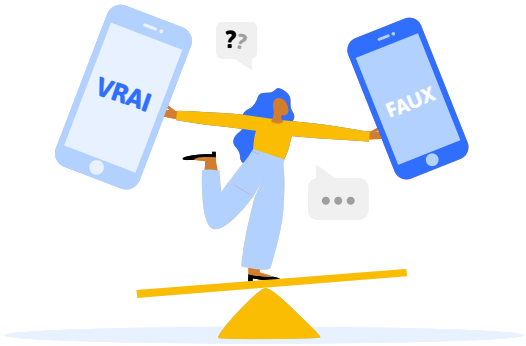
Fiche thématique

LA DÉSINFORMATION

Distinguer le vrai du faux à l'ère numérique



Avant-propos

La désinformation est un phénomène aux multiples visages : elle se présente sous forme d'article d'actualité, de publication d'utilisateur, de courriel, d'image ou encore de *deepfake*, c'est-à-dire de vidéos manipulées. Toute personne qui utilise les médias et les réseaux sociaux y est régulièrement confrontée. Ces informations trompeuses ont surtout des conséquences politiques du fait de leurs répercussions sur les processus démocratiques, mais elles peuvent aussi avoir un impact social négatif ou mettre notre santé en péril.

De nos jours, la désinformation peut se propager plus rapidement que jamais. Les réseaux sociaux et les messageries permettent un partage à grande échelle de fausses informations souvent automatisées et soutenues par intelligence artificielle (IA), si bien qu'elles semblent étonnamment authentiques.

Mais comment distinguer le vrai du faux ? Comment lutter contre le fléau de la désinformation ? Compte tenu de l'ampleur croissante du phénomène et des avancées constantes facilitant la production et la propagation de la désinformation, des instances gouvernementales, des instituts de recherche et même l'Union européenne (UE) se sont déjà attaqués à ce problème depuis plusieurs années. De nombreuses campagnes visent à informer et sensibiliser la population.

En tant qu'utilisateurs, nous disposons aussi de moyens de nous protéger des informations trompeuses sur Internet. Dans cette publication, BEE SECURE présentera ces possibilités et répondra aux questions liées à la désinformation.

Sommaire

1. Qu'est-ce que la désinformation ?

L'accès illimité à une multitude d'informations nous permet de former notre propre opinion, notamment sur des questions politiques. Il s'agit là d'une condition importante pour pouvoir participer activement aux débats publics et exprimer notre volonté dans des processus démocratiques libres et justes. La désinformation est diffusée de manière ciblée afin d'influencer les opinions au sein de la société, par exemple en renforçant des préjugés, des conflits ou des peurs.

Ce phénomène s'est manifesté clairement lors de l'élection présidentielle américaine et du référendum sur le Brexit en 2016. La diffusion délibérée de désinformation sur les médias sociaux a été identifiée rétrospectivement comme un facteur clé ayant influencé les résultats des élections et du référendum. Le terme « fake news », utilisé pour désigner les informations mensongères propagées à des fins politiques ou financières, s'est rapidement popularisé. Toutefois, les fausses informations qui n'ont pas cette visée sont désormais aussi qualifiées de *fake news*. Du fait de son instrumentalisation politique, par exemple lorsqu'un acteur politique qualifie publiquement une opinion contraire de *fake news*, ce terme est en outre associé au combat politique. Malgré un usage moins répandu, il en va de même pour son synonyme *hoax* (canular).

Un groupe d'experts de l'UE a formulé une définition claire du terme « désinformation », qui est également utilisé dans le langage technique.

La « désinformation » désigne « les informations dont on peut vérifier qu'elles sont fausses ou trompeuses, qui sont créées, présentées et diffusées dans un but lucratif ou dans l'intention délibérée de tromper le public et sont susceptibles de causer un préjudice public[1] ».

La désinformation est donc **partagée délibérément, dans le but de nuire, à des personnes, des organisations, des groupes sociaux ou des pays**.

Pour définir la désinformation, il est important de faire la **distinction entre les faits et les opinions**. La désinformation repose toujours sur des allégations de faits, et non pas sur des prises de position subjectives ou des jugements. Il est donc possible de vérifier qu'elles sont fausses. À contrario, les opinions sont personnelles et variées, et doivent pouvoir être exprimées librement dans une démocratie. Elles peuvent être basées sur de fausses informations, mais elles ne peuvent pas être considérées comme « fausses » en tant que telles et ne sont pas vérifiables.

