence de Bogota - L'engagement transformateur de la France, Soutenir les parents dans la gestion des risques liés aux usages numériques, en particulier la violence en ligne*, Lien : https://endviolenceagainstchildrenconference.org/wp-content/uploads/2024/11/France-3.pdf
- *Conférence de Bogotá - L'engagement transformateur de la France, Violence contre les enfants dans l'environnement numérique,* Lien ; https://endviolenceagainstchildrenconference.org/wp-content/uploads/2024/11/France-4.pdf
- *Dialogue interactif sur le rapport relatif aux droits de l'Homme et à l'émergence des nouvelles technologies,* Représentation permanente de la France auprès des Nations Unies à Genève et des organisations internationales à Genève, 10 juillet 2024, Lien : https://onu-geneve.delegfrance.org/Dialogue-interactif-sur-le-rapport-relatif-aux-droits-de-l-Homme-et-a-l
- *Forum de Paris sur la Paix - Appel à solutions 2022*, Représentation permanente de la France auprès des Nations Unies à New York, 13 janvier 2023, Lien ; https://onu.delegfrance.org/forum-de-paris-sur-la-paix-appel-a-solutions-2022
- *La France appelle à assurer la protection des droits des enfants, Déclarations de la France à l'ONU, Intervention de M. Tudor ALEXIS, Secrétaire général adjoint mission AGNU 79 à l'Assemblée générale des Nations Unies*, 10 octobre 2024, Lien : https://onu.delegfrance.org/la-france-appelle-a-la-pleine-mise-en-oeuvre-de-la-convention-internationale
- *« Position de la France »,* Représentation permanente de la France auprès de la Conférence du désarmement à Genève, 13 mars 2023, Lien : https://cd-geneve.delegfrance.org/Position-de-la-France

III) PRESSE

A) Articles de médias nationaux

- GAN N., LIU J., *« China announces high-tech fund to grow AI, emerging industries »,* CNN, 10 mars 2025, Lien : https://edition.cnn.com/2025/03/06/tech/china-state-venture-capital-guidance-fund-intl-hnk/index.html
- DEPRET F., *« Les origines de la diplomatie »*, Le Monde, 31 décembre 1945, Lien : ttps://www.lemonde.fr/archives/article/1945/12/31/les-origines-de-la-diplomatie_1857157_1819218.html,
- *« En France ou ailleurs, couper l'accès aux réseaux sociaux pour couper court aux émeutes ? »,* The Conversation, 26 juillet 2023, Lien : https://theconversation.com/en-france-ou-ailleurs-couper-lacces-aux-reseaux-sociaux-pour-couper-court-aux-emeutes-209583
- *« Intelligence artificielle : Emmanuel Macron annonce des investissements en France de 109 milliards d'euros dans les prochaines années »*, Le Monde, 9 février 2025, Lien : https://www.lemonde.fr/pixels/article/2025/02/09/intelligence-artificielle-emmanuel-macron-annonce-des-investissements-en-france-de-109-milliards-d-euros-dans-les-prochaines-annees_6539115_4408996.html
- *« L'ONU approuve son premier traité contre la cybercriminalité »*, Le Monde, 9 août 2024, Lien : https://www.lemonde.fr/pixels/article/2024/08/09/l-onu-approuve-son-premier-traite-contre-la-cybercriminalite_6273668_4408996.html
- *« Peut-on expliquer l'Intelligence artificielle ? »*, Le Monde, 28 février 2024, Lien : https://www.lemonde.fr/sciences/article/2024/02/28/peut-on-expliquer-l-intelligence-artificielle_6219018_1650684.html
- *Pour la ministre chargée de l'IA et du Numérique Clara Chappaz : « Les réseaux sociaux avant 15 ans, c'est non »,* La Tribune Dimanche, 11 mai 2025, Lien : https://www.latribune.fr/la-tribune-dimanche/dimanche-eco/pour-la-ministre-chargee-de-l-ia-et-du-numerique-clara-chappaz-les-reseaux-sociaux-avant-15-ans-c-est-non-1024669.html
- *« Sommet de l'IA à Paris : d'où proviendront les 1,09 milliard d'euros promis par Emmanuel Macron ? »*, Europe 1, 21 mai 2024, Lien : https://www.europe1.fr/technologies/sommet-de-lia-a-paris-dou-proviendront-les-109-milliards-deuros-promis-par-emmanuel-macron-302162

