

<https://www.laicite-aujourd'hui.fr/?Trafic-2>



Trafic des opinions , réseaux sociaux (2)

- NOS TRAVAUX -



Publication date: lundi 3 juin 2024

Copyright © Laïcité Aujourd'hui - Tous droits réservés

Pour la réunion du 15 mai, par JYR

Trafic des opinions, réseaux sociaux ou de la toxicité des données et de leurs supports pour la démocratie

Partie 2

De l'exploitation rationnelle et industrielle des faiblesses cognitives à la « guerre cognitive »

Dans la première partie, on s'est penché sur quelques déterminants de la publicité ou la propagande et on a évoqué la possibilité de « guerre cognitive » via des stratégies et technologies numériques, mettant à mal le libre arbitre lui-même et sapant les bases de la démocratie.

A travers quelques exemples documentés, déjà anciens, on essaiera d'illustrer la situation actuelle de l'exploitation rationnelle et industrielle de nos faiblesses cognitives par les réseaux sociaux.

- Comment ça fonctionne ?
- A qui cela profite ?

Comment définir un réseau social numérique ?

On peut définir un réseau social comme un agencement de liens entre des individus ou des organisations, constituant un groupement qui a un sens : la famille, les collègues, un groupe d'amis, une communauté. En pratique tous les sites web, applications mobiles et plateformes permettant de créer du lien social en ligne peuvent être considéré comme des réseaux sociaux.

Quelques exemples connus Facebook, Instagram, X-Twitter, Tiktok, Youtube, Spotify, Snapchat, LinkedIn, Viadeo, Vimeo, Daylimotion Tumblr, MeetUp, Eventbrite, Flickr, Twitch, Whatsapp, Deezer, Spotify, Discord etc.

Les réseaux sociaux (RS) sont l'objet de nombreuses critiques sévères, ou de mise en accusation.

Loin de leur objet initial, en général faire de l'argent, elles ont dérivé plus ou moins volontairement.

Jaron.Z. Lanier, un des pionniers de la réalité virtuelle, est également connu pour ses analyses de l'utilisation d'internet, et sa critique des réseaux sociaux tels que Twitter ou Facebook. Selon lui, « Vous ne pouvez pas lutter face à l'algorithme de Twitter qui est construit pour exciter vos émotions négatives et vous transformer en trou du cul. C'est le meilleur moyen de vous rendre dépendant, ce sont les mêmes ressorts comportementaux que les machines à sous dans les casinos ».

Il fait une critique virulente du concept de la « Sagesse des foules » selon laquelle on résoudrait mieux un problème en s'y mettant nombreux.

Il décrit ainsi que **la perte du libre arbitre** par les RS, l'altération de la vérité, la perte de sens des propos ainsi que de la capacité d'empathie, conduisent à une polarisation avec radicalisation des foules.

Des exemples de manipulations



L'analyse des manipulations survenues lors de l'élection présidentielle de 2017 en France permet d'en démontrer la mécanique et son tempo :

D'abord, instaurer une relation de confiance par la mise en ligne de sites prétendant créer de l'information : de faux comptes échangent avec vrais comptes sur sujets anodins (animaux, foot, mais aussi n'importe quoi tel que fausses nouvelles inquiétantes etc.). Environ deux semaines avant le scrutin apparaissent des « mêmes » négatifs par rapport à un candidat, mais aussi des rumeurs plus au moins vraies ou fausses.

Enfin, une phase coup de poing, souvent entre les deux tours, par des messages à fort impact avec délai trop court pour vérifier, comme pour les « Macron leaks »

#Macronleaks

Le 15 mars 2017, LREM subit un siphonage de ses données numériques.

La société japonaise de cybersécurité Trend Micro a identifié l'attaque et l'a attribuée au groupe de cyberespionnage APT28 lié à l'agence de renseignement militaire russe GRU.

Quand Macron dépasse Fillon dans les sondages, il devient la cible d'attaques plus agressives et plus organisées provenant de deux sources : les médias du Kremlin (RT et Sputnik) et l'alt-right américaine.