Voici un exemple :

Fausse allégation de fait : « Voter aux élections européennes est un délit, comme le montre un arrêt de la Cour constitutionnelle allemande. »

Opinion : « Voter aux élections européennes devrait être considéré comme un délit. »

Opinion basée sur de faux faits : « Je pense que c'est une bonne chose que le vote aux élections européennes soit un délit. »

Désinformation ou mésinformation ?

La **désinformation repose toujours sur des faits inexacts** et cache une intention (malveillante) visant un objectif précis.
Elle se **distingue de la mésinformation, qui est partagée sans intention de tromper**. Il peut s'agir par exemple de contenus satiriques ou de fausses informations diffusées par négligence.

2. Pourquoi la désinformation est-elle propagée ?

Pour comprendre les motivations qui poussent à partager de la désinformation, il est essentiel d'examiner de plus près les acteurs en jeu. Il y a eu dans le passé des campagnes de désinformation soutenues par des gouvernements, comme le signale le rapport de 2017 du *Conseil de l'Europe*. Cependant, de nombreux acteurs non gouvernementaux pratiquent également la désinformation, dont des groupes ou des communautés d'intérêts qui soutiennent des causes spécifiques.

Il peut s'agir aussi bien de personnes opérant à titre individuel que de groupes organisés. Différentes personnes, voire des **technologies automatisées** (*des bots*) peuvent intervenir dans chacun des processus de conception, de production et de diffusion.

[1] Commission européenne. Plan d'action contre la désinformation, p. 1
www.eeas.europa.eu/sites/default/files/plan_daction_contre_la_desinformation.pdf

Le *Conseil de l'Europe* a identifié quatre facteurs principaux qui motivent la propagation de la désinformation : les facteurs financier, politique, social et psychologique. Le **facteur social** implique la volonté de partager de la désinformation afin de se constituer un réseau. Le **facteur psychologique** relève de l'objectif d'attirer l'attention ou d'obtenir l'approbation d'autres personnes. Les facteurs **financier** et **politique** sont les motifs les plus fréquents de la désinformation. Il est intéressant d'approfondir leur analyse.

Motivation financière

Sur Internet, les clics rapportent souvent de l'argent. Cela tient au fait que les exploitants de sites Web génèrent des revenus avec la publicité diffusée sur le site. Plus il y a de visiteurs sur un site Web (*traffic*), plus il est intéressant pour les annonces publicitaires et plus il permet de générer des recettes. Pour qu'un site Web attire un grand nombre d'internautes, des titres accrocheurs sont souvent utilisés pour capter leur attention (*clickbaiting* ou piège à clics), comme le fait cet article en allemand : « *Jeder der Wählen geht leistet Beihilfe zu einer Straftat!* » (« *Toute personne qui va voter se rend complice d'un délit !* »). Les informations que l'on trouve dans ce type de publications reflètent rarement la réalité. Aujourd'hui, il existe de faux sites Web d'informations et d'actualités entièrement générés par IA. En revanche, derrière des contenus créés par des humains peuvent se cacher des « fermes à trolls », où des employés rédigent ces annonces en échange d'une faible rémunération. De tels sites Web sont souvent relayés par les réseaux sociaux et leur diffusion peut se faire de manière autonome et incontrôlée par des utilisateurs (inconscients de leurs actes). Le partage de la désinformation constitue donc une activité peu coûteuse et lucrative.

Motivation politique

La désinformation en rapport avec les sujets politiques vise généralement à influencer l'opinion publique. Elle peut avoir des conséquences sur des élections et donc aussi sur les rapports de force politiques.

Dans le cadre des élections européennes de 2024, des tentatives de convaincre un public cible de suivre les orientations politiques d'un parti à l'aide de *deepfakes* publiés sur les réseaux sociaux ont été observées en France. Les vidéos diffusées n'étaient pas authentiques, même si elles en avaient l'air. Il s'agissait de *deepfakes* dans lesquels les visages des personnes apparaissant dans la vidéo d'origine avaient été remplacés (*face swap*) par ceux d'une femme politique et de sa nièce. Cela donnait l'impression que ces personnes faisaient la promotion d'un parti ou d'une orientation politique, en l'occurrence du *Rassemblement National* (RN). Ces vidéos, conçues de manière attrayante, visaient à accroître la sympathie des jeunes électeurs pour le parti du RN. Il est probable que des groupes d'intérêts politiques de droite étaient à l'origine de la création et de la diffusion de cette désinformation. BEE SECURE a également publié une contribution à propos de la désinformation dans ce contexte.

