Numérique : activisme et influence politique

François-Bernard Huyghe[1]

Dans les années 1990, les premières anticipations sur le devenir d'internet se construisent autour de trois mythes fondateurs :

- celui du contrôle absolu à la Big Brother : les techniques instruments de surveillance du citoyen tracé, observé, espionné, prévisible et conforme ;
- celui du chaos : le grand accident informatique ou le grand sabotage plongeant dans l'anarchie nos systèmes économiques et politiques dépendants de l'informatique ;
- celui de la prise de pouvoir démocratique : ne pouvant plus être isolés ou censurés, désormais capables de s'exprimer ou de participer à la vie publique, les citoyens allaient inventer de nouvelles formes de démocratie sur l'Agora planétaire qu'ouvrirait le cybermonde.

Deux ans après une ébauche de « Twitter révolution » iranienne manquée, c'est ce dernier thème qu'a semblé illustrer le printemps arabe de 2011 d'abord en Tunisie puis en Égypte, avec des révoltes ou révolutions vite baptisées « Facebook » ou « 2.0 » par leurs propres partisans. Des révoltes que tentent d'ailleurs vite d'imiter des manifestants d'autres pays après qu'elles se soient répandues dans le monde arabe comme par mimétisme d'un activisme inédit.

Bien sûr, personne ne soutient sérieusement que les printemps arabes aient donné raison seuls au cyberutopisme militant. Si les révolutions politiques ne dépendaient que de conditions technologiques, ce serait trop simple. Ce serait négliger des disparités (voir le taux d'équipement internet très différent de la Tunisie à la Libye), sous-estimer le rôle des télévisions par satellite arabophones et la mobilisation de l'opinion libérale internationale. Ce serait surtout oublier qu'une révolution est un acte de confrontation physique par lequel des foules s'emparent d'un pouvoir face à une police qui tire ou ne tire pas. Ce serait enfin ignorer que l'efficacité des réseaux sociaux pour « dégager » un pouvoir discrédité ne garantit ni une fin heureuse, ni une victoire électorale, ni ne protège contre le retour des « vieux » coups d'État ou de la violence djihadiste.

Mais, même réduit à un rôle d'accélérateur, d'amplificateur ou de déclencheur d'événements qui ont d'autres causes et impliquent d'autres processus, internet a changé la façon de militer, de se mobiliser voire d'être ensemble et de faire de la politique.

---

1 Directeur de recherche à l'IRIS.

Les États le savent et recherchent de nouvelles stratégies de censure, ou veulent tourner à leur profit le phénomène des réseaux sociaux, qu'il s'agisse de combattre leurs adversaires politiques ou d'amplifier une influence, déjà relayée par des médias classiques et des réseaux humains…

Mais le jeu s'ouvre à d'autres acteurs encore : groupes de hackers professant parfois une idéologie de la transparence hostile à tout pouvoir, éventuellement groupes mercenaires à faux drapeaux, acteurs économiques qui ont des intérêts financiers évidents dans leur conquête des marchés mais qui se trouvent confrontés à des questions d'éthique et de politique relatives au contrôle d'internet (voir l'exemple du bras de fer entre la Chine et Google ou Facebook rétropédalant pour assurer qu'il combattra la diffusion de fausses nouvelles susceptibles notamment d'influer sur les élections).

Les réseaux sociaux se sont montrés extraordinairement efficaces pour exprimer des opinions interdites, pour stimuler des indignations contagieuses, pour trouver des appuis hors frontières (médias, diaspora, groupes militants tels les Anonymous…), pour montrer les exactions du pouvoir, pour donner des mots d'ordre de rassemblement ou énoncer des revendications et pour jouer à cache-cache avec la police.

