Architecture Globale de la Souveraineté Numérique

Titre : *Architecture globale de la souveraineté numérique : Analyse comparative des modèles de censure et de contrôle de l'internet en 2025*
Auteur : NOX

Résumé :

Cet article examine l'évolution des pratiques de censure et de contrôle d'Internet dans les principaux pays du monde en 2025. L'analyse repose sur une approche comparative, identifiant trois modèles dominants : le modèle autoritaire-souverain (Chine, Russie, Iran, Corée du Nord), le modèle libéral-réglementaire (États-Unis, Union européenne, Israël) et le modèle hybride (Turquie, Égypte, ainsi que plusieurs pays d'Asie, d'Afrique et d'Amérique latine). Il est démontré qu'en 2025, le concept d'« internet souverain » est passé d'une idée théorique à une architecture techno-juridique mise en œuvre. L'attention est portée sur les outils technologiques (DPI, IA), les fondements juridiques et les objectifs géopolitiques qui sous-tendent les restrictions. Il en ressort un renforcement de la fragmentation de l'internet mondial (*Splinternet*) et l'émergence d'écosystèmes numériques résilients régis par leurs propres règles.

Mots-clés : censure sur Internet, souveraineté numérique, 2025, inspection approfondie des paquets (DPI), intelligence artificielle, régulation, droits de l'homme, cybersécurité.

Introduction

En 2025, Internet n'est plus l'espace global unifié qu'il prétendait être à l'origine. Sous l'effet des conflits géopolitiques, des impératifs de sécurité nationale et de la quête de souveraineté culturelle, des modèles nationaux et régionaux de contrôle du cyberespace ont vu le jour. Le terme « censure » a évolué pour englober non seulement le blocage de contenu, mais aussi des systèmes complexes de modération préventive, des pressions législatives sur les plateformes, la manipulation du trafic et la désinformation ciblée.

L'objectif de cet article est de réaliser une analyse comparative des modèles de contrôle d'internet dans les grandes puissances, d'identifier leurs points communs et leurs différences fondamentales, ainsi que d'évaluer leur impact sur les droits des citoyens, l'économie numérique et la stabilité internationale.

---

1. Méthodologie

Cette étude repose sur une analyse qualitative et comparative. Les pays ont été choisis en fonction de leur influence sur la politique numérique mondiale et de leur représentativité d'un modèle donné. Les sources incluent :

- Lois nationales (internet souverain, protection des données, lutte contre l'extrémisme) ;
- Rapports d'organisations internationales (Freedom House, RSF, Access Now) ;
- Rapports techniques d'entreprises de cybersécurité (Citizen Lab, Palo Alto Networks) ;
- Déclarations publiques d'autorités et de régulateurs.

---

2. Analyse Comparative des Modèles de Contrôle de l'Internet

2.1. Modèle Autoritaire de Souveraineté Numérique

Chine :
En 2025, le Grand Pare-feu chinois (GFW) a évolué vers un système de gouvernance numérique complet appelé « Crédit social 2.0 ». Le blocage basé sur le DPI est complété par des algorithmes prédictifs d'intelligence artificielle capables d'identifier et d'étouffer les discussions « indésirables » dès leur apparition. Les plateformes internationales ont été remplacées par des équivalents nationaux (WeChat, Douyin, Baidu), sous contrôle total de l'État. L'exportation de ce modèle, notamment via l'initiative des « Nouvelles Routes de la Soie », est devenue un instrument clé de puissance douce en Afrique et en Asie.

Russie :
La mise en œuvre de la loi sur « l'internet souverain » (2019) est achevée. En 2025, un système national de noms de domaine (DNS) permet d'isoler le segment russe du réseau global (Runet) si nécessaire. Le DPI est utilisé pour cibler les services VPN et le trafic chiffré. Les principales cibles de la censure : critique du pouvoir, opérations militaires, contenus LGBTQ+ et médias indépendants. Bases juridiques : lois sur les « fake news », les « agents étrangers » et l'« extrémisme ».

Iran :
Le modèle iranien combine contrôle technique et répression sévère. Le pays possède l'un des systèmes de filtrage les plus avancés, capable de bloquer dynamiquement les messageries (Telegram, WhatsApp) et les réseaux sociaux lors de manifestations. En 2025, l'identification des utilisateurs est obligatoire pour accéder au Wi-Fi ou acheter une carte SIM. Le ralentissement volontaire du réseau (*throttling*) est couramment utilisé.