3. Où et comment la désinformation est-elle partagée ?

Aujourd'hui, les médias sociaux et les services de messagerie font partie du quotidien de la majeure partie de la population. Nombreux sont ceux qui s'y informent chaque jour de l'actualité et d'autres sujets d'intérêt. Ces plateformes offrent ainsi un **moyen simple et peu coûteux de propager de la désinformation très rapidement à un grand nombre de personnes**.

Par rapport aux médias classiques tels que la presse et la radio, la structure émetteur-récepteur est complètement différente sur les réseaux sociaux. **Chaque utilisateur peut endosser les deux rôles : il peut se contenter de lire des informations (récepteur), mais il peut aussi créer, publier et partager lui-même des contenus (émetteur)**. Par ailleurs, ces contenus ne sont généralement pas vérifiés avant leur publication.

Chacun peut ainsi contribuer sciemment ou non à la propagation de la désinformation.

Reprenons l'exemple de la vidéo *deepfake* de la femme politique et de sa nièce pour illustrer le parcours de la propagation. Le militant d'un parti crée la vidéo avec un outil d'échange de visages et la publie sur un faux profil *TikTok* (producteur et émetteur) afin de conférer une image attractive au parti et de motiver les jeunes électeurs à voter pour lui. Les utilisateurs qui visionnent la vidéo (récepteurs) la partagent, par exemple sur *Facebook* ou des messageries comme *Telegram* (émetteurs), soit pour soutenir la cause, soit pour montrer leur désaccord à leurs *followers* (les personnes abonnées à leur compte). Dans les deux cas, le producteur de la vidéo a obtenu ce qu'il voulait : la vidéo et la désinformation se répandent.

La propagation est par ailleurs influencée par des algorithmes personnalisés.

Algorithmes et bulles de filtres

Sur les réseaux sociaux, chacun a sa « propre vision du monde ». Les articles qui vous sont proposés dépendent d'un **algorithme de personnalisation**. Cet algorithme **collecte des informations sur vos recherches Internet**, sur les contenus que vous avez regardés, aimés et écrits ainsi que sur les articles que vous avez achetés. Il est donc en mesure de **vous présenter essentiellement des contenus qui correspondent à vos préférences et à vos points de vue**. Vous êtes pris dans une « bulle de filtres » (*filter bubble*), dans laquelle les autres contenus peuvent difficilement entrer.

Le problème dans cette situation réside dans le fait que les sujets sont souvent abordés sous un seul angle et que cette vision partiale est renforcée, notamment quand on lit plusieurs fois la même information (« effet de vérité illusoire » ou *truth effect*). Les fausses informations sont plus faciles à croire lorsqu'elles correspondent à notre propre vision du monde et qu'elles concordent avec nos opinions (« biais de confirmation »). Les producteurs de désinformation savent comment exploiter les algorithmes et essayent, grâce à des mots clés spécifiques, de pénétrer dans des « bulles » récurrentes.

La désinformation sur Internet se propage grâce au partage des utilisateurs sur les réseaux sociaux. En revanche, elle peut aussi être relayée manuellement par des utilisateurs et des fermes à trolls ou être diffusée à l'aide de technologies (semi)/automatisées.

Des **robots sociaux** (*social bots*) sont utilisés à cette fin. Ils interagissent par l'intermédiaire de faux profils sur les réseaux sociaux qui ont l'air authentiques et se comportent comme de vraies personnes, mais sont contrôlés par un programme. Ils peuvent publier, aimer et commenter des contenus. Ils s'appuient souvent sur des modèles de langage assistés par IA (algorithmes capables de traiter, « comprendre » et générer du texte), ce qui leur permet de produire des réponses plus variées et plus naturelles.

Ces modèles d'IA apprennent, en outre, à partir d'articles publiés sur les canaux publics des réseaux sociaux qui expriment une opinion ou traitent d'un sujet donné, à reproduire ces opinions dans les textes qu'ils génèrent. Ils sont notamment employés en marketing afin d'établir un dialogue avec des clients (potentiels) et de promouvoir certaines offres. Mais ils peuvent également être utilisés en politique afin d'influencer l'opinion publique, ce qui les rend dangereux. Ils peuvent par exemple générer une grande quantité de déclarations en soutien à un parti politique et dénigrer le parti adverse.

