Synthèse

« La Balkanisation du web : chance ou risque pour l'Europe ? »

Le terme de « balkanisation » n'est pas un concept opératoire mais bien une représentation géopolitique qui sert des intérêts divers. Il couvre différents débats tels le filtrage et la fragmentation potentielle résultant des politiques de sécurité nationale ; le maintien de l'interopérabilité du réseau et d'un fichier racine commun ; les conflits autour des enchevêtrements de juridictions et de l'application extensive de la loi américaine via le principe d'extra-territorialité ; le contrôle politique national des contenus et des usages dans le cyberespace ; la remise en cause du modèle de gouvernance multi-acteurs ; ou les pressions commerciales qui cloisonnent les contenus numériques.

Des leaders de la communauté Internet l'utilisent comme une arme dans les débats sur l'évolution des règles de gouvernance de l'Internet ou pour lutter contre l'expression de la souveraineté des Etats dans le cyberespace (technique, politique ou juridique). Ces évolutions récentes entraînent — et sont causées par— une remise en question de la suprématie des Etats-Unis dans le cyberespace.

La connotation très péjorative du terme de « balkanisation », la diversité des débats qu'il recouvre et l'ambiguïté qu'il installe quant à ses implications invitent à l'utiliser avec la plus grande circonspection, particulièrement dans le cadre des négociations internationales. Il est préférable d'être clair et précis dans les termes que l'on emploie pour désigner les dynamiques multiples et parfois contradictoires de fragmentation/ouverture qui s'opèrent à différents niveaux sur la couche physique, logique et sémantique du cyberespace.

De plus, la configuration des rapports de force et des logiques de coopération/compétition entre acteurs n'est pas la même en fonction des enjeux. Définir une stratégie pour la France ou l'Europe nécessite de comprendre finement ces dynamiques, leurs différents enjeux, en les distinguant au mieux même s'ils sont liés, pour s'appuyer sur les bonnes coopérations et établir les bons rapports de force afin de défendre des objectifs.

Des dynamiques multiples et parfois contradictoires :

• Il n'existe pas un mais des cyberespaces. Les réseaux qui constituent l'Internet sont connectés et interopérables au niveau mondial, l'interaction des utilisateurs est globale mais le cyberespace est néanmoins constitué de sous ensembles linguistiques, politiques et culturels qui engendrent une grande diversité des expériences du web selon l'endroit d'où l'on se connecte sur la planète. L'idée d'un cyberespace libre, ouvert, où l'information circule sans restriction et où tout est accessible à tous à partir de n'importe où relève largement du mythe.

• La suprématie américaine reste extrêmement importante à tous les niveaux, (infrastructure physique, couche logique ou contenus) et dans le domaine politique de la gouvernance, de la gestion technique de l'architecture et du fonctionnement du réseau, des activités militaires et de renseignement ou encore du domaine juridique, étendu par le principe d'extraterritorialité.

• L'affaire Snowden a considérablement accéléré les tendances de fond de remise en question de cette suprématie, alors que le centre de gravité de l'Internet se déplace vers l'Asie et le Sud. Elle a aussi entraîné une prise de conscience politique et une montée en puissance des revendications de souveraineté numérique, qui se traduit par des initiatives politiques, industrielles et juridiques permettant de préserver l'intégrité et la confidentialité des données des appétits de gouvernements étrangers. Or la logique de repli souverain est susceptible d'entrer en contradiction avec les logiques de coopération internationale nécessaires à la lutte contre la cybercriminalité.

• La marchandisation des services en ligne entraîne des dynamiques de fragmentation sur les couches supérieures du cyberespace, comme la remise en cause de la neutralité du Net, mais aussi une dynamique opposée sur les couches inférieures car tous les acteurs économiques ont un intérêt clair à maintenir l'ouverture et l'interopérabilité de l'Internet pour développer leurs activités.

• Il n'y a donc pas de logique unique de « balkanisation », ni de la part d'un Etat particulier, ni comme tendance générale même si, par ailleurs, des intiatives peuvent fragmenter certaines dimensions de l'Internet avec des conséquences dommageables (contenus limités, accès restreint, etc.). On observe des intérêts concurrents entre les différents acteurs (étatiques, privés, citoyens, techniques) au sein de chaque Etat.

Les enjeux pour l'Europe :

• La dépendance des pays européens, et plus particulièrement la France, aux équipements étrangers (principalement chinois et américains) et aux plate-formes étrangères — géants du web américains en particulier— est très forte ; l'exposition à la surveillance (intelligence économique, vol de propriété intellectuelle et secrets d'affaire) est donc très importante et les retombées économiques de la captation des flux de données leur échappe en grande partie. L'absence de maîtrise des données met en jeu les bases de la croissance économique future (les données sont considérées comme l'or noir du 21ème siècle), la protection des données personnelles et plus généralement, la défense des valeurs de l'Europe.

