

Que faire face aux attaques sur les réseaux sociaux en période électorale ?

Ressources d'autodéfense à destination des associations



**Ce guide recense des ressources à destination des associations, pour leur permettre de répondre aux attaques, abus et difficultés qu'elles peuvent rencontrer sur les réseaux sociaux en période électorale.*

Éléments de compréhension

Le rôle des plateformes dans les attaques et violences en ligne

Si les réseaux sociaux sont constamment des vecteurs et des amplificateurs de violences et de discriminations, **les périodes électorales sont des moments particulièrement sensibles car elles voient un accroissement des violences et abus à des fins politiques**, notamment contre les associations. Ils se retrouvent à plusieurs niveaux :

1. Attaques et violences par des utilisateur·ices

- **Attaques à l'encontre d'une personne ou d'une entité** : [cyberharcèlement](#), cyberviolences (dont usurpation d'identité, divulgation de données personnelles sur Internet...)
- **Production ou relai de discours haineux ou violents** envers des communautés et groupes de personnes
- **Production ou relai de désinformation**, notamment via des [deepfakes](#) (hypertrucages) politiques ou des [vidéos générées par IA](#)

Ces actions en ligne se conjuguent souvent avec [des actions hors ligne](#). Elles peuvent être menées par des individus ou dans le cadre d'actions coordonnées.

2. Rôles joués par les plateformes

Les plateformes comme YouTube, X, Facebook ou TikTok utilisent toutes des [algorithmes fondés sur l'« engagement »](#). L'objectif est simple : proposer aux utilisateur·ices des contenus qui les incitent à regarder, cliquer, faire défiler et rester scotchés, afin de vendre plus de publicité.

Cela a des conséquences à plusieurs niveaux :

- **Défaut de réaction et de réponse lors de signalements de contenus illicites ou illégaux.** Cela inclut l'impossibilité de signaler facilement des contenus illicites ou illégaux, [le défaut de réaction](#) ou de suivi après un signalement ou l'absence d'interlocuteur·rice humain·e. Dans ces cas, les plateformes sont susceptibles de manquer à leurs obligations légales, prévues par le règlement européen sur les services numériques.
- **Algorithmes et politiques de modération.** Les algorithmes de recommandation des plateformes peuvent [amplifier les contenus violents, haineux et la désinformation](#). Certains contenus ou comptes peuvent, à l'inverse, être dépriorisés ou invisibilisés (« shadowban »), réduisant la portée des contre-discours. Certains contenus peuvent aller jusqu'à être dépubliés. À noter que dans ce cas-là, les plateformes ont l'obligation d'apporter une justification suffisante.
- **Publicités politiques et monétisation de comptes.** Les publicités politiques et posts sponsorisés sont soumis à des règles spécifiques, notamment des règles de transparence pas toujours respectées.

Tous ces processus contribuent distinctement à la déstabilisation des processus démocratiques, à l'érosion du respect des droits humains, et affectent le travail des associations.



Éléments de compréhension

Contenus illégaux/illicites versus contenus contraires aux conditions générales d'utilisation

1. Quelles différences ?

En matière de violences et d'attaques en ligne, on distingue les **contenus illégaux** (aussi appelés illicites) et les **contenus contraires aux conditions générales d'utilisation** des plateformes.

- **Contenus illégaux** : les contenus illégaux sont des contenus dont la simple existence ou diffusion est interdite par la loi, au niveau de l'Union Européenne ou à l'échelon national. Concrètement, l'apologie du terrorisme, les contenus pédopornographiques ou les discours de haine incitant à la violence constituent des contenus illégaux sur les plateformes.
- **Contenus contraires aux CGU (conditions générales d'utilisation)** : ce sont des contenus que les plateformes choisissent d'interdire sur leur espace indépendamment de toute obligation légale. Une plateforme peut par exemple interdire la nudité, les discours politiques, la désinformation, ou certains contenus commerciaux sans qu'ils soient nécessairement illégaux.

2. Pourquoi la distinction importe ?

La distinction importe à la fois en termes de responsabilité des plateformes, et en termes de conséquences pour les personnes qui publient ou relaient du contenu.

