

Durée : 2 heures / 6 à 12 participants

Objectifs :

- Identifier les principales manipulations en ligne
- Découvrir et comprendre les mécanismes de la manipulation de l'information
- Acquérir les bons réflexes pour se protéger de la désinformation en ligne

Programme :

- 1) Définition et prise de parole
- 2) Cas pratiques
- 3) Les différents types de désinformation
- 4) Les bonnes pratiques
- 5) Apports et ressources pour aller plus loin

1. Introduction : 10 min

→ Cadrage et définition :

La **désinformation** est la diffusion **volontaire et intentionnelle** de fausses informations, avec pour objectif de tromper, manipuler l'opinion publique, semer la confusion ou nuire à une personne, un groupe ou une institution. Contrairement à une simple erreur ou rumeur, elle repose sur une **intention claire de manipulation**, souvent orchestrée à des fins politiques, économiques ou de réputation.

→ Augmentation des actions de désinformation en période préélectorale

→ Consigne : Cet atelier s'appuiera sur des exemples politiques mais n'est pas un espace de partage d'opinions.

2. Tour de table sur l'expérience des participants : 10 – 20 min

Avez-vous déjà entendu parler ou observer de la désinformation en ligne ? (Internet, réseaux sociaux...) ?

3. ACTIVITE 1 : Identifier les cas de désinformation en période pré-électorale : 20 – 45 min

CONSIGNE : En binôme/groupe et sur la base du(des) dossier(s) qui vous a été remis, résumez aux autres participants les documents qui vous seront donnés »

Dossier 1 :

- Article « Dans les Landes, une vidéo très gênante générée par IA circule sur la maire de Soustons »
- Article « Des personnalités politiques de Guéret victimes d'images malveillantes générées par IA »
- Vidéo « Coup d'Etat en France »

Dossier 2 :

- Article « La Seine en bleu »
- Vidéo « Blue pond dye treatment »

Dossier 3 :

- Article «Affaire Epstein : de fausses informations circulent sur les liens entre Emmanuel Macron et le pédocriminel »
- Post sur X de France Soir

Dossier 4 :

- Article « Zuckerberg et les actionnaires de Meta s'accordent pour éviter un procès »
- Article « Le scandale Cambridge Analytica : un tournant décisif pour la protection des données et la responsabilité des entreprises »
- Vidéo « L'affaire Cambridge Analytica... on t'explique ! »

Dossier 5 :

- Article « Ce réseau de profils contestataires, très populaires sur le X français, émane-t-il d'une usine à trolls russe ? »
- Post « #désinformation#bots#trolls#manipulation#réseauxsociaux »
- Vidéo « Les fermes à trolls »

Dossier 6 :

- Article « Présidentielle en Roumanie : des ONG demandent une enquête sur l'influence de TikTok dans la campagne »
- Vidéo Election Roumanie

➔ Restitution de chaque groupe et échanges : 45 – 60 min

Pause : 60 – 65 min

4. ACTIVITE 2 : 65 – 80 min – Connaître les différentes méthodes de désinformation

Catégoriser les différents modes opératoires de la désinformation de façon collective

➔ Des cartes comportant un type de désinformation sont placées au centre de la table. Chaque binôme/groupe doit sélectionner celle qui correspond à leurs documents.

- Carte 1 : Deep fake / IA
- Carte 2 : Décontextualisation d'images et de vidéos
- Carte 3 : Usurpation d'identité de médias (typosquatting)
- Carte 4 : Recours dissimulé à des influenceurs
- Carte 5 : Exploitation illégale des données personnelles
- Carte 6 : Recours à des comptes inauthentiques (bots, trolls)
-

5. ACTIVITE 3 : 80 – 95 min : Identifier des parades

Pour chaque type de désinformation, phase de réflexion en groupe pour aller chercher des solutions pour s'en prémunir ou vérifier l'information → post-it solutions à placer dans des bulles type de désinformations.

CONSIGNE : « Trouvez des solutions, des idées qui vous permettent de contrer ce type de désinformation. »

Restitution : 95 – 110 min

Type de désinformation / Mode opératoire et tactiques de déstabilisation	Solutions / vérifications
Deepfake → IA	- Développer son esprit critique - vérifier et croiser les sources - Chercher les anomalies (défauts, mouvements non naturels)
Image décontextualisée	- Google Lens ou TinEye pour retrouver la source, vérifier la date et le lieu
Typosquatting et usurpation d'identité de médias connus	- Vérification URL - Recherche manuelle en ligne
Recours dissimulé à des influenceurs	- Vérifier le profil de l'influenceur (ses thématiques habituelles) - Vigilance face aux intérêts politiques soudains et inexpliqués
Exploitation des données persos des RS à usage politique (Ex. de Cambridge Analytica)	- Multiplier les sources d'information (RS, radio, télé, presse) - Renforcer la protection de sa vie privée en ligne et les paramètres de confidentialité
Recours à des comptes inauthentiques (bots, trolls)	-Vérifier la date de création du compte -Comportement répétitif et automatisé

6. Partages de ressources et échanges : 110 – 120 min

Viginum : Service technique et opérationnel de l'Etat chargé de la vigilance et de protection contre les ingérences numériques étrangères

<https://www.sgdsn.gouv.fr/publications/protection-du-debat-public-numerique-en-contexte-electoral-publication-dun-guide-de>

L'AFP : <https://factuel.afp.com/>

Le Monde : <https://www.lemonde.fr/verification/>

France 24 : <https://observers.france24.com/fr/guide-de-verification>

France Info : <https://www.franceinfo.fr/vrai-ou-fake/>