<https://politoscope.org/2017/05/finalpush/>

En brun essentiellement Extrême droite USA ... en Bleu Extrême droite Française

Le 5 mai 2017 19h59, publication de plus de 21 000 des courriels piratés et de faux courriels sur 4CHAN par William Craddick (auteur du Pizzagate, Hillary Clinton), relayée aussitôt sur Facebook et Twitter sous le hashtag #macronleaks, d'abord Jack Posobiec sur Tweeter, et l'Alt-right américaine (en brun sur graphique) et suivie par les militants du Front National ou Extrême-droite (en bleu sur graphique) (Fl. Phillipot, M Le Pen, Samuel Lafont...). #macronleaks apparait 47000 fois en 3h30, relayée par 18000 bots. ½ million de tweets apparaissent en 24h avec des traces de modifications de fichier (en particulier en cyrillique très probablement d'origine russe).

Cette affaire des Macronleaks, a donné lieu à une étude très détaillée de l'Atlantic Council's Digital Forensic Research et l'IRSEM 1

1 https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf

Autre exemple, **#Alijuppé**, ou la campagne Ali Juppé, imam de Bordeaux

On est lors des primaires de la présidentielles de 2017.

En 2008, Alain Juppé avait donné son accord pour la construction de la grande mosquée de Bordeaux.

Déjà en 2016, il est accueilli à la Fac de droit d'Assas avec une banderole « Ali Juppé, grand mufti de Bordeaux »

Le hashtag #Ali Juppé est lancé pendant les primaires pour la présidentielle de 2017 par des éléments du Front National, relayés par les droites classiques avec de nombreuses caricatures et mêmes diffusés par les réseaux et des chaînes de courriels.

Autre exemple : comment créer un problème ? Le néologisme « islamo-gauchisme »

- islamo-gauchisme : mot-valise introduit en 2002 par **P.A. Taguief** (dans son livre *La Nouvelle Judéophobie*) - lors de la 2de Intifada –pour désigner une convergence contre Israël, entre une partie d'extrême-gauche et les intégristes musulmans. Devenu un mot flou et stigmatisant, popularisé notamment par l'extrême droite, le terme désignerait plutôt maintenant une proximité supposée entre des idéologies, personnalités ou partis de gauche et les milieux musulmans, voire islamistes.

- Selon l'Institut des Systèmes Complexes de Paris (** CNRS (UAR 3611) (données du Politoscope)2

2 Création d'un problème – Toxic data , comment les réseaux manipulent nos opinions ; D. Chavalarias - Champs actuels 2022 - p 223 : <http://toxicdata.chavalarias.org/analyses/islamogauchisme.html>

Entre 2017 et 2020, l'expression est utilisée de manière péjorative, majoritairement sous la plume des partisans de l'extrême droite.

- ▶ pour discréditer les opposants de gauche, surtout la France Insoumise
- [-] pour convaincre l'opinion publique d'une nouvelle catégorie d'acteurs : des ennemis intérieurs, alliés aux forces de l'islamisme radical.

L'extrême droite a échoué pendant 15 ans à imposer la croyance collective en un ennemi intérieur islamo-gauchiste... Deux ministres vont la booster.

Tout change après l'assassinat de Samuel Paty le 16/10/2020. Les déclarations de **J.M. Blanquer** (Min. E.N.) 22/10/2020, (*relayées aussitôt par l'extrême droite*) et surtout les déclarations de **D. Vidal** (Min. Univ.) 16/02/2021, vont enflammer les réseaux sociaux, d'abord le RN (600 000 Tweets entre le 31/01/2021 et le 11/05/2022, puis LFI, en réaction (400 000 Tw pendant le même temps). Enfin Zemmour entre en pré-campagne présidentielle en octobre 2021 et va produire 450 000 Tw jusqu'à la mi-juin 2022.

Des caractéristiques de ce type d'évènement numérique

Cela semble venir de partout, c'est « déspatialisé » et massif.

C'est quasi instantané.

Il y a une confusion volontaire des identités, mise à profit, en particulier, par l'Alt Right et illibéraux minoritaires, pour toucher les masses.