Leurs atouts :

- vitesse de communication et de mouvement supérieure à celle de l'adversaire débordé,
- initiative constante et prise de décision décentralisée bien en accord avec la structure des réseaux,
- recours à « l'intelligence des foules », des solutions élaborées collectivement, que ce soit pour contrer les initiatives policières ou imaginer des contre-discours,
- faculté de faire converger des indignations diffuses en mobilisations contre un objectif symbolique (l'autocrate à qui on crie « dégage » ou le système),
- capacité éventuellement de converger physiquement de partout vers un objectif unique comme une sorte d'essaim, de « swarming » suivant la terminologie américaine,
- volonté de déborder les frontières nationales pour trouver un écho, des alliés ou des ressources techniques,
- théâtralité, sens de l'image proposée aux médias (une révolte populaire, sans chefs, directe, sans médiations ni partis, représentative de la société civile, n'ayant besoin ni d'avant-gardes ni de violence pour parvenir à ses fins) : autant de leçons stratégiques à retenir de ces affrontements.

Le « faible » (la foule coordonnée par les technologies de l'information) menace le « fort » (l'État). Ce dernier ne peut plus exercer ses attributs classiques : le monopole de la violence légitime (qui arrêter ?), la territorialité (les électrons ignorent les barrières douanières et l'État doit combattre

des cyberadversaires ou cyberdissidents hors frontières), l'autorité (débordée par des foules plus rapides, plus coordonnées…) et même le spectacle du pouvoir (le discours officiel n'attire même plus l'attention des populations qui se tournent, soit vers le web, soit vers les télévisions internationales d'information).

Les réseaux sociaux ne servent pas seulement à publier des opinions qui seraient autrement étouffées ou à faire des révélations qui seraient censurées : ils font naître de nouvelles formes de communautés et de faire passer d'un lien « faible » dans le cybermonde à un lien fort et passionnel dans la « vraie vie », comme ils commencent à créer l'ébauche d'un espace public pour une société civile sous le boisseau. Sans oublier qu'ils servent aussi à provoquer symboliquement un pouvoir (en attendant de le défier physiquement par des occupations interdites des places et des rues).

Les autocraties sont parfois capables de réagir : elles vont utiliser de nouveaux instruments sur la Toile, plus subtils que les arrestations de blogueurs influents ou la coupure du Net (intenable plus de quelques heures). Adopter de fausses identités pour infiltrer la cyberdissidence, créer des réseaux de blogueurs « patriotes à la chinoise », se doter d'équivalents nationaux de Facebook ou de Google, et d'une blogosphère sous contrôle, peser sur les fournisseurs d'accès, exploiter des mots clefs pour attirer les recherches sur des sites souhaités comme en Syrie, attaquer des sites étrangers qui aident la contestation, utiliser de la technologie occidentale pour filtrer et repérer en attendant de se doter d'un internet « balkanisé », avoir le contrôle sur ses propres fournisseurs d'accès, ses moteurs de recherche et ses réseaux, « géolocaliser » les adversaires en mouvement, analyser les réseaux sociaux et leurs échanges pour prédire qui risque de rentrer dans la dissidence (comme les sociétés commerciales « prédisent » l'intérêt de tel internaute pour tel type de produit) : telles sont les ripostes qui se dessinent sous nos yeux. Et il n'est nullement certain qu'elles soient partout inefficaces.

L'État peut aussi espérer gagner une influence au-delà de ses frontières grâce à ces mêmes technologies 2.0, ou du moins déstabiliser des rivaux en encourageant des mouvements d'opinion.

Le politique peut exercer une contrainte ou un contrôle, passer des alliances ou entamer une confrontation avec des acteurs économiques et techniques - opérateurs, fournisseurs d'accès, services de connexion - pour faciliter ou écraser tel courant d'opinion. Il peut aussi imiter les techniques du « faible ». Par exemple en déstabilisant un État ou un mouvement d'opinion adverse par des « leaks », de fuites, qui combinent la méthode du hacker pour accéder aux documents compromettants, la tactique de l'activiste pour leur donner un écho international et une stratégie globale de guerre de l'information.