Corée du Nord :
Reste l'exemple extrême de contrôle total. Kwangmyong, l'intranet national, est entièrement coupé de l'internet mondial. L'accès au web global est réservé à une élite très restreinte. Le contenu se limite à la propagande d'État, aux matériaux idéologiques et à quelques ressources scientifiques.

2.2. Modèle Libéral-Réglementaire (États-Unis, UE, Israël)

États-Unis :
La censure étatique directe est absente, mais un système complexe de régulation publique et privée s'est mis en place. Sous la pression de la société civile et des régulateurs (FCC, FTC), les grandes plateformes (Meta, X, Google) ont durci leur politique de modération sur les discours haineux, la désinformation et l'incitation. Le débat central en 2025 concerne la Section 230, qui accorde l'immunité aux plateformes pour les contenus publiés par les utilisateurs. Sa remise en question pousse les entreprises à renforcer l'autorégulation, transférant ainsi la censure au secteur privé.

Union européenne :
L'UE a mis en place le cadre réglementaire le plus avancé au monde, établissant de facto des normes mondiales. La censure se fait de manière indirecte via des obligations juridiques strictes :

- **RGPD :** blocage des sites ne respectant pas les normes de protection des données ;
- **DSA (Digital Services Act) :** obligation pour les plateformes de supprimer rapidement les contenus illégaux (terrorisme, haine), sous peine de lourdes amendes ;
- **DMA (Digital Markets Act) :** lutte contre les positions dominantes.

L'UE ne bloque pas directement les sites, mais crée un environnement où le non-respect des règles conduit à une exclusion de fait du marché.

Israël :
Cas particulier d'un modèle libéral régulé, avec un accent fort sur la sécurité nationale. En tant que démocratie technologique, Israël respecte généralement les principes d'un internet ouvert. Cependant, face à des menaces permanentes, la censure s'applique de manière ciblée et sur des bases légales solides :

- **Cadre juridique :** L'instrument principal est la censure militaire, héritée de la fondation de l'État. Tous les médias – y compris numériques – doivent soumettre les contenus relatifs à la sécurité au bureau de censure militaire. Ce principe a été adapté à l'ère numérique.
- **Pratique :** Les autorités peuvent exiger des fournisseurs d'accès et des plateformes la suppression de contenus jugés menaçants pour la sécurité nationale ou incitant à la violence. Ces décisions sont souvent contestées devant la Cour suprême, qui joue un rôle de contre-pouvoir. Lors des escalades militaires, la censure se renforce. Contrairement aux régimes autoritaires, Israël dispose d'une presse libre et d'une société civile active, garantissant une certaine transparence.

2.3. Modèle Hybride (Turquie, Égypte, Asie, Afrique, Amérique latine)

Turquie :
Dispose de l'un des plus vastes registres de blocages au monde. La loi n° 5651 a été renforcée en 2025, permettant au régulateur BTK de bloquer un contenu en moins de 4 heures sans décision judiciaire. La loi n° 7416 impose aux plateformes de désigner un représentant local et d'obéir aux injonctions de l'État ; en cas de refus, le trafic est ralenti progressivement (*throttling*) jusqu'à l'inaccessibilité.

Égypte :
Utilise les licences de télécommunications comme levier de contrôle. Le blocage des VPN et des applications chiffrées (comme Signal) est monnaie courante. Lors de tensions politiques, l'accès à internet peut être suspendu au niveau national. La loi sur la cybercriminalité confère aux autorités de larges pouvoirs de censure et de surveillance.

Asie (Inde, Vietnam) :
L'Inde pratique des coupures régionales régulières de l'internet pour des raisons de sécurité publique. La législation donne au gouvernement des pouvoirs étendus de blocage. Le Vietnam suit le modèle chinois : les entreprises doivent stocker les données localement, les fournir sur demande, et supprimer le contenu sous 24 heures.

Afrique :
Des pays comme l'Éthiopie, l'Ouganda et le Zimbabwe ont recours à des coupures d'internet pendant les élections ou les protestations. L'influence des technologies chinoises (Huawei, ZTE) et des modèles de contrôle associés s'accroît.

Amérique latine :

En 2025, la région montre une dynamique hétérogène, avec une tendance générale vers un modèle hybride.