On joue sur les émotions, pour créer des interrogations ou des croyances à travers des **biais de perception** créés par une activité intense artificielle des réseaux.

Au total : comment ça marche ?

Premier temps, il faut **capter l'attention**,

- [-] en faisant peur (par exemple : les vaccins à ARN modifient votre génétique en changeant votre ADN),
- ▶ en racontant des choses vraies au milieu d'histoires fausses invraisemblables,
- [-] en créant l'attente de matérialisation de prédictions, même infondées, et très vagues ou improbables.

Travailler les biais de groupe, de représentativité et de halo

- [-] En créant de nouveaux sites relais ou prétendant informer : bots, activités de fermes à trolls

En créant de la polémique grâce à des trolls

Créer des chambres d'écho

- [-] tromper sur l'intensité de l'adhésion à une cause (bots, trolls etc.)

- [-] tromper sur le caractère spontané de l'adhésion (faux comptes...)

[-] Faire de l'astroturfing : c'est une stratégie de communication (publicitaire ou politique) dont la source réelle est occultée, créant l'illusion d'un consensus ou d'un soutien spontané d'une population à une cause. C'est une contrefaçon de mouvement populaire.

Exemple : durant l'élection présidentielle de 2022, l'équipe de campagne d'Éric Zemmour a créé des milliers de comptes Twitter pour gonfler artificiellement sa présence sur le réseau social. L'objectif était de diriger les internautes vers sites gérés par l'association des amis d'Éric Zemmour et d'assurer un afflux d'adhérents et de dons. (02 février 2022, Le Monde.fr)

Créer des bulles

[-] en resserrant les mêmes contenus aux mêmes groupes et polariser

[-] créer de la contagion algorithmique : un compte sur réagit, ses « amis » sont poussés à liker

– la bulle de filtre polarisée exclue les nuances, et se renforce en interne par effet psychologique de biais de confirmation renforcés par des messages angoissants.

[-] Ainsi se créent des boucles infernales s'amplifiant les unes les autres, créant de grosses bulles d'opinion hyperpolarisées, où disparaissent les nuances, et qui viennent elles-mêmes renforcer les autres.

Des boucles infernales

<https://www.laicite-aujourd'hui.fr/local/cache-vignettes/L52xH52/pdf-39070-1a839.png>

Commentaires

La conjecture de von Foerster énonce que plus les éléments d'un système sont solidement connectés, moins ils auront d'influence sur le système dans son ensemble.

Elle a donné lieu dans le champ sociologique au **Théorème de Forster- Dupuis** qui énonce que :

1. Pour un individu au sein d'une société, plus l'influence sociale entre individus est forte, plus les dynamiques et les directions que prendra cette société seront a priori imprévisibles à ses yeux – dans sa bulle il ne voit rien autour.
2. Pour une entité capable d'observer les actions de chaque individu, plus l'influence sociale entre individus est forte, plus cette entité est en mesure de prévoir et anticiper le comportement global de ces individus
3. Corollaire, les réseaux sociaux et les acteurs de la Big Tech, disposent d'un point de vue extérieur, et s'efforcent d'augmenter l'influence sociale de leurs plateformes afin de mieux prévoir et orienter les comportements collectifs.

Par exemple :

sur le plan commercial, Amazon, Netflix etc. anticipent les achats sur les données de ses clients et des contextes, et poussent leur comportement dans le sens souhaité (nudge).

Le plan politique est illustré par le scandale Cambridge analytica (société promue par Steve Banon, conseiller de Trump, Nigel Farage –(Brexit) - ou M Le Pen aux Elections européennes 2019) avec le siphonage des données de 87 Millions d'utilisateurs de Facebook pour les profiler et micro-cibler les messages pour D Trump -2016- mais aussi le BREXIT ou M. Le Pen (Européennes 2019)

Les réseaux sociaux ne sont pas neutres : Créés initialement pour faire de l'argent, leurs algorithmes de modération peuvent être politiquement orientés : Elon Musk, (X tweeter), Mark Zuckerberg (Facebook) sont devenu objectivement des soutiens de l'extrême-droite américaine et, plus, ils ont réduit leurs possibilités de modération.