B) Articles de médias gouvernementaux

- *« An action plan for artificial intelligence in Australia »*, Australian Government, 18 juin 2021, Lien : An action plan for artificial intelligence in Australia | Department of Industry Science and Resources

- *« Déclaration de M. Emmanuel Macron, président de la République, sur l'action de la France en faveur des droits de l'homme, à Paris, le 10 décembre 2023 »,* Vie publique, 10 décembre 2023, Lien : https://www.vie-publique.fr/discours/292372-emmanuel-macron-10122023-droits-de-lhomme
- *« IA : quel potentiel et quels risques dans les services publics ? »*, Vie publique, 2024, Lien : https://www.vie-publique.fr/parole-dexpert/293547-ia-quel-potentiel-et-quels-risques-dans-les-services-publicsVie Publique
- *« Intelligence artificielle : 25 propositions pour une stratégie française »*, Vie publique, 2024, Lien : https://www.vie-publique.fr/en-bref/293421-intelligence-artificielle-25-propositions-pour-une-strategie-francaise
- *« Intelligence artificielle : 25 propositions pour une stratégie française »,* Vie publique, 2024, Lien : https://www.vie-publique.fr/en-bref/293421-intelligence-artificielle-25-propositions-pour-une-strategie-francaiseVie Publique+1Vie Publique+1
- *« Intelligence artificielle : le cadre juridique européen en 7 questions »,* Vie publique, 2025, Lien : https://www.vie-publique.fr/questions-reponses/292157-intelligence-artificielle-le-cadre-juridique-europeen-en-7-questionsVie Publique
- *« Loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique »*, Vie publique, 17 avril 2025, Lien : https://www.vie-publique.fr/loi/289345-loi-du-21-mai-2024-securiser-et-reguler-lespace-numerique-sren
- *« Qu'est-ce que la diplomatie ? »,* Vie publique, 16 septembre 2024, Lien : https://www.vie-publique.fr/fiches/269886-quest-ce-que-la-diplomatie

C) <u>Articles d'organisations régionales et internationales</u>

- *« Combattre la désinformation »,* Nations Unies, Lien : https://www.un.org/fr/countering-disinformation
- Communiqué de presse, « *L'intelligence artificielle menace la vie privée : Bachelet appelle à une réglementation urgente* », Haut-Commissariat aux droits de l'Homme, 15 septembre 2021, Lien : https://www.ohchr.org/fr/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet
- *« European Media Freedom Act : tout savoir sur le règlement européen sur la liberté des médias »*, Toute l'Europe, 15 mai 2025, Lien : https://www.touteleurope.eu/societe/qu-est-ce-que-l-acte-europeen-sur-la-liberte-des-medias-european-media-freedom-act/

