Thème 4 : S'informer : un regard critique sur les sources et modes de communication

Chapitre (axe) 3 conclusif : L'information à l'heure d'Internet

Pourquoi l'essor d'Internet ne s'est-il pas traduit par un progrès de la liberté et de la fiabilité de l'information ?

I) Témoignages et lanceurs d'alerte : une liberté plus grande ?

Définition de lanceur d'alerte : ***whistleblower*** en anglais de *blow* (souffler) et *whistle* (sifflet) = un policier qui siffle dans son sifflet pour dénoncer un délit dans la rue et demander de l'aide aux passants pour l'arrêter => une réaction collective saine dans l'intérêt commun. Terme inventé au début des années 1970 par un avocat (écologiste) qui s'est présenté 5 fois à la présidentielle US, Ralph Nader. Il cherche un terme qui n'aurait pas la connotation négative d'« informateur » (*informer*) ou de mouchard et de balance (*snitch*).

A- Biographie d'Édouard Snowden : né en 1983, Snowden est un Américain qui se destine à être militaire. Sa vie bascule le 11-09-2001 : attentats des tours jumelles du world trade center. Il veut servir son pays contre le terrorisme => il s'engage dans la guerre contre le terrorisme lancée par le président G. W. Bush. Mais, un accident (il se brise les deux jambes à l'exercice) en 2004 à 21 ans le prive d'une carrière dans les forces spéciales => comme il était bon informaticien durant ses études => il se reconvertit dans l'informatique au sein de la CIA. 2006 : il rentre à la NSA et connaît une carrière brillante (se spécialise dans les écoutes) ; 2007 : à l'ambassade États-unienne à Genève, il écoute l'ONU et démasque les fraudeurs de fisc États-unien. 2008 : élection d'Obama qui ferme Guantanamo => Snowden croit que les écoutes vont cesser ; mais cela continue => il décide de dévoiler ce qu'il sait ; il collecte des infos avec des clés USB (dont les manuels destinés aux opérateurs de la NSA et un diaporama présentant le programme PRISM). En 2009, il quitte la CIA (et la Suisse) pour le Japon où il travaille pour Dell. 2013 : il fuit à Hong-Kong et contacte deux journalistes et avocats spécialistes de la question (Glenn Greenwald écrit un livre sur les écoutes et Laura Poitras fait un documentaire sur les écoutes). Il leur donne 58 000 documents classés par dossiers sur des disques durs, des docs anonymes pour ne pas porter atteinte à des collègues. Le *Washington Post* publie des articles et Snowden passe à TV => procès aux États-Unis contre lui en 2014 et mandat d'arrêt international => recherché, Snowden quitte Hong-Kong pour un vol Moscou-Brésil en juin 2014 (mais, dans l'avion, les États-Unis suppriment la validité de son passeport => il reste coincé à l'aéroport de Moscou). Les JO d'Hiver de Sotchi doivent avoir lieu en décembre 2014 => des citoyens américains veulent boycotter les JO => pour prouver que la Russie n'est pas une dictature (et que les États-Unis en sont une) Poutine accorde l'asile politique à Snowden qui reste coincé à Moscou.

B- Le système d'écoute de la NSA :

Le 11-09-2001 : un choc dans l'opinion publique états-unienne qui découvre l'Islamisme, le terrorisme et des infiltrations possibles aux États-Unis (l'écoute des tél. portables aurait permise de neutraliser les terroristes qui ont communiqué avant et pendant les attentats par tél. portable) => vote du **Patriot Act** fin 2001 qui autorise l'écoute sans demande d'un juge (ce qui est contraire à la Constitution des États-Unis) et la collecte de données dans les datacenters des GAFAM même si ces datacenters sont localisés à l'étranger.