Sur la responsabilité des plateformes : le Digital Services Act (DSA), règlement européen visant à encadrer la responsabilité des plateformes en ligne, articule les deux niveaux de manière très précise.

- **Pour les contenus illégaux**, les obligations sont contraignantes : les plateformes doivent prévoir des mécanismes de signalement accessibles (article 16), traiter les signalements de la part des signaleurs de confiance en priorité (article 22) et retirer rapidement les contenus illégaux sous peine d'engager leur responsabilité (article 6).
- **Pour les contenus contraires aux CGU**, le DSA impose surtout des obligations de transparence et d'équité : les CGU doivent être claires et accessibles (article 14), les décisions de modération doivent être motivées (article 17) et les utilisateurs doivent avoir accès à un mécanisme de recours interne (article 20).

En résumé : dans tous les cas, vous pouvez signaler aux plateformes tout contenu qui est soit illégal, soit contraire aux conditions générales d'utilisation des plateformes. Quand le contenu est illégal, cela relève également du droit pénal et ouvre des possibilités supplémentaires d'action en justice.

Pour plus d'informations sur le DSA :

Le guide de l'association [AlgorithmWatch](#), « [A guide to the Digital Services Act, the EU's new law to rein in Big Tech](#) »

[La fiche de service-public.fr](#) sur la responsabilité en matière de contenus illégaux



Que faire si l'on est victime ou témoin d'abus en ligne ?

En tant qu'association, vous pouvez mettre en œuvre plusieurs stratégies. Nous les présentons brièvement ici, et les ressources proposées plus loin vous permettent de les mettre en œuvre concrètement.

Documenter

Conserver des [preuves de l'abus ou de l'attaque](#) est essentiel : capture d'écran du contenu, copie de votre signalement auprès des plateformes (voir plus bas) pour pouvoir contester en cas de non-réponse. Le [Digital First Aid Kit](#) de la coalition de Digital Defenders est un excellent outil pour cibler ce qu'il faut documenter et dans quel but en cas d'attaque en ligne.

Signaler

Les grandes plateformes de réseaux sociaux sont tenues de mettre à disposition un mécanisme de signalement en ligne et de retirer tout contenu illégal. Elles doivent également examiner les contenus qui contreviennent à leurs conditions générales d'utilisation. Les démarches à suivre pour signaler des contenus sur chaque plateforme sont notamment détaillées au sein du guide [Nos Voix Nos Combats](#). Au besoin, vous pouvez vous tourner vers [les signaleurs de confiance](#), des organisations qui disposent d'un statut spécial et bénéficient d'un traitement prioritaire de la part des plateformes.

De plus, si vous n'êtes pas d'accord avec la décision d'une plateforme de supprimer, restreindre ou rendre moins visible une publication ou un compte, vous pouvez adresser votre réclamation au système de traitement des réclamations de la plateforme. [Le guide « Stay Loud » de Bits of Freedom](#) (en anglais) vous indique la marche à suivre pour chaque plateforme pour réaliser ce contre signalement.

Se protéger

Si vous êtes attaqué·e en ligne, vous pouvez prendre des mesures techniques pour réduire la portée de l'attaque (exemple : paramétrage des réseaux sociaux). Le guide réalisé par Nos Voix Nos Combats détaille la marche à suivre en cas d'attaque en ligne pour [se protéger soi](#), mais également [protéger les autres](#). De manière générale, ce guide a pour but d'orienter les associations si elles subissent une attaque, [avec des protocoles spécifiques à leur moyens et leur structure](#).



Vous pouvez également mettre en place des mesures préventives si vous êtes victime d'une attaque hors réseaux sociaux (par exemple, par un média d'extrême-droite) et avez peur que celle-ci soit suivie d'attaques en ligne (exemples : blocage de comptes spécifiques, fermeture des espaces commentaires, diagnostic de sécurité numérique, etc.).

Enfin, ne négligez pas votre santé mentale. Les ressources ci-dessous vous redirigent vers des professionnels et donnent des conseils pour ne pas rester seul·e si vous subissez ou observez des violences. [L'association Féministes contre le cyberharcèlement](#) dispose d'un guide dans lequel vous trouverez des conseils pratiques à mettre en œuvre, avec une expertise particulière sur les violences sexistes et sexuelles. Vous retrouverez toutes les associations spécialisées et numéros à joindre pour vous protéger et en parler.