A qui profite les fausses informations ?

Interrogation de IA générative de Google, Bard (07/02/2024) (devenue Gemini)

Réponse, (sic)

Les fausses informations sur les réseaux sociaux profitent à plusieurs groupes :

1. Les acteurs politiques malveillants :
 - Propagation de la désinformation et des discours de haine
 - Déstabilisation des démocraties pour saper la confiance dans les institutions démocratiques et semer la discorde au sein de la société.
 - Gagner du pouvoir et de l'influence pour accroître leur popularité

2. Les entreprises et les organisations à but lucratif :

- Augmentation de la visibilité et du trafic : pour générer du buzz et de la publicité
- Manipulation du marché boursier : influencer les décisions des investisseurs.
- Augmentation des ventes et des profits : tromper les consommateurs et les inciter à acheter des produits ou des services dont ils n'ont pas besoin.

3. Les groupes extrémistes :

- Recrutement de nouveaux membres
- Justification de leurs actions
- Création d'un climat de peur et d'intimidation : dissuader les gens de s'exprimer ou de s'opposer à leurs actions.

4. Les individus malintentionnés :

- Diffusion de rumeurs et de mensonges : Les fausses informations peuvent être utilisées pour nuire à la réputation d'une personne ou d'un groupe.
- Escroquerie et fraude : Les fausses informations peuvent être utilisées pour escroquer les gens ou leur voler de l'argent.

- Harcèlement et cyber intimidation : Les fausses informations peuvent être utilisées pour harceler et intimider les gens en ligne.

On pourrait croire cette IA capable d'ironie quand elle conclut : « ... Il est important de noter que les fausses informations ne profitent pas à tout le monde.

Elles peuvent avoir des conséquences négatives graves pour les individus, les sociétés et les démocraties. Il est donc important de rester vigilant face aux fausses informations et de s'assurer de ne partager que des informations provenant de sources fiables. »

Des agences spécialisées dans la désinformation

Exemples (non limitatifs !) d'agences célèbres de désinformation

QAnon Mouvement sectaire conspirationniste d'extrême droite et soutien de D. Trump.

Le mouvement QAnon a pris énormément d'ampleur depuis ses débuts en 2017, et certaines de ses vidéos explicatives atteignent des millions de vues.

Le 5 juillet 2020 une vidéo du Général Michael Flynn, ancien conseiller à la sécurité nationale de Trump, le montre prêtant allégeance à QAnon.

Exemple de teaser de Qanon : Générateur de prédictions constamment renouvelées - Stratégie, utilisée par « Q » et d'autres influenceurs complotistes. Ce dispositif permet de capter l'attention et de rassembler une audience importante : plusieurs millions de vues sur X (Twitter)

<https://www.conspiracywatch.info/comment-un-generateur-de-predictions-qanon-totalise-des-millions-de-vues-sur-x.html>

APT28 (Advanced Persistent Threat 28) aussi nommé Fancy Bear, Pawn Storm, ou Sednit) groupe hacker accusé d'être lié à l'agence de renseignement militaire russe GRU. A l'origine de nombreuses attaques, de TV5 Monde à des cibles de type géostratégiques.

I R A : Internet Research Agency – basé à St Pétersbourg, est un groupe industriel de type Ferme à Trolls Créée par Evgueni Prigojine (*Wagner*). Avec environ 400 employés, il industrialise les commentaires de l'actualité, mêlant vraies et fausses nouvelles, relaye Qanon et les conspirationnistes etc. sur LiveJournal, Twitter, VKontakt, Facebook, Instagram, Ticktok, etc

Mais aussi bien d'autres privées ou d'Etat :

Les États peuvent recruter directement des hackers par l'intermédiaire de leurs armées et de certains organismes gouvernementaux, comme la NSA américaine (mais aussi affaire Snowden).

La frontière entre organisations criminelles et services gouvernementaux se brouille

Des groupes de hackers parrainés par les États peuvent cibler d'autres États à différentes fins.