Comment reconnaître un robot social ?

La plupart du temps, on identifie un robot social grâce au **nombre élevé de publications que le compte produit en peu de temps**, l'objectif étant de générer un maximum d'informations pertinentes en un minimum de temps. Lorsque l'on communique directement avec un robot, il **répond généralement en quelques secondes. Il échoue souvent quand on lui pose des questions qui sortent de son sujet de prédilection**. Contrairement aux comptes authentiques, **un compte contrôlé par un robot social n'affiche jamais de coche bleue sur le profil**. Sur de nombreux réseaux sociaux, cette coche indique que le compte a été vérifié et authentifié. **Le profil vaut également la peine d'être examiné**. Les profils des robots sociaux **ne contiennent généralement que des informations très générales ou n'affichent aucune information**, avec un pseudonyme parfois composé d'une suite de lettres et de chiffres aléatoires, sans photo ou avec une photo générique.

La même technologie peut être employée pour créer de faux sites Web d'actualités. Dans ce cas, le modèle d'IA génère des articles d'information plutôt que des contributions (***content farming*** ou « fermes de contenus »). L'objectif premier est le plus souvent de nature financière, ces pages contiennent donc beaucoup de publicité. On peut souvent les démasquer par l'absence de références aux auteurs et de mentions sur les droits d'auteur. En outre, les contenus peuvent paraître invraisemblables et aller à l'encontre des connaissances généralement admises.

4. Quels sont les dangers de la désinformation ?

La désinformation peut vous affecter personnellement tout autant que la société dans son ensemble. En effet, elle peut s'immiscer dans la vie politique ou des processus démocratiques comme les élections, mais elle peut aussi avoir des effets sur la sécurité et l'environnement. Elle peut même compromettre notre santé.

Voici l'impact qu'elle peut avoir concrètement :

- **Démocratie :** Une information au sujet d'une décision de justice concernant les élections européennes de 2024, « *Jeder der Wählen geht leistet Beihilfe zu einer Straftat!* » (« Toute personne qui va voter se rend complice d'un délit ! »), devait créer un effet de défiance vis-à-vis de la politique. La vidéo *deepfake* déjà évoquée au chapitre 2 a été utilisée pour rallier des électeurs pour un parti populiste de droite. Le référendum sur le Brexit ainsi que l'élection présidentielle américaine de 2016 ont été clairement influencés par des campagnes de désinformation d'origine gouvernementale.
- **Sécurité :** Avant la guerre en Ukraine, le Kremlin a mené une campagne de désinformation russe bien orchestrée pendant plusieurs années. Une campagne de désinformation ciblée a été diffusée dans les deux pays dans le but d'affaiblir et de déstabiliser l'Ukraine, et de la présenter comme un ennemi pour légitimer son agression.
- **Santé :** Pendant la pandémie de COVID-19, une multitude de publications sur les réseaux sociaux ont alimenté l'incertitude sur le traitement de la maladie, la sécurité et l'efficacité des vaccins, l'utilité de la distanciation sociale, etc. Cette situation a entraîné des protestations et des troubles dans la société. De nombreuses personnes ont en outre vécu des conflits personnels et ont été exclues de leur environnement social et professionnel. Les vaccins n'ont pas été acceptés aussi rapidement qu'il l'aurait fallu. Dans certains cas, le nombre de décès a même augmenté. Les « guides des champignons » vendus sur Amazon constituent un autre exemple plus récent. Ils ont été générés par IA et l'exactitude des informations n'a pas été vérifiée. Les champignons comestibles ressemblent souvent à s'y méprendre aux champignons vénéneux. Toute erreur, même minime, comme l'IA est susceptible d'en faire, peut alors présenter un risque mortel.
- **Dans la sphère personnelle**, la désinformation peut également causer d'importants préjudices quand elle est utilisée à des fins de harcèlement et de chantage. Par exemple, le *deepfake porn* et les applications d'échange de visages permettent de créer des contenus pornographiques avec les visages des victimes dans le but de les exploiter de manière malveillante.

La désinformation a trait à **des dangers en ligne qui peuvent avoir des conséquences fatales dans le monde réel**.