En 2001, la **NSA** (Agence nationale de sécurité créée au début de la Guerre Froide en 1947) obtient un bâtiment de 100 000 m² pour stocker 2 000 fois le trafic annuel mondial du Net. Elle va utiliser le Patriot Act pour renforcer 3 programmes d'écoute anciens, apparus au début de la Guerre Froide : **PRISM**, **MUSCULAR**, **FIVE EYES**

- PRISM : écoute des citoyens US ; la NSA se donne le droit d'envoyer une NSL ou « lettre de sécurité nationale » aux GAFAM pour avoir les « fadettes » de citoyens américains, ou pour les écouter, ou pour lire leurs mails. Le ciblage est du hasard et le taux de réussite des écoutes est de 1 %.
- MUSCULAR : écoute des citoyens du monde ; un sous-marin nucléaire US est équipé pour pouvoir se brancher sur le réseau de câbles Internet sous-marin et écouter les flux.
- Les Five EYES : 4 pays alliés (Royaume-Uni et ses anciennes colonies : l'Australie, la Nouvelle-Zélande et le Canada) des États-Unis + la France et la Suède (façade occidentale de l'Europe) acceptent de capter gratuitement pour les États-Unis le trafic Internet entrant dans le pays par les câbles et de le transmettre à la NSA pour que cette agence de renseignement surveille le monde entier.

Qui a été écouté ? L'essentiel est constitué de citoyens quasi-anonymes. Mais, en 2013, on apprend que 35 chefs d'État ont été surveillé dont Angela Merkel et Nicolas Sarkozy...

C- La protection limitée des lanceurs d'alerte par la loi : 4p247

Aux États-Unis (2010, 2012) comme en France (2013, 2016 et 2022) la loi a été modifié pour protéger les lanceurs d'alerte mais ces lois ont des limites importantes.

1- Le lanceur d'alerte est autorisé à dénoncer des faits graves (fraude, atteinte aux personnes, violences… y compris psychologiques) pour protéger l'environnement ou la santé publique car les premières alertes sont dans ces domaines. Ex : Erin Brockovitch (1993) face à la compagnie de gaz du Pacifique et la pollution des eaux au chrome ou le docteur Irène Frachon qui a dénoncé les effets du médiator[1] (2011) ou la corruption et des fraudes fiscales (depuis l'affaire J. Cahuzac qui avait fraudé le fisc et menti à l'Assemblée nationale). La loi américaine va + loin que la loi française pour donner suite au scandale Madoff : un employé de la finance qui dénoncerait des malversations de son employeur peut toucher de l'État fédéral 30 % des futures amendes collectées.

2- Une fois que le lanceur d'alerte a fait ses révélations, il est protégé par la loi car il devient **irresponsable pénalement**, c'est-à-dire qu'il ne peut être accusé et condamné, à condition que ses révélations ne relèvent pas de la **diffamation** ou de délation erronée : dans la loi française, un lanceur d'alerte condamné pour diffamation doit payer une amende de 45 000 euros ! Donc, les lanceurs d'alerte ont souvent des procès car les coupables les attaquent pour prouver qu'il s'agit d'une dénonciation calomnieuse.

3- Le lanceur d'alerte ne peut subir des pressions ou de **représailles** de la part de ses employeurs. Ex : une baisse de salaire, un refus de promotion ou de prime, une mise au placard, un renvoi, un non-renouvellement d'un CDD, une orientation ou enfermement en asile…

4- Si le lanceur d'alerte est bien protégé dans son milieu professionnel : le lanceur d'alerte ne peut briser le **secret défense** (donc il ne peut être un espion), le **secret médical** (donc il ne peut être un médecin), le **secret judiciaire** (un avocat, un juré). Dans l'administration, une clause spéciale encourage peu à devenir un lanceur d'alerte : le **devoir de réserve**. Seule la loi étatsunienne donne le droit à un fonctionnaire (mais pas à un haut-fonctionnaire) d'être un lanceur d'alerte : mais sans aucune protection prévue.

---

1 Médicament commercialisé pour lutter contre le diabète alors qu'il s'agissait d'amphétamine (faisant maigrir) ; or, à long terme, ce médicament détruisait le cœur.

II) Une information plus fiable ?