Des agences peuvent travailler à dépister la désinformation et en produire : comme PERCEPTO en Israël avec la création de faux journalistes « deep avatars » (Anita Pettit censée travailler entre la France et l'Afrique, ou Chloé Boyer au Burkina Faso) etc.

IRAN : tout un écosystème de désinformation dont l'IRIB Radiotélévision de la République islamique (Sāzmān-e Sedā va Sima-ye Jomhūrī-ye Eslāmī-ye Īrān

La CHINE par le contrôle interne de sa population, mais aussi des outils de pénétration tels que Tiktok, la 5G de Huawei ou le Routes numériques de la Soie

Etc.

[JPEG](#)

Conclusion : Capitalisme d'influence et Démocratie

Pour le Capitalisme d'influence :

– l'opinion : est la nouvelle matière première à travailler.

– Les nouveaux barons du capitalisme d'influence, s'en chargent

Les maîtres des environnements numériques ont un intérêt économique à les saturer d'influence sociale.

La saturation facilite la manipulation des collectifs par des agents extérieurs.

La saturation rend les comportements collectifs instables et massifs.

► Des manipulations modérées conduisent à des mouvements de grande ampleur

Les démocraties deviennent des régimes très instables

Les acteurs hostiles à la démocratie agissent sur nos systèmes sociaux à des moments propices.

Ils sapent la démocratie.

Pour contrôler leur populations et assurer leur pérennité, ils exploitent soit des environnements numériques fermés (Chine, Russie etc.), soit, en environnements ouverts, des bulles d'influence.

Le BigTech sont devenus des acteurs technologiques plus ou moins sous contrôle des Etats.

Les Etats sont devenus dépendants des BigTech

Selon **Asmah Mallah**, « Le système capitaliste semble être arrivé à son paroxysme : les BigTech ne sont plus des acteurs du système, ils sont à la fois l'infrastructure – la condition du nouveau système économique – et la superstructure, en tant qu'entités idéologiques et politiques... Ils structurent la sphère immatérielle qu'est le cyberspace comme ultime espace de création de richesses et de conflictualités...une extension du domaine de la guerre³ ».

3 Asmah Mhalla : Technopolitique – Comment la technologie fait de nous des soldats – le Seuil – 2024

Selon **l'IRSEM**, « la guerre cognitive apparaît clairement dans la doctrine chinoise, depuis 2012, où l'enjeu n'est pas tant de savoir quelle force armée va gagner, mais quel récit, quelle version des faits va l'emporter auprès de l'opinion publique »⁴ .

4Citation : Ibid : p. 124

Nos cerveaux sont devenus l'ultime champ de bataille.

Il est urgent de le penser car c'est le nouvel ordre mondial qui est en jeu, et la démocratie...

Les acteurs hostiles à la démocratie Agissent sur nos systèmes sociaux à des moments propices.

Ils sapent la démocratie.

Pour contrôler leur populations et assurer leur pérennité, ils exploitent soit des

environnements numériques fermés (Chine, Russie etc.), soit, en environnements ouverts, des bulles d'influence.

Le BigTech sont devenus des acteurs technologiques plus ou moins sous contrôle des Etats.

Les Etats sont devenus dépendants des BigTech.

Selon **Asmah Mallah**, « Le système capitaliste semble être arrivé à son paroxysme : les BigTech ne sont plus des acteurs du système, ils sont à la fois l'infrastructure – la condition du nouveau système économique – et la superstructure, en tant qu'entités idéologiques et politiques... Ils structurent la sphère immatérielle qu'est le cyberspace comme ultime espace de création de richesses et de conflictualités...une extension du domaine de la guerre³ ».

Selon l'IRSEM, « la guerre cognitive apparait clairement dans la doctrine chinoise, depuis

2012, où l'enjeu n'est pas tant de savoir quelle force armée va gagner, mais quel récit,

quelle version des faits va l'emporter auprès de l'opinion publique »⁴ .

Nos cerveaux sont devenus l'ultime champ de bataille.