Le rapport BEE SECURE Radar 2024 suggère que la désinformation fait partie des dangers les plus fréquemment observés en ligne :

- La désinformation et les fausses nouvelles ont été citées comme le risque en ligne le plus préoccupant par 50 % des 129 jeunes de 17 à 30 ans interrogés.
- Parmi les 283 parents d'adolescents de 12 à 16 ans interrogés, 42 % les ont placées en deuxième position.
- 25 % des 217 parents d'enfants de 3 à 11 ans interrogés ont considéré le risque comme plus faible.

5. La lutte contre la désinformation

Pour faire face à la menace croissante que représente la désinformation, les gouvernements et les organisations du monde entier prennent des mesures pour protéger la population et les acteurs politiques. À cet égard, la mise en place d'une coopération transfrontalière est importante afin d'échanger des informations et d'élaborer des stratégies communes.

- **Renforcer la coopération**
  L'*Union européenne* a mis sur pied plusieurs initiatives, dont le plan d'action contre la désinformation 2018 et le plan d'action pour la démocratie européenne 2020. Ces deux plans renforcent la coopération et la transparence au sein de l'UE. Depuis 2019, les institutions européennes et les États membres de l'UE partagent des informations et signalent d'éventuelles anomalies via un « système d'alerte précoce ». En signant la déclaration mondiale sur l'intégrité de l'information en ligne, plus de trente pays du monde entier se sont unis pour lutter contre la désinformation en adoptant différentes stratégies.
- **Mieux reconnaître et analyser la désinformation**
  Un budget plus important sera investi dans la vérification des données et des faits, la recherche et la formation du personnel. L'*Observatoire européen des médias numériques* (*European Digital Media Observatory*, *EDMO*), une entité indépendante, soutient les vérificateurs de faits et les chercheurs en désinformation. Il surveille également la mise en oeuvre des stratégies de lutte contre la désinformation. Le groupe de travail *East Stratcom* du Service européen pour l'action extérieure, dont la fonction est de détecter et déjouer les campagnes de désinformation russes dans le cadre du projet EUvsDisinfo, constitue un autre exemple dans ce domaine.
- **Réglementer et contrôler les géants du marché numérique**
  En 2018, l'Union européenne a instauré le Code de bonnes pratiques contre la désinformation, puis l'a renforcé en 2022. De nombreuses grandes entreprises telles que *Google*, *Microsoft*, *Meta* et *TikTok* se sont engagées (de leur propre gré) à le respecter. Elles garantissent ainsi une plus grande transparence et s'engagent à lutter activement contre les contenus illégaux et la désinformation. Les infractions sont contrôlées et sanctionnées par la *Commission européenne*.
- **Supprimer plus facilement les contenus illégaux et mieux identifier la publicité**
  Depuis 2024, la « législation sur les services numériques » (*Digital Services Act*, DSA) entrée en vigueur en 2022 est pleinement applicable. Elle vise à rendre plus sûr l'ensemble de l'espace numérique de l'UE, tout en garantissant les droits fondamentaux des utilisateurs, tels que la liberté d'expression. Tous les services numériques qui proposent des biens, des services ou des contenus aux consommateurs, même s'ils sont situés en dehors de l'UE, sont concernés. Cela inclut les plateformes de médias sociaux, mais aussi les services d'hébergement et les marchés en ligne. Les services numériques doivent désormais s'attaquer plus rapidement aux contenus illégaux et abusifs, tels que les robots sociaux ou les discours haineux (*hate speech*), et continuer à gagner en transparence.
- **Fournir des informations plus fiables et renforcer la communication sur la désinformation**
  Les médias indépendants et les vérificateurs de faits reçoivent davantage de soutien, par exemple, de la part du Réseau européen des normes de vérification des faits (EFCNS, *European Fact-Checking Standards Network*), qui est constitué de plusieurs organisations européennes de vérificateurs de faits. Il définit des normes de vérification des faits (*fact checking*), forme les vérificateurs de faits et met en lumière des cas concrets de désinformation sur des sujets spécifiques comme la crise climatique et les élections européennes de 2024.

- **Sensibiliser la société et la rendre plus résistante à la désinformation**

  En Europe et dans le monde, les citoyens sont sensibilisés aux risques et apprennent à reconnaître et à combattre la désinformation. Pour ce faire, il existe de nombreuses campagnes qui s'adressent aux enfants dès leur plus jeune âge. Avec l'initiative pour un Internet meilleur pour les enfants (*Better Internet for Kids*, BIK), menée en coopération avec le réseau de centres pour un Internet plus sûr dans les États membres cofinancé par l'UE (dont BEE SECURE est le représentant pour le Luxembourg), l'*Union européenne* vise à rendre les plateformes en ligne plus sûres pour les enfants et, en parallèle, à éduquer les enfants aux médias. Elle fournit des ressources aux enfants, aux parents, aux enseignants, ainsi qu'au secteur de la recherche et à l'industrie.