Communiquer

Votre stratégie de communication va dépendre de votre analyse de la portée et des conséquences de l'attaque. Vous pouvez par exemple choisir de ne pas communiquer sur l'attaque pour ne pas attirer l'attention. Si vous choisissez ou avez besoin de prendre la parole, prenez le temps d'évaluer les risques et mettre en place des mesures de sécurité au préalable. [Le guide « Les associations et les syndicats face aux menaces et violences d'extrême droite »](#) de VoxPublic donne une série de conseils et de pistes d'action concrètes sur les stratégies médiatiques et de communication à adopter en cas d'attaque en ligne (page 6).

Passer par la voie légale

Les abus et attaques relèvent de différents cadres juridiques, notamment sur le numérique (règlement européen sur les services numériques, loi dite « SREN »), les influenceur·euses, l'encadrement des campagnes électorales. Par ailleurs, beaucoup de cyberviolences sont punies pénalement.

Il est ainsi possible de déposer plainte en cas d'attaque. La marche à suivre est détaillée au sein du guide de [Nos Voix Nos Combats](#), qui aborde toutes les questions relatives au dépôt de plainte jusqu'à la possibilité de faire appel à une aide juridictionnelle. Le [guide de Féministe contre le cyberharcèlement](#) dresse également un processus étape par étape très clair pour porter plainte en cas d'attaque.

Prévenir et anticiper

Pour se prémunir contre les attaques ou en minimiser les conséquences, réaliser des diagnostics de sécurité en ligne comme hors ligne (évaluation des risques, de leur portée, des moyens existants pour les mitiger, des actions à mettre en œuvre pour renforcer sa sécurité). La prévention passe aussi par des actions de formation et l'élaboration de protocoles (par exemple : protocole de prise en charge des salarié·es en cas de raid de cyberharcèlement). Tous ces conseils sont explicités au sein du guide de [Nos Voix Nos Combats](#).



Ressources

Pour ne pas vous retrouver seul·es face aux violences en ligne, cette section vous propose une liste non exhaustive de ressources concrètes, pour agir et vous protéger, en fonction de votre situation :

Cyberharcèlement / cyberviolences

- Nos Voix Nos Combats : [Guide d'autodéfense contre le cyberharcèlement visant les militant·e·s des droits](#)

Un guide à destination des associations et des militant·es utile pour se prémunir contre les attaques, agir en cas de cyberviolences et riposter. Il fournit des définitions précises et juridiques des différentes violences en ligne ([cyberharcèlement](#), [raids de cyberharcèlement](#), [menaces](#), [usurpation d'identité](#), [injure](#), [diffamation...](#)).

- Féministes contre le cyberharcèlement : [Que faire en cas cyberharcèlement et de cyberviolences ?](#)

Un guide également complet sur les cyberviolences en général. Il est aussi très utile pour les signalements sur les réseaux sociaux et la conservation des preuves, avec une expertise supplémentaire sur les violences sexistes et sexuelles en ligne. Il [répertorie](#) les numéros de soutien, les liens vers les plateformes de signalement et les associations d'accompagnement des victimes.

- Le [Digital First Aid Kit](#) de la coalition de Digital Defenders

Un guide qui vous accompagne de A à Z pour enregistrer d'éventuelles attaques numériques.

Lutter contre les stratégies d'extrême droite

- VoxPublic : [Les associations et les syndicats face aux menaces et violences d'extrême droite](#)

Une ressource utile pour comprendre les procédés violents de l'extrême droite hors et en ligne. En cas d'attaque, il donne des conseils stratégiques de [riposte médiatique et sur les réseaux sociaux](#) (page 6).

Responsabilité des plateformes

- Le guide [« Stay Loud »](#) de l'association Bits of Freedom

Ce guide (en anglais) détaille précisément vos droits en matière de signalement, et vous explique comment contester un retrait ou une restriction de contenu injustifié sur différents réseaux sociaux.

- L'outil [Open Terms Archive](#)

Cet outil enregistre publiquement chaque version des conditions d'utilisation des services en ligne pour en permettre le contrôle démocratique. L'objectif est de rendre ces conditions d'utilisation plus transparentes, pour pouvoir contrôler les décisions prises par les plateformes en matière de modération de contenus.

