

page 5

éditorial

PRE

Pour des milliards d'humains désormais, l'internet n'est pas seulement un auxiliaire de vie, l'instrument d'une ouverture inimaginable au début même de ce siècle. Il est la métaphore d'un monde nouveau, centré sur des valeurs d'échange, d'instantanéité, de multiplicité d'acteurs, monde dont nous n'avons ni maîtrise ni gouvernement.

L'affaire Snowden n'a, pour les faits, pu surprendre que les naïfs. Mais elle a violemment éclairé quelques questions jusqu'alors contenues au cercle des spécialistes. Quelles informations sont accumulées à partir des techniques de l'internet ? Qui les garde, les contrôle, les exploite ? Et pour quoi faire ? Sous le masque d'une *soft* démocratie universelle, perce désormais l'image d'une anarchie sous-tendue d'une entreprise politique et économique localisée, structurée, au service d'officines de renseignement ou de la guerre économique. Si l'affaire Snowden fut utile, c'est d'abord en rappelant à des millions d'utilisateurs que l'internet est tout sauf une entreprise immatérielle, qu'elle est œuvre humaine, technique, et qu'elle doit donc relever des mêmes réflexions que les autres constructions technico-sociales de l'esprit humain.

Le dossier que présente ce numéro de *Politique étrangère* parcourt quelques-unes de ces réflexions, parmi les plus urgentes. On en relèvera ici deux. D'abord la question – désormais lieu commun – de la gouvernance. Doit-on faire confiance au marché ? À des syndicats de bonnes volontés qui réuniraient toutes les parties prenantes (autorités publiques nationales, entités transnationales, éléments des sociétés civiles, groupes de spécialistes, etc.) ? Ou en revenir à un gouvernement politique bouclé par les États, par accords directs ou à travers des organisations interétatiques ? La tendance « désétatisante » de la dernière décennie ne s'inverse-t-elle pas, en partie sous le poids de puissances émergentes qui entendent contrôler le système pour leur plus grand profit politique ? La réponse n'est pas simple, les composantes possibles de cette gouvernance (autorités politiques, sociétés civiles, etc.) étant très diverses et affichant des intérêts et des stratégies contradictoires.

Il faut cependant aller plus loin, et se demander si cette manière de poser la question – assez classique en ce qu'elle se réfère à des architectures institutionnelles – n'est pas dépassée par la technique elle-même. La fameuse « neutralité » de l'internet résistera-t-elle aux nouvelles techniques de traitement des informations massives, et au désir de valoriser des infrastructures de plus en plus coûteuses ? Les techniques de recueil, et de traitement, de volumes massifs de données ne constituent-elles pas un saut révolutionnaire ? Pour la logique de fonctionnement de la toile

mondiale certes ; et au-delà pour l'information et donc le pouvoir économiques, pour la manière dont nous accumulons et gérons notre information sur les faits sociaux ? L'approche par le Big Data ne recentre-t-elle pas notre philosophie de la connaissance sur la mesure statistique plus que sur l'obligation analytique ? Avec les abîmes intellectuels et sociaux que l'on peut imaginer ? Les barrières doivent-elles être posées dans les technologies elles-mêmes ou dans les procédures d'utilisation ? Autrement dit, c'est le concept même de « gouvernance de l'internet » qui doit maintenant être défini, sous les fausses évidences institutionnelles.

On le voit, réfléchir sur l'internet, ses techniques, ses manipulations, ses efforts de gouvernance, c'est suivre une métaphore de notre monde international, hétérogène, multicentré, aux acteurs difficilement dénombrables, et que la logique peine à ordonner.

Hors dossier mais en lien avec ces questions, on s'interroge également ici sur la manière dont les catégories de la logique stratégique (identification des acteurs, temporalité des réactions, maîtrise des actions et réactions, etc.) survivraient à une cyberagression ou à une cyberguerre. Le moins que l'on puisse dire est que s'il nous faut une stratégie face à ces hypothèses – qui croissent en crédibilité –, elle reste, comme ses moyens, à inventer.

Depuis la pandémie de sida, le concept de sécurité sanitaire s'est imposé dans le champ international. 2014 l'a remis sur le devant de la scène avec l'épidémie du virus Ebola. Deux textes posent dans ce numéro des questions de fond pour la gestion des épidémies – dont le danger va croître inévitablement avec l'accélération des circulations humaines. Première question : la coopération internationale répond-elle au danger, au niveau et avec l'efficacité requis ? Il semble bien que non, en particulier parce que – toujours la gouvernance... –, la répartition des rôles n'est pas claire entre organisations non gouvernementales et États, ces derniers disposant seuls, *in fine*, de la force de frappe et des moyens nécessaires. Deuxième question : pourquoi les sociétés locales peinent-elles à se conformer aux règles (sociales, sanitaires, etc.) qui paraissent évidentes, impératives, aux sociétés développées qui interviennent chez elles en temps d'urgence ? Sans doute parce que, au-delà de la désorganisation des systèmes de santé locaux, la mémoire de la colonisation, l'image d'un monde de rapports inégaux, font entendre notre intervention de pays riches comme l'écho d'une entreprise multiséculaire de domination. La remarque vaut pour la gestion des futures crises sanitaires, mais sans doute aussi pour l'ensemble de nos interventions extérieures...

Au fil de cette livraison qui parcourt nombre d'enjeux fondamentaux du monde actuel, on relèvera trois autres thèmes de réflexion. Premier thème : l'étrange mélange de forces publiques et privées qui prétend aujourd'hui concourir à la sécurité du Mexique. On sait que, désormais, dans un nombre croissant de pays, le maintien de l'ordre public est affermé à des officines privées, plus ou moins économiques, plus ou moins criminelles : l'exemple des groupes d'autodéfense civile mexicains est emblématique des problèmes que pose ce glissement. Deuxième réflexion : sommes-nous en train de changer la logique d'usage des armes avec les « robots tueurs », ou ceux-ci, créations humaines et donc contrôlées par l'homme, relèvent-ils des mêmes cadres, logiques et juridiques, que d'autres armements utilisables à distance ? Troisième interrogation – liée, paradoxalement, à la précédente – : si nos sociétés démocratiques endossent la responsabilité de ce qu'elles font sur le champ de bataille, comment cette responsabilité peut-elle être justement mesurée, sans que soit bridée ou, pire, ignorée, la spécificité de l'engagement militaire ? Les réponses françaises sont ici étudiées, à partir de l'exemple de la prévôté aux armées, active particulièrement sur les champs d'intervention extérieurs.

Internet, Ebola, sécurité intérieure, opérations extérieures : *Politique étrangère* se mesure aux thèmes les plus rudes du débat international – un débat qu'interroge une fois encore, et qui s'en étonnera, la rencontre, particulièrement créatrice et violente pour notre temps, de la technique et de l'humain.

politique étrangère