  Le plan d'action en matière d'éducation numérique (2021–2027) de l'UE s'adresse à tous les groupes cibles. Il définit les actions qui permettront d'améliorer l'éducation aux médias des citoyens de l'UE, que ce soit dans un cadre scolaire ou à travers des ateliers numériques gratuits (p. ex. via le pôle européen d'éducation numérique).

  Au Luxembourg, BEE SECURE sensibilise le grand public à une utilisation plus sûre et responsable des technologies numériques. Des offres et activités diverses, spécialement conçues pour les enfants, les jeunes et leur entourage (parents, enseignants, éducateurs, etc.), sont proposées sur l'utilisation sûre d'Internet. Les formations de sensibilisation en sont l'élément central. À l'instar des multiples publications, les formations couvrent un large éventail de sujets. En outre, l'initiative organise régulièrement des campagnes et des événements thématiques.

  Dans le cadre de ces démarches, le sujet de la désinformation est régulièrement mis en lumière, notamment en collaboration avec des partenaires tels que la fondation *Zentrum fir politesch Bildung*, l'*ALIA* et *EDMO Belux*. De plus, la formation aux médias fait déjà partie intégrante des « sciences numériques » dans le programme scolaire.

6. Que puis-je faire contre la désinformation ?

La désinformation peut se présenter sous différentes formes, qu'il s'agisse de texte, d'images, de vidéos ou de fichiers audio. Elle est omniprésente sur Internet, que ce soit dans les publications sur les réseaux sociaux, dans les messages électroniques de votre boîte de réception, dans les *reels* (courtes vidéos) sur *Instagram* ou encore dans les informations sur *WhatsApp*. Mais vous n'êtes pas sans défense. Des protections existent !

Pour vous prémunir, une méthode reconnue est le ***pré-bunking*** : plus vous en saurez en amont sur la désinformation et les stratégies qu'elle emploie, plus vite vous la démasquerez.

Pré-bunking

Le ***pré-bunking*** vise à prévenir la désinformation en en expliquant les mécanismes. Il est souvent difficile, notamment dans un contexte politique, de contrer une désinformation après coup à l'aide des méthodes de vérification des faits et de ***debunking*** (rétablissement de la vérité). Les effets de la désinformation se font généralement déjà ressentir dès sa propagation et seule une petite partie des récepteurs peut encore être atteinte pour une rectification des informations véhiculées.

Une campagne de ***pré-bunking*** à l'échelle européenne, organisée par ***Jigsaw***, une filiale de ***Google***, et diverses organisations, informe le public sur les stratégies de manipulation habituelles. Si vous les connaissez, vous pourrez plus facilement les démasquer !

Il convient désormais d'aborder brièvement brièvement **trois mécanismes de désinformation** très répandus. Les campagnes vidéo correspondantes sont accessibles à partir des liens respectifs :

1. **La méthode du bouc émissaire :**

   La méthode du bouc émissaire consiste à tenir à tort une personne ou un groupe pour seul responsable d'un problème. La véracité de telles accusations doit toujours être confirmée.

2. **Décontextualisation :**
   La décontextualisation consiste à utiliser des vidéos et des photos dans un autre contexte ou à utiliser des images générées ou modifiées par IA. Elle se caractérise aussi par l'absence de sources fiables concernant les informations publiées, qui ont souvent surprenantes ou choquantes.
3. **Atteinte à la réputation :**
   L'atteinte à la réputation consiste à faire des déclarations sur des personnes ou des groupes de personnes qui mettent en doute leur intégrité et leur crédibilité. Il n'existe pas de preuves pour les étayer.

Bien entendu, il existe d'autres stratégies de manipulation comme le recours au langage émotionnel, à de faux experts ou à une argumentation incohérente. Une vue d'ensemble simple vous est proposée sur le site Web de la campagne de *pré-bunking*.

Pour les situations pratiques, BEE SECURE a élaboré une **check-list qui vous permettra de confirmer la véracité des informations.** Vous pourrez ainsi vous protéger et empêcher la propagation de la désinformation.