- *« Intelligence artificielle : la Défenseure des droits appelle à garantir le droit de la non-discrimination dans les discussions européennes »,* International Obudsman Institut, 2023, Lien : https://www.theioi.org/ioi-news/current-news/intelligence-artificielle-la-defenseure-des-droits-appelle-a-garantir-le-droit-de-la-non-discrimination-dans-les-discussions-europeennesThe IOI
- *« L'action de l'Union européenne contre la désinformation en 3 minutes »*, Toute l'Europe, 19 mars 2023, Lien : https://www.touteleurope.eu/economie-et-social/l-action-de-l-union-europeenne-contre-la-desinformation-en-3-minutes/
- *« La Troisième Commission adopte neuf projets de résolution, consacrant l'essentiel de son attention aux violences à l'égard des femmes dans l'environnement numérique »*, Nations Unies, Couverture des réunions & communiqués de presse, AG/SHC/4430, 14 novembre 2024, Lien : https://press.un.org/fr/2024/agshc4430.doc.htm
- *« Les réseaux sociaux, principale source d'information des jeunes européens »*, Toute l'Europe, 20 février 2025, Lien : https://www.touteleurope.eu/societe/podcast-les-reseaux-sociaux-principale-source-d-information-des-jeunes-europeens/
- *Logiciels espions et surveillance : l'ONU met en garde contre les menaces croissantes pour la vie privée,* ONU Info, 16 septembre 2022, Lien : https://news.un.org/fr/story/2022/09/112718
- *« L'ONU appelle à un encadrement plus strict des technologies numériques afin de protéger les droits humains »*, ONU Info, 15 septembre 2021, Lien : https://news.un.org/fr/story/2021/09/1103762

D) Presse de la société civile

- *« Préoccupations et recommandations de Human Rights Watch sur la France »,* Human Rights Watch, 22 juin 2015, Lien : https://www.hrw.org/fr/news/2015/06/22/preoccupations-et-recommandations-de-human-rights-watch-sur-la-france

IV) Vidéos

- MACRON E., *Emmanuel Macron s'exprime sur les enjeux de l'intelligence artificielle,* YouTube, 2025, Lien : https://www.youtube.com/watch?v=wBe97k57KxYYouTube
- MACRON E., *Discours d'ouverture du sommet sur l'intelligence artificielle à Paris*, YouTube, 21 mai 2024. Lien : https://www.youtube.com/watch?v=YSfAwQDQuHQ
- UNESCO, *Social Media 4 Peace*, Youtube, Lien : https://www.youtube.com/watch?v=T-TtQ8fWLb0&t=57s

ANNEXES

Annexe 1 - Instruments juridiques relatifs aux droits de l'Homme applicables à la France dans le contexte de la diplomatie numérique

Infractions pénales commises via l'Internet et d'autres réseaux informatiques : infractions portant atteinte aux droits d'auteurs, de la fraude liée à l'informatique, de la pornographie enfantine,infractions liées à la sécurité des réseaux.

Nom de l'instrument	Date de signature / ratification par la France	Domaine couvert	Juridiction ou organe de suivi
ONU			
Déclaration Universelle des Droits de l'Homme (DUDH)	Adoptée en 1948; Valeur non contraignante juridiquement, mais référence fondamentale reconnue dans la jurisprudence française et internationale	Droits civils, politiques, économiques, sociaux et culturels	
Pacte international relatif aux droits civils et politiques	Signé : 1966 Ratifié : 1980	Liberté d'expression, procès équitable, vie privée, etc.	Comité des droits de l'homme
Pacte international relatif aux droits économiques, sociaux et culturels	Signé : 1966 Ratifié : 1980	Droit au travail, à l'éducation, à la santé, etc.	Comité des DESC
Convention contre la torture	Signée : 1984 Ratifiée : 1986	Interdiction de la torture et traitements inhumains	Comité contre la torture
Convention relative aux droits de l'enfant	Signée : 1989 Ratifiée : 1990	Protection des droits de l'enfant	Comité des droits de l'enfant
Convention internationale sur l'élimination de toutes les formes de discrimination raciale	Signée : 1966 Ratifiée : 1971	Lutte contre le racisme et la discrimination	Comité pour l'élimination de la discrimination raciale

Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes (CEDEF)	Signée : 1980 Ratifiée : 1983	Égalité femmes-hommes	Comité CEDEF
Convention relative aux droits des personnes handicapées	Signée : 2007 Ratifiée : 2010	Inclusion et non-discrimination des personnes handicapées	Comité des droits des personnes handicapées
Conseil de l'Europe			
Convention européenne des droits de l'homme	Signée : 1950 Ratifiée : 1974	Droits civils et politiques	Cour européenne des droits de l'Homme
Charte sociale européenne	Signée : 1965 Ratifiée : 1973	Droits sociaux (travail, logement, santé)	Comité européen des droits sociaux
Convention 108 (Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel)	Adoptée le 28 janvier 1981 Ratifiée : 1981	Protection des données personnelles et vie privée	Comité Consultatif de la Convention 108 (Groupe de travail du Conseil de l'Europe)
Charte européenne des langues régionales ou minoritaires	Adoptée : 1992 Signée : 1999 Jamais ratifiée par la France; raisons : le Conseil constitutionnel a jugé que certaines dispositions de la Charte étaient contraires à la Constitution française (principe d'unicité de la République et de l'usage du français comme langue de la République).	Protéger et promouvoir les langues régionales ou minoritaires en tant que patrimoine culturel de l'Europe, en garantissant leur usage dans la vie publique et privée.	Comité d'experts (COMEX); Comité des Ministres

Convention de Budapest sur la cybercriminalité	Adoptée : 2001 Ratifiée : 2006	Lutte contre les infractions pénales commises via la technologie et coopération entre les Etats parties à la Convention dans le domaine de la cybercriminalité	Comité de la Convention sur la cybercriminalité
Convention-cadre sur l'intelligence artificielle, les droits de l'Homme, la démocratie et l'État de droit	Adoptée : 2024 Signée : 5 septembre 2025, non encore ratifiée (juillet 2025)	Encadrement du développement, de la conception, de l'utilisation et du déploiement de l'IA dans le respect des droits humains, de la démocratie et de l'État de droit	Conseil de l'Europe ; mécanisme de suivi prévu par la Convention avec un comité des Parties
Union européenne			
Charte des droits fondamentaux de l'Union européenne	Adoptée le 7 décembre 2000, intégrée au traité de Lisbonne en 2009	Droits civils, politiques, économiques, sociaux et droits relatifs à la dignité humaine	Cour de justice de l'Union européenne (CJUE)
Directive 2000/31/CE relative à certains aspects juridiques des services de la société de l'information (Directive sur le commerce électronique)	Adoptée en 2000	Harmonisation des règles concernant divers aspects liés commerce électronique (notamment dans les domaines suivants : services d'information, vente, publicité, services professionnels, services de loisirs, services intermédiaires de base, services gratuits financés par la publicité, le parrainage)	Commission européenne, CJUE, juridictions nationales
Règlement 2016/679 relatif à la protection des personnes physiques à l'égard	Adopté en 2016	Protection des données personnelles, vie privée, droits des individus sur leurs données, transparence et contrôle	Autorités nationales de protection des données (en France : CNIL)

du traitement des données à caractère personnel (RGPD)		des traitements de données	
Directive 2018/1972 établissant le code des communications électroniques européen (refonte)	Adoptée en 2018	Actualisation des règles visant à réglementer les réseaux de communication électroniques (télécommunications), les services de télécommunication, et les ressources et services associés	Commission européenne, CJUE, juridictions nationales
Digital Markets Act (DMA)	Adopté en 2022	Régulation des grandes plateformes dites « gatekeepers » (contrôle des marchés numériques, pratiques anticoncurrentielles, accès équitable)	Commission européenne, autorités nationales de concurrence
Règlement 2022/2065 relatif à un marché unique des services numériques (Digital Services Act)	Adopté en 2022 – applicable depuis le 17 février 2024	Régulation des services numériques : obligations des plateformes, modération de contenus, transparence des algorithmes, lutte contre les contenus illicites	Commission européenne, autorités nationales de coordination désignées par les États membres (en France : l'ARCOM), et un comité européen des services numériques
Directive *2*016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (Directive SRI)	Adoptée en 2016, plus en vigueur depuis 2024	Sécurité des réseaux et systèmes d'information, gestion des risques cyber, notification des incidents	Commission européenne ; Agences nationales de cybersécurité (en France : ANSSI)
Règlement 2019/881 relatif à l'ENISA (Agence de l'Union	2019	Coordination européenne en cybersécurité, soutien	Commission européenne ; ENISA

européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications (règlement sur la cybersécurité)		aux États membres, développement de capacités de cybersécurité, mise en place d'un cadre européen de certification de la sécurité des technologies numériques de l'information et de la communication	
Règlement 2019/796 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses Etats membres	Adopté en 2019	Cadre de sanctions (gel d'avoirs, interdictions) contre des acteurs responsables de cyberattaques ciblant l'Union ou ses États membres	Conseil de l'Union européenne, Commission européenne
Règlement 2021/784 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne	Adopté en 2021	Lutter contre l'utilisation abusive des services d'hébergement pour la diffusion publique de contenus à caractère terroriste en ligne	Commission européenne, CJUE, juridictions nationales
Règlement 2022/1925 sur les marchés contestables et équitables dans le secteur numérique (Digital Markets Act)	Adopté en 2022	Garantir un secteur numérique compétitif et équitable, en permettant aux entreprises numériques innovantes de se développer et en assurant la sécurité des utilisateurs en ligne	Commission européenne, CJUE, juridictions nationales
Directive 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive SRI 2)	Adoptée en 2022	Cadre réglementaire commun visant à améliorer le niveau de cybersécurité dans l'Union européenne	Commission européenne, CJUE, juridictions nationales

Règlement 2022/868 portant sur la gouvernance européenne des données	Adopté en 2022	Rendre davantage de données disponibles pour la réutilisation et à faciliter le partage des données au profit des citoyens et des entreprises de l'Union européenne, en créant des emplois et en stimulant l'innovation	Commission européenne, CJUE, juridictions nationales
Règlement 2024/2642 concernant des mesures restrictives eu égard aux activités déstabilisatrices menées par la Russie	Adopté en 2024	Sanctions visant les personnes, les entités et les organismes russes impliqués ou soutenant des mesures portant atteinte à la démocratie, à l'État de droit, à la stabilité et à la sécurité au sein de l'Union européenne, et au niveau international	Commission européenne, CJUE, juridictions nationales
Règlement 2024/1083 établissant un cadre commun pour les services de médias dans le marché intérieur (règlement européen sur la liberté des médias)	Adopté en 2024	Cadre commun pour les services des médias : renforcement de leur liberté éditoriale et l'indépendance ; possibilité d'opérer plus facilement par-delà les frontières au sein du marché intérieur ; bénéficier de la transformation numérique de l'espace des médias ; garanties contre l'ingérence ; transparence ; renforcement de la coopération et la convergence réglementaires	Commission européenne, CJUE, juridictions nationales

Règlement 2022/868 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données)	Adopté en 2022	Rendre davantage de données disponibles pour la réutilisation et à faciliter le partage des données au profit des citoyens et des entreprises de l'UE, en créant des emplois et en stimulant l'innovation	Commission européenne, CJUE, juridictions nationales
Règlement 2024/1689 établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'intelligence artificielle)	Adopté en 2024	Encourager le développement et l'adoption de systèmes d'intelligence artificielle (IA) sûrs et dignes de confiance dans l'ensemble du marché unique	Commission européenne, CJUE, juridictions nationales
Règlement 2024/2847 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques (règlement sur la cyber résilience)	Adopté en 2024	Renforcer la cybersécurité, en établissant un cadre global pour garantir que les produits et services numériques sont sûrs dès leur conception, résilients contre les cybermenaces et capables de fournir une protection continue tout au long de leur cycle de vie	Commission européenne, CJUE, juridictions nationales

TABLE DES MATIÈRES