Comme on le voit, les « coups » que peuvent jouer les acteurs - activistes, bureaucraties, organisations non-étatiques, entreprises - sont nombreux, complexes et souvent entourés d'un halo de secret.

À cette complexité technique et stratégique, il faut ajouter un élément idéologique au sens le plus large : le poids de ce que l'on croit vrai en fonction de ses valeurs et de l'opposition à un adversaire politique. L'élection présidentielle américaine de 2016 - l'année où « ère de la post-vérité » a été promu mot de l'année par les Oxford Dictionnaries - a montré une double rhétorique de défense promue notamment par l'administration Obama et la majorité des médias *mainstream* américains :

- Premier élément : l'hypothèse d'une intervention russe pour fausser le processus démocratique. Celle-ci aurait pris la quadruple forme d'intrusions informatiques (hacking, utilisation de trolls pour polluer les débats), de mobilisation de réseaux humains complices (dont ceux de Trump lui-même), de l'utilisation de médias internationaux de propagande (comme Rossia Today ou Radio Spoutnik qui feraient dans le sens Est-Ouest ce que Voice of America et Radio Free Europe faisaient dans le sens Ouest Est pendant la guerre froide) et enfin de la diffusion de « fakes », de fausses nouvelles déstabilisatrices et subversives sur les réseaux sociaux.

- Second facteur : la réceptivité du public à ces « fakes » justement qui auraient largement déterminé le vote à partir de données ou de rumeurs volontairement biaisées. Que l'on explique cela par l'habileté des faussaires en ligne, par la crédulité du public envers tout ce qui flatte ses préjugés et qui le rend imperméable à l'information *mainstream* ou encore par un effet pervers : les réseaux sociaux enferment dans des « bulles d'isolement » favorables par nature à la propagation d'une information douteuse « de pair à pair » et au développement d'interprétations délirantes et théories complotistes.

Du coup on voit se mobiliser des gouvernements, de médias, mais aussi des grandes compagnies du Net pour repérer, signaler, vérifier, réfuter et éventuellement rendre inaccessibles aux tentatives de recherches des contenus faux, relevant d'opérations d'influence ou de discours de haine.

Ils réagissent comme si une allergie des masses au réel menaçait nos démocraties. Le discours d'en haut, censé s'appuyer sur la science ou des faits, est concurrencé par des réalités alternatives conformes aux passions et aux peurs des masses ; ces dernières se détournent des mass médias au profit des « révélations » des « communautés » virtuelles. Si l'on attribue souvent la faute aux manœuvres des démagogues et truqueurs (voire à des services d'États étrangers), il a bien fallu que leur message rencontre un milieu favorable et soit repris par des médias adaptés, et il a fallu qu'il soit relayé. Soit dit en passant, par rapport aux propos qui se tenaient en 2011 le point de vue sur les interventions de médias étrangers ou sur la faculté des réseaux sociaux d'exprimer une opinion reflétant la sagesse des foules et qu'aucun gouvernement ne devrait pouvoir censurer ont singulièrement évolué en cinq ans.

L'idéologie dominante ne se reconnaît pas au fait que tout le monde y adhérerait (elle peut même être assez minoritaire), mais à sa position qui lui permet de réclamer le monopole de l'évidence ou des opinions acceptables sans scandale et souvent aussi à son programme d'en finir avec toutes les idéologies (puisqu'elle possède le vrai). Or c'est ce régime qui se détraque.

Nos sociétés souffrent à la fois de surinformation (toutes les versions de la réalité en ligne), de clôture informationnelle (chacun peut s'isoler dans sa bulle de confirmation de la réalité) et de concurrence informationnelle (les deux camps s'accusant mutuellement de nier la réalité). Et la lutte entre les activistes et leurs adversaires devient moins un conflit pour dire ou révéler qu'une compétition pour l'attention et la confiance, deux ressources que le cerveau humain produit en quantité limitée et qu'il alloue de façon parfois surprenante.