Certes, les premières vérifications peuvent prendre du temps, mais « c'est en forgeant qu'on devient forgeron » ! En vous exerçant, vous gagnerez en rapidité et en assurance et, avec le temps, vous pourrez vous passer de cette liste.

Vous trouverez ci-dessous une version condensée de la check-list, que vous pouvez glisser dans votre poche ou photographier avec votre smartphone. Une version plus détaillée, offrant des informations supplémentaires, est disponible en annexe.

1. **Qui se cache derrière ces informations ?**
   a. Qui est l'auteur ? Inconnu ou non mentionné Mauvais signe !
   b. Qui a partagé l'information ? Cette personne a-t-elle vérifié l'information ?
   c. Le compte ou le site Web sont-ils authentiques ? Étudier les mentions légales, les informations du profil et la logique de publication.
   d. Quelle intention se cache derrière l'information ? Quel est le but poursuivi ?
2. **La source est-elle digne de confiance ?**
   Les chiffres ou les faits sont-ils correctement cités ? L'information est-elle rapportée à d'autres endroits ?
3. **Comment le sujet est-il présenté par les autres auteurs**
   Croisez vos lectures et faites appel aux vérificateurs de faits !
4. **Comment l'information est-elle présentée ?**
   - Les différents éléments (titre, texte et images) concordent-ils avec le contenu ? (Faites une recherche inversée à l'aide des images !)
   - Le texte tend-il à généraliser, est-il partial ou manque-t-il de cohérence ?
     → Alerte !
   - S'agit-il de faits ou d'opinions ?
   - Une réaction émotionnelle forte est-elle visée ?
     → Encore une alerte !
5. **Check yourself !**
   - À quel point êtes-vous pris dans votre bulle de filtre ?

Liens utiles

- EUnVDnDisinfo : https://euvsdisinfo.eu/fr
- Pré-bunking : https://prebunking.withgoogle.com/fr
- EDMO Fact-checking : https://belux.edmo.eu/fact-checking
- Mimikama : https://mimikama.org
- Correktiv : https://correctiv.org
- Politifact : https://politifact.com
- FactCheck : https://factcheck.org
- snopes : https://snopes.com

- Pôle européen d'éducation numérique : education.ec.europa.eu/focus-topics/digital-education/action-plan/european-digital-education-hub

- Test interactif pour la propre bulle de filtre : www.filterbubble.lu

Bibliographie

- **BEE SECURE**. BEE SECURE Radar 2024 www.bee-secure.lu/fr/publication/bee-secure-radar
- **Internet meilleur pour les enfants**. The rising importance of disinformation in media literacy www.betterinternetforkids.eu/practice/articles/article?id=7225534
- **Conseil de l'Europe**. Information disorder: Toward an interdisciplinary framework for research and policy making (2017) https://edoc.coe.int/fr/medias/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html
- **European Union: External Action**. Plan d'action contre la désinformation www.eeas.europa.eu/node/54866_en
- **EUnVDnDisinfo**. https://euvsdisinfo.eu/fr
- **franceinfo**. Réseaux sociaux : l'Europe durcit le ton sur la désinformation www.francetvinfo.fr/internet/reseaux-sociaux/facebook/reseaux-sociaux-l-europe-durcit-le-ton-sur-la-desinformation_6133656.html
- **klicksafe**. Prebunking – So schützt man präventiv gegen Desinformationen www.klicksafe.de/news/prebunking-so-schuetzt-man-praeventiv-gegen-desinformationen
- **Luxemburger Wort**. Ermittlungen gegen Facebook und Instagram www.wort.lu/wirtschaft/ermittlungen-gegen-facebook-und-instagram/12391748.html
- **JIGSAW l Google**. Le pré-bunking est une technique permettant d'éviter les manipulations en ligne https://prebunking.withgoogle.com/fr
- **toute l'europe**. Désinformation : la Commission européenne ouvre une enquête contre le réseau social X (ex-Twitter) www.touteleurope.eu/economie-et-social/desinformation-la-commission-europeenne-ouvre-une-enquete-contre-le-reseau-social-x-ex-twitter
- **Saferinternet.at**. Was ist ein Social Bot? www.saferinternet.at/faq/informationskompetenz/was-ist-ein-social-bot
- **Saferinternet.at**. Wie erkenne ich Social Bots? www.saferinternet.at/faq/informationskompetenz/wie-erkenne-ich-social-bots
- **Saferinternet.at**. Was ist ein Algorithmus und wie entstehen Filterblase? www.saferinternet.at/was-ist-ein-algorithmus-und-wie-enstehen-filterblasen
- **The New York Times**. See How Easily A.I. Chatbots Can Be Taught to Spew Disinformation www.nytimes.com/interactive/2024/05/19/technology/biased-ai-chatbots.html
- **U.S. Department of state**. Building A More Resilient Information Environment www.state.gov/building-a-more-resilient-information-environment
- **bpb**. Fake News, Misinformation, Desinformation www.bpb.de/shop/zeitschriften/izpb/medienkompetenz-355/539986/fake-news-misinformation-desinformation
- **mimikama**. Nein, die Stimmabgabe bei den Europawahlen ist keine Straftat www.mimikama.org/stimmabgabe-eu-wahlen-2024-keine-straftat
- **BEE SECURE**. Élections européennes : manipulation via désinformation et deepfakes www.bee-secure.lu/fr/news/elections-europeennes-manipulation-par-la-desinformation-et-deepfakes