- **Brésil :**
  La plus grande économie de la région tente de concilier liberté d'expression et lutte contre la désinformation. Le *Marco Civil da Internet*, inspiré de l'UE, reste la base du cadre réglementaire. Toutefois, les décisions judiciaires ordonnant le blocage de messageries comme WhatsApp ou Telegram se multiplient, pour refus de fournir des données ou de combattre les fausses informations.
- **Venezuela & Nicaragua :**
  Tendent vers un modèle autoritaire. Les autorités bloquent les sites d'information indépendants et les réseaux sociaux, surtout lors de crises politiques. Au Venezuela, le Conatec (Centre national de gestion du cyberespace) coordonne la censure. Des lois criminalisent la critique du gouvernement sur Internet.
- **Cuba :**
  Approche du contrôle total. L'accès à Internet s'est développé mais reste coûteux et strictement encadré. L'opérateur public ETECSA permet le filtrage de contenus et la surveillance des utilisateurs. Les critiques du régime et les médias indépendants sont systématiquement bloqués.

---

3. Discussion et Conclusions

En 2025, le monde est passé d'un Internet global unifié à une multitude d'espaces numériques fragmentés : la **Splinternet**. Principales tendances :

- **Raffinement technologique :**
  Les blocages simples ont cédé la place à des systèmes sophistiqués à base de DPI et d'IA, capables de modération prédictive et de contournement ciblé.

- **Justification juridique :**
  La censure se présente de plus en plus sous couvert de lutte contre l'extrémisme, protection des données (UE), souveraineté (Russie, Chine) ou sécurité (Israël), ce qui la rend plus légitime aux yeux de la communauté internationale.
- **Privatisation de la censure :**
  Dans les démocraties libérales (USA, UE), la censure est transférée au secteur privé via des pressions réglementaires. En Israël, elle reste étatique mais encadrée par la justice.
- **Dimension géopolitique :**
  Deux modèles s'affrontent : celui des États-Unis/UE, fondé sur les droits et le marché, et celui de la Chine/Russie, basé sur le contrôle étatique. Les pays de la « ceinture hybride » (notamment en Amérique latine) puisent dans les deux selon leur contexte politique.

Danger : création de bulles informationnelles, montée de l'autoritarisme, ralentissement des échanges transfrontaliers de savoir.
Le dilemme entre ouverture et sécurité nationale, illustré par le cas israélien, est la contradiction centrale de l'avenir d'Internet.

Annexe : DPI et Interception de Certificats

L'inspection approfondie des paquets (DPI) est une technologie qui permet d'analyser le trafic Internet au-delà des adresses IP, jusqu'au contenu même des données échangées.
Elle permet de savoir si l'utilisateur regarde une vidéo, utilise Tor ou VPN, échange des messages, etc.

Applications du DPI :

- Blocage ou ralentissement de services spécifiques ;
- Contournement de l'anonymat des VPN ou de Tor ;
- Surveillance du comportement en ligne ;
- Censure de masse, y compris sur trafic chiffré.

Le vrai danger : perte de confiance dans les technologies fondamentales d'Internet.

Dans de nombreux pays, sous couvert de lutte contre le terrorisme ou de protection de l'enfance, les États imposent le DPI et créent des **autorités de certification (CA)** contrôlées.
Cela leur permet de substituer des certificats HTTPS sans alerte au navigateur — et d'intercepter tout le trafic.

La connexion paraît « sécurisée », mais l'État peut lire, enregistrer et modifier le trafic — légalement, via une infrastructure de confiance détournée.
C'est ce qu'on appelle **l'interception via falsification de certificat**. Combinée au DPI, cela constitue une infrastructure légale d'intrusion.

Cela viole la neutralité du Net, la confidentialité et l'idée même d'un Internet sécurisé.
Quand l'État remplace la confiance, il ne protège plus — il contrôle.

Sources :

- Deibert, R. (2024). *The Great Firewall 2.0: AI and the Future of Internet Control*. MIT Press
- Freedom House. (2025). *Freedom on the Net 2025*
- Commission européenne. (2024). *Rapport annuel sur la mise en œuvre du Digital Services Act*
- Soldatov, A., & Borogan, I. (2023). *The Red Web*. HarperCollins
- RSF – Reporters Sans Frontières. (2025). *Index mondial de la liberté de la presse : l'oligarchie de la vérité*
- Zuboff, S. (2023). *L'ère du capitalisme de surveillance*. PublicAffairs
- Cohen, M., & Leybovich, G. (2024). *La démocratie numérique assiégée*. Tel Aviv University Press
- Americas Quarterly. (2025). *L'autoritarisme numérique en Amérique latine*
- Carrasco, E., & Silva, L. (2024). *La gouvernance d'Internet au Brésil*. São Paulo University Press

---