A) Une information horizontale :
Les **réseaux sociaux** suppriment la distinction traditionnelle entre émetteurs (journalistes professionnels triant et vérifiant l'info avant de la diffuser pour avoir une info de qualité) et récepteurs (chaque citoyen qui reçoit l'info sélectionnée) => chaque cybercitoyen peut s'improviser « pseudo-journaliste ». Cela crée des dangers (pour nos démocraties) à la réception et à l'émission :

1- À la réception : algorithmes et bulles de filtres
Comme récepteur, quand on est sur Internet, on a accès à une offre culturelle quasi-illimitée, car, comme émetteur, on produit chacun tous les jours bcp d'info => autant de données produites en 2 ans que depuis l'apparition de l'Homme ! Donc, comment trier l'info ? Le choix n'est-il pas trop vaste ? Comment sélectionner ce qu'il faut consulter ou pas ?
a) Les algorithmes :
Pour filtrer/sélectionner l'info, les firmes (**GAFAM**) du net ont recours à des **algorithmes** gérés par une **intelligence artificielle**. Quand on fait une demande sur Google, c'est cet algorithme qui choisit la réponse. Autrement dit : c'est un programme informatique qui construit les réponses et donc notre savoir !
D'où l'importance de savoir de quoi dépendent les réponses proposées par cet algorithme ? Dans quelle mesure ces réponses (sélectionnées par l'intelligence artificielle) sont-elles des menaces (ou pas) pour nous ou la démocratie ?
b) Les bulles de filtres :
Les réponses proposées dépendent de nos idées politiques et de ce que l'on aime déjà : les algorithmes nous enferment dans une bulle relative à nos recherches précédentes. Sur Google, la réponse est dictée par les **bulles de filtres** qui analysent **57 critères** avant de donner une réponse, comme notre géolocalisation récente, notre âge, notre sexe, nos idées politiques, nos recherches précédentes **5p245** => cela entraîne un conformisme politico-culturel, une « **bulle cognitive** » qui favorise l'égocentrisme, l'absence d'ouverture culturelle, politique et de pluralisme => ces algorithmes sont bien une menace pour la démocratie. Google nous propose ce que l'on connaît déjà => Google ne nous rend pas intelligent !

2- À l'émission : théories du complot et tentative de coup d'État
a) Des théories du complot…
Chaque citoyen peut dire tout et n'importe quoi sur le Net => on trouve sur le net les fameuses **théories du complot** (qui ont fleuri avec le Covid 19
Ex : l'hydroxy chloroquine serait la solution miracle, essor des antivaccins en France : le Covid 19 serait un virus créé par la Chine pour vendre des vaccins dans le monde... Or, c'est plus long de démonter une théorie du complot que d'en diffuser une (quasiment en un clic).
b) … au coup d'État :
Ces « épidémies de crédulité » ont connu un apogée le 6 janvier 2021 (le jour de l'officialisation des résultats de l'élection présidentielle de 2020) avec la **prise du capitole** demandée par Trump sur **Twitter** sous le faux prétexte du « trucage du résultat des élections ». Ce réseau social (sans le vouloir) a failli renverser la démocratie étatsunienne (la 2e plus vieille démocratie du monde moderne). Le compte Twitter de Trump a aussitôt été bloqué. Ce dernier s'est alors exprimé sur une application cryptée du « Dark Web », telegram.

B) La propriété des données fabriquées sur les réseaux sociaux :
Normalement, ces données sont privées, mais elles sont vendues très cher par les firmes du Net comme Facebook à d'autres firmes => nous travaillons gratuitement sans le savoir à enrichir des firmes privées étrangères !

- Nos données sont collectées gratuitement par Facebook mais elles se transforment en produits vendus. Facebook vend 24 h de données 500 000 dollars à des entreprises de pub qui, en échange, connaissent nos goûts et nous proposent des achats en nous envoyant de la pub sur le net. On travaille donc gratuitement pour Facebook sans le savoir.
- La protection par les normes : l'Union européenne a voté en **2016** la **loi RGPD** : règlement général sur la protection des données) qui est entrée en application en 2018. Elle (re)donne la propriété de leurs données aux utilisateurs et empêche (en théorie) la surveillance ; chaque utilisateur de réseau social peut désormais :
    - Porter plainte si on vole ses données ;
    - Demander la suppression gratuite de ses données personnelles (ex : la famille après la mort d'une personne).

- Le **cloud souverain** : il s'agit, pour la Russie, de relocaliser les datacenters en construisant des « **territoires disques durs** » dans des régions froides comme la Sibérie : construction de grands datacenters capables de stocker les données nationales (en Sibérie, là où le refroidissement des datacenters coûte moins cher). **Loi russe de 2016** impose le stockage des données des citoyens russes dans des datacenters russes obligatoirement localisés en Russie.