- **SOCIAL MEDIA PSYCHOLOGY**. The psychology of fake news: how disinformation spreads online https://socialmediapsychology.eu/2018/09/20/the-psychology-of-fake-news-how-disinformation-spreads-online
- **Online Lexikon für Psychologie & Pädagogik.** confirmation bias https://lexikon.stangl.eu/10640/confirmation-bias-bestaetigungsfehler-bestaetigungstendenz#google_vignette
- **EuvsDisinfo**. « Contrer les campagnes de désinformation menées actuellement par la Russie » : huit ans d'activités d'EUvsDisinfo https://euvsdisinfo.eu/fr/contrer-les-campagnes-de-desinformation-menees-actuellement-par-la-russie-huit-ans-dactivites-deuvsdisinfo
- **Organisation mondiale de la Santé**. Désinformation et santé publique www.who.int/fr/news-room/questions-and-answers/item/disinformation-and-public-health
- **heise**. „Völlig unverantwortlich" : KI-generierte Pilzratgeber bei Amazon angeboten www.heise.de/news/Voellig-unverantwortlich-KI-generierte-Pilzratgeber-bei-Amazon-angeboten-9293723.html
- **Commission européenne**. Protéger la démocratie https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy_fr
- **European Digital Media Observatory** https://edmo.eu
- **Commission européenne**. Code de bonnes pratiques contre la désinformation 2022 https://digital-strategy.ec.europa.eu/fr/policies/code-practice-disinformation
- **Commission européenne**. Paquet « Législation sur les services numériques » https://digital-strategy.ec.europa.eu/fr/policies/digital-services-act-package
- **EFCSN.** Advancing fact-checking https://efcsn.com/advancing-fact-checking
- **Commission européenne**. Une stratégie européenne pour un Internet meilleur pour les enfants (BIK+) https://digital-strategy.ec.europa.eu/fr/policies/strategy-better-internet-kids
- **Commission européenne**. Plan d'action en matière d'éducation numérique (2021-2027) https://education.ec.europa.eu/fr/focus-topics/digital-education/action-plan
- **Commission européenne**. Tackling Disinformation and Information Manipulation https://ec.europa.eu/commission/presscorner/api/files/attachment/878789/Tackling Disinformation_Factsheet_DE.pdf
- **DW**. Wie erkenne ich KI-generierte Websites? www.dw.com/de/faktencheck-was-sind-ki-generierte-websites-und-wie-erkenne-ich-sie/a-65546851
- **DW**. Faktencheck: Wie man Desinformation vor EU-Wahlen erkennt www.dw.com/de/faktencheck-wie-man-desinformation-im-europawahlkampf-erkennt/a-69008051
- **Le Gouvernement du Grand-Duché de Luxembourg**. digital sciences https://innovative-initiatives.public.lu/initiatives/digital-sciences

Éditeur : Service national de la jeunesse (SNJ)
Service national de la jeunesse - B.P. 707 L-2017 Luxembourg
www.snj.lu | www.bee-secure.lu

Fiche thématique
La désinformation
Distinguer le vrai du faux à l'ère numérique
09.2025
ISBN 978-2-919828-90-6
Ressource électronique

Initié par : LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse

Opéré par : Service national de la jeunesse · KJT.lu

Cofinancé par : Cofinancé par l'Union européenne