• Les politiques de *data localization* et offres de « cloud souverain » permettent de réduire quelque peu la dépendance à l'offre américaine et de faire pression sur les entreprises américaines pour tenir compte des revendications de confidentialité de leurs clients européens. Mais ces initiatives doivent donc s'inscrire dans un projet de développement européen et international pour être compétitives et ne résolvent pas la problématique de l'extra-territorialité et de l'accès aux données.

• La volonté de sanctuarisation du territoire comporte aussi des risques et des effets paradoxaux : elle peut s'avérer difficilement réalisable d'un point de vue opérationnel et juridique, d'autant que les infrastructures vitales sont largement détenues et opérées par le secteur privé ; elle pose problème pour la coopération internationale nécessaire à la lutte contre la cybercriminalité ou à la cybersécurité ; elle recèle des risques d'escalade des conflits liés à une maladresse ou une erreur de calcul entre acteurs étatiques, en l'absence de processus de coopération et de règles du jeu clairement définies ; elle contribue à la difficulté de faire émerger des solutions au sein de l'Union européenne, malgré les enjeux. La limite de souveraineté est difficile à dépasser d'autant que la disparité des moyens entre les Etats est très forte et que les logiques bilatérales, notamment avec les Etats-Unis, prévalent.

Pistes de réflexion stratégique pour l'Europe :

• Des initiatives conduisant à une certaine fragmentation peuvent s'avérer nécessaires dans certains domaines spécifiques qui touchent aux intérêts les plus sensibles d'un Etat (infrastructures, informations stratégiques publiques ou privées). Mais la sécurité a un coût en termes financiers, en de créativité, d'innovation et/ou de performance . Il est donc essentiel de penser ces enjeux dans une logique de gestion du risque et d'envisager la sécurité dans l'esprit d'ouverture qui a fait le succès du réseau et fera la croissance économique de demain.

• D'un point de vue technique, l'enjeu est de parvenir à utiliser de façon sécurisée une infrastructure par définition non sécurisée. Ceci implique de penser toute la chaîne de confiance qui doit être ininterrompue de l'émetteur au destinataire. L'utilisation sécurisée est permise par l'établissement de liens systématiquement sécurisés —entre chaque relais de messagerie—, et une double identification du serveur de messagerie de l'émetteur -avec si possible certificat électronique - et de l'émetteur lui-même. Il est aussi nécessaire de garantir l'intégrité des messages, leur confidentialité et leur traçabilité et de penser l'archivage de façon sécurisée, à la fois par une réflexion sur la durée de vie des messages et sécurisation des données stockées.

• D'un point de vue économique, il est indispensable de développer une politique industrielle de confiance à l'échelle européenne. Il s'agit de structurer un écosystème cohérent d'entrepreneurs (grands groupes et PME), de laboratoires de recherche (universitaires et privés) et d'investisseurs pour développer une politique d'innovation et un socle technologique. D'une part il faut s'assurer de la compétitivité des entreprises (marché européen et international). D'autre part, il faut développer la

confiance, qui peut s'installer entre quelques partenaires puis s'étendre à d'autres pays européens, en pensant des solutions maîtrisées par des fournisseurs européens. Enfin, il est nécessaire de structurer le dialogue public-privé sur les questions de politique industrielle et d'envisager la création d'un label européen de confiance et une politique de soutien aux PME.

• D'un point de vue politique, le pouvoir normatif et règlementaire de l'Europe pourrait se jouer en sa faveur. L'Europe est un modèle d'intégration économique et de gouvernance, et de gestion partagée de la norme. Développer un régime juridique de protection des données personnelles qui soit à la fois solide et équilibré pourrait permettre : 1. Qu'il puisse être reproduit par d'autres pays et exercer ainsi un pouvoir d'influence ; 2. Qu'il puisse être attractif pour que les entreprises étrangères souhaitent héberger leurs données sous le régime juridique européen, ce qui permettrait par leurs flux de données de générer de la valeur ; 3. Qu'il constitue un levier politique et juridique pour contrecarrer l'extra-territorialité des Etats-Unis.

• Enfin, à condition de s'en donner les moyens, l'Europe pourrait peser dans les discussions et les décisions qui permettront d'une part de redéfinir la gouvernance de l'Internet au niveau mondial et d'autre part d'établir les nouveaux cadres de la sécurité collective à l'âge des réseaux interconnectés. Ceci implique d'articuler une position commune aux pays européens sur la gouvernance du cyberespace dans le respect de la souveraineté des Etats membres et des valeurs qui les unissent. Cette réflexion est indispensable si l'on souhaite que l'Europe devienne une force de proposition et un levier politique pour façonner et non subir le cyberespace du futur.