Sécurité en ligne

- [Nothing2Hide](#)

Il vaut mieux prévenir que guérir ! Le site internet de Nothing2Hide accompagne les journalistes, militant·es et activistes dans l'installation de [nombreux outils](#) pour améliorer leur sécurité en ligne et renforcer leurs libertés numériques. Surtout, il propose une [assistance numérique d'urgence](#) en cas de piratage.

Combattre la désinformation

- ISD (Innover contre l'extrémisme, la haine et la désinformation) : [Désinformation en période électorale : Comment la société civile peut-elle répondre ?](#)

Un guide qui évalue les différents risques que représente la désinformation en période électorale. Il fournit des conseils pour les identifier et y répondre le plus stratégiquement possible.

- AFP (Agence France Presse) : [Combattre la désinformation en période électorale](#)

Un cours en ligne qui permet d'apprendre à identifier et vérifier les principaux types de désinformation qui circulent pendant une campagne électorale, ou encore reconnaître un narratif trompeur. Il présente également des outils utiles pour faire la veille d'internet et des réseaux sociaux en période électorale.

Combattre la désinformation (suite)

- [Désinfox Migrations](#)

Sur son site internet, l'organisation propose des informations vérifiées et accessibles sur les questions migratoires, pensées pour répondre à la désinformation à ce sujet.

- Les plateformes de fact checking de la presse peuvent aussi s'avérer utiles

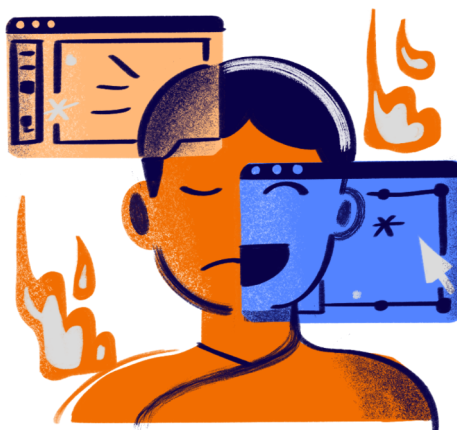
Par exemple, [l'AFP Factuel](#) regroupe tous les articles vérifiés par l'AFP (Agence France Presse), ou encore la rubrique [Décodeurs du Monde](#) qui distingue le vrai du faux dans l'actualité. De [nombreux médias](#) proposent ce genre de contenu.

- [Ask Vera, l'intelligence artificielle contre la désinformation](#)

Cette IA a été créée par l'association à but non lucratif LaReponse.tech. Ask Vera se présente comme « le numéro de confiance pour vérifier les faits ». C'est une IA gratuite et simple d'utilisation : il suffit d'enregistrer son numéro - 09.74.99.12.95 - et de lui écrire sur la messagerie WhatsApp ou de l'appeler par téléphone pour lui demander si telle information est vraie.

- [ODIL, la plateforme francophone des initiatives de lutte contre la désinformation](#)

ODIL est un projet porté par l'Organisation Internationale de la Francophonie (OIF) qui a pour objectif de visibiliser les initiatives en matière de lutte contre la désinformation. Pour cela, est mis en place un [moteur de recherche](#) pour avoir accès à toutes les initiatives actives dans le pays souhaité, ainsi qu'un [centre de ressources](#) qui accueille des articles scientifiques, rapports, études et ressources pédagogiques destinés aux acteurs de la lutte contre la désinformation.



Besoin d'aide ?

Si vous êtes témoin ou que votre association est victime d'une attaque en ligne pendant la campagne électorale des municipales de 2026, et que vous souhaitez être aiguillé·e vers les bons interlocuteur·rice·s, vous pouvez contacter l'association VoxPublic par email : contact@voxpathic.org

À propos

Ce guide est le fruit d'un travail interassociatif au sein du projet sur la responsabilité des réseaux sociaux dans la montée des discriminations, dans le contexte des élections municipales de 2026.

Pour en savoir plus sur le projet "Big Tech et discriminations" de VoxPublic, vous pouvez consulter [la page dédiée sur notre site internet](#).