Il est urgent de le penser car c'est le nouvel ordre mondial qui est en jeu, et la démocratie...

Les guerres informationnelles qui s'y jouent sont désormais industrialisées, s'épanouissent à bas coût et à bas bruit sur des réseaux sociaux devenus partie intégrante de l'arsenal des guerres hybrides dont les trois matières premières et intangibles sont : les modèles artificiels de viralité, l'information (et son corollaire, la désinformation), nos schémas cognitifs et perceptifs.

3 Asmah Mhalla : Technopolitique – Comment la technologie fait de nous des soldats – le Seuil – 2024

4 Citation : Ibid : p. 124

BONUS : Comment se protéger des fausses informations ?

• **Observer les détails** : le titre, les dates, la structure du site... souvent accrocheur, avec des points d'exclamation.

• **Vérifier qu'il s'agit d'une source fiable** :

• **Privilégier les sources d'informations reconnues** (ministères, revues scientifiques, ONG...). avec des urls telles que .gouv.fr, .org, .asso.fr.

Les blogs et sites personnels requièrent plus de vigilance.

• **Varié les sources d'information** : comparer et croiser les données

• **Décrypter les images** : trouver la source d'une image pour la contextualiser, être attentif à sa construction, ou encore utiliser des moteurs de recherche d'images inversées comme Google images ou Tineye.com, pour vérifier qu'une image n'est pas détournée.

[JPEG](#)

Petite Bibliographie et liens

(De nombreux éléments du texte en sont issus)

• Chavalarias David « Toxic Data » E d. Flammarion Champs 2022

• Mhalla Asma : « Technopolitique, Comment la technologie fait de nous des soldats, Ed. Le Seuil fév. 2024

- Lanier Jaron : « Stop aux réseaux sociaux – 10 bonnes raisons de s'en libérer - © De Boeck Supérieur ed., 2020)
- Khaneman Daniel : Système 1, Système 2, les deux vitesses de la pensée, Ed. Flammarion 2012
- <https://www.institutmontaigne.org/expressions/les-reseaux-sociaux-nourrissent-ils-lespopulismes>
- <https://www.institutmontaigne.org/expressions/liberte-dexpression-et-reseaux-sociauxlimpasse-de-la-moderation>
- <https://www.conspiracywatch.info/comment-un-generateur-de-predictions-qanon-totalisedes-millions-de-vues-sur-x.html>
- <http://toxicdata.chavalarias.org/analyses/islamogauchisme.html>
- <https://www.radiofrance.fr/franceculture/podcasts/le-temps-du-debat/les-ingerencesetrangeres-vont-elles-influencer-le-scrutin-europeen-6138983>
- https://hal.science/file/index/docid/632280/filename/SocieteRecommandA_e.pdf
- <https://www.senat.fr/rap/r22-831-1/r22-831-1.html> - La tactique TikTok : opacité, addiction et ombres chinoises – Rapport

Quelques outils de vérification

- <https://www.gouvernement.fr/fausses-nouvelles-guide-des-questions-a-se-poser-face-a-une-information>
- FactCheck.org (en anglais)
- The Atlantic Council's Digital Forensic Research Lab (DFRLab)
- Les Décodeurs (Le Monde)
- <https://www.francetvinfo.fr/vrai-ou-fake/>
- Tineye.com (images)
- Google images (identifier une image)

JPEG

Les débats ont porté :

[-] sur les effets de boucle, la démocratie, une bascule plus facile de par les moyens actuels, un temps de production et d'action différent, l'**I.A.** et la production de contenus sans limite, sa vitesse qui interroge celle du cerveau humain, ... son utilité en médecine (imagerie, détection de l'émergence de maladies, ...)

► sur la nécessité de croiser les informations

[-] sur le caractère anxiogène des informations

[-] sur l'impact sur les jeunes esprits (la force des images ...), leur capacité à s'adapter, les comportements d'évitement, de refuge

Autant d'invitations à se replonger dans l'exposé (1)

<https://www.laicite-aujourd'hui.fr/?Trafic-des-opinions-reseaux-sociaux-1>