# **Audition de Camille François** (Graphika)

18 octobre 2021

Au sein de ce qu'on regroupe sous le terme anglais d'*Information disorders*, il importe de séparer différents types de menaces, en utilisant le prisme ABC : A pour Acteurs, B pour comportement (Behavior), C pour Contenus.

**Une prise de conscience collective des menaces numériques sur la démocratie**

L'élection de 2016 restera un traumatisme durable pour les entreprises de la Silicon Valley, dont l'incapacité à protéger le système électoral américain a été pointée du doigt par toute la société américaine ; faisant amende honorable, elles ont amorcé un processus d'assainissement qui a permis de ne pas répéter les mêmes erreurs aux élections suivantes : à partir des élections américaines de mi-mandat de 2018, elles ont notamment travaillé main dans la main avec le FBI.

2017 a marqué un accroissement des problèmes de manipulation stratégique des informations, venus notamment de Russie et d'Iran. Les plateformes ont alors fait des efforts notables de détection et de lutte contre les ingérences étrangères, d'abord en partageant les résultats de leur détection avec les gouvernements, puis très vite en les mettant à disposition du grand public.

Un rapport de 200 pages a été publié dans le cadre de *l'Electoral integrity project*, lancé par l'université de Harvard et celle de Sidney, pour analyser la transparence des élections dans le monde et pointer du doigt les menaces étrangères qui pèsent sur elle.

Le sujet des ingérences est source de tension tripartite entre gouvernements, chercheurs et plateformes : dans le cadre d'un rapport sur l'ingérence de la France dans les affaires africaines, Politico a accusé la France d'avoir envoyé des rapports secrets à Facebook dénonçant les comportements des russes.

**Un début d'essoufflement**

Après les efforts de 2017-2020, la pression publique se détourne peu à peu des questions d'ingérence étrangère au profit des phénomènes conspirationnistes. Symptôme d'un essoufflement de la vigilance, la banque d'informations où Twitter révèle les manœuvres d'ingérence étrangères qu'il a repérées en son sein n'est plus alimentée depuis 9 mois.

**Une asymétrie de définition et de lutte contre les ingérences**

Chacun des trois géants de la Silicon Valley traite la question des ingérences avec un crible différent.

**Twitter** définit l'ingérence a minima, comme un acte de falsification coordonnée en provenance d'une puissance étrangère identifiée ; s'il n'a a pas réussi à la relier à un Etat, il ne publiera aucune information sur cette ingérence. Cette conception est chaque jour moins adaptée aux conflits numériques contemporains, où les attaque sont de plus en plus polymorphes et cryptées, sous couvert de faux-drapeaux et d'intermédiaires fantômes, à

l'instar des attaques iraniennes de 2020. De nombreuses opérations peuvent être téléguidées par des intérêts étatiques, sans être pour autant le fait d'états étrangers.
**Facebook** a une définition a maxima, considérant comme une ingérence toute forme de « Coordinated inauthentic behavior », même s'il n'a pas réussi à les rattacher à une puissance étrangère.
**Google** n'a pas publié de définition claire ; il est celui qui a partagé le moins d'informations, et le plus tard.

Vis-à-vis du conspirationnisme, même dissymétrie :
Quand le phénomène QAnon s'est répandu sur les réseaux sociaux, Twitter a traité le flux à la source, en supprimant des milliers de compte actifs dans la propagation de ces théories. Facebook est allé plus loin et a supprimé tous les comptes représentant QAnon, quand bien même ils n'avaient publié aucun contenu politique. Google en revanche s'est contenté de supprimer les posts relayant les théories de QAnon, au cas par cas, travail de modération difficile qui entraînait des délais de suppression longs.`

**Le problème est donc double :**
1) Les régimes de lutte contre les ingérences sont insuffisants
2) Ils sont progressivement abandonnés

**Pistes de solution**

Un volet de régulation s'impose : inciter les services de sécurité des plateformes à prendre un engagement plus clair et à s'y tenir. La France et l'UE peuvent les pousser à reprendre leurs efforts et à faire converger les définitions (dans le sens de l'élargissement), sans qu'il soit nécessaire d'imposer une uniformisation parfaite. Les plateformes sont globalement preneuses d'intervention gouvernementale, qu'elles voient non pas comme une coercition, mais comme une aide ; il arrive fréquemment qu'elles affichent par écrit leur gratitude envers les états qui leur ont prodigué des « tips ».

Un travail de décryptage rétroactif est nécessaire. Après les élections de 2016, les Américains ont travaillé à discerner précisément le rôle qu'avaient joué les puissances étrangères. La France n'a pas encore procédé à ce travail de recherche, alors qu'elle aussi a été la cible d'ingérences malveillantes : l'équipe de recherche de Camille François a dévoilé il y a deux semaines l'ampleur des attaques iraniennes à l'encontre de la France.
Grâce à une vigilance accrue des plateformes et des pouvoirs publics, les disfonctionnements de 2017 ne devraient pas se répéter en 2021. Pour autant, seul un travail de recherche et de relecture approfondi permettra une pleine lucidité vis-à-vis des menaces à venir.