LE DOXING (ou doxxing)

Divulguation des données personnelles

COMPRENDRE POUR MIEUX AGIR



296 cas de doxing signalés par le 3018 aux plateformes en ligne au cours du 1er semestre 2026.*

Source : données du 3018, 2026

DE QUOI PARLE-T-ON ?

Le doxing (ou doxxing) est le fait de divulguer en ligne les **données personnelles** d'une personne, **sans son consentement** et dans un **but malveillant**.

Qu'est ce qu'une **donnée personnelle** ?
Les données personnelles sont toutes les informations qui permettent d'identifier directement ou indirectement une personne.
Exemples : nom complet, adresse électronique, numéro de téléphone, adresse du domicile, photos, vidéos, comptes de réseaux sociaux, mots de passe ...

Toute personne, peu importe son âge, peut être victime de doxing.

OÙ LES DONNÉES PEUVENT-ELLES ÊTRE DIFFUSÉES ?

- Réseaux sociaux (Instagram, TikTok, Snapchat...)
- Plateformes de vidéo en ligne (YouTube, Twitch...)
- Applications de messagerie : messages privés, groupes et canaux de discussion (WhatsApp, Telegram...)
- Forums de discussion et blogs en ligne
- Sites Internet

DANS QUELS CONTEXTES :

- L'**extorsion :** menace de divulguer les données personnelles si une personne refuse de céder à ses exigences, qu'elles soient financières, sexuelles ou autres.
- La **vengeance**
- L'**humiliation** ou l'**intimidation**

QUE DIT LA LOI ?

Le doxing constitue une atteinte à la vie privée et est puni par la loi :

Le fait de révéler, diffuser ou transmettre des informations personnelles sur la vie privée, familiale ou professionnelle d'une personne, permettant de l'identifier ou de la localiser dans le but de l'exposer (ou d'exposer sa famille) à un risque direct d'atteinte à la personne ou aux biens, est sanctionné par l'*article 223-1-1 du Code pénal*.

Les peines encourues sont **plus sévères** lorsque la victime est mineure.

COMMENT SE PROTÉGER ?

- **Limiter l'exposition de sa vie privée en ligne** : passer ses comptes en mode privé, utiliser des pseudonymes, ne pas publier de contenus privés.
- **Ne pas partager publiquement des données personnelles sensibles** : numéro de téléphone, adresse e-mail, adresse postale, mot de passe...
- **Sécuriser ses comptes :** choisir un mot de passe unique et robuste pour chaque compte créé, activer la double authentification.
- **Même si vous aviez partagé des informations**, personne n'a le droit de les utiliser pour vous nuire, vous n'êtes pas responsable de cette violence.

⚠ **Éviter de partager tout contenu permettant d'identifier sa localisation**

QUE FAIRE FACE À CES SITUATIONS ?



MESURER LES IMPACTS ET SAVOIR RÉAGIR

QUELS PEUVENT ÊTRE LES RETENTISSEMENTS ?

- **Réactions psychiques et émotionnelles :** sentiment de honte, peur, stress, anxiété, sentiment d'insécurité, des pensées envahissantes, un besoin d'être constamment sur ses gardes, peur de sortir ou d'aller à l'école.
  La divulgation de données personnelles peut donner le sentiment de ne plus maîtriser sa vie privée et de ne plus être en sécurité. La peur de ce que d'autres pourraient faire de ces informations peut persister même après leur suppression.
- **Manifestations physiques :** troubles du sommeil, fatigue, agitation, difficultés de concentration.
- **Risques pour la sécurité physique :** risques d'agressions physiques rendues possibles par la divulgation d'information sur la localisation de la victime.
- **Autres violences :** usurpation d'identité, harcèlement et cyberharcèlement, deepfakes, contacts non sollicités par des personnes malveillantes, swatting...
- **Atteinte à la réputation :** risque d'impact sur le parcours scolaire et professionnel de la victime.

LES BONS RÉFLEXES SI UN CONTENU A ÉTÉ DIFFUSÉ

POUR LES VICTIMES

- En cas de chantage : ne pas céder aux demandes et chercher de l'aide rapidement. Si vous avez déjà cédé, vous pouvez être aidé en appelant le 3018.
- Parler à un adulte de confiance.
- Garder des preuves (captures d'écran, messages...).
- Signaler le compte et le contenu sur la plateforme.
- Contacter le 3018 pour obtenir une aide et être assisté dans les démarches de retrait des contenus.
- En cas de soupçon de piratage : changer ses mots de passe.

POUR LES PARENTS ET PROFESSIONNELS

- Accueillir la parole de l'enfant sans jugement ni reproche, le remercier de sa confiance et lui rappeler qu'il n'est pas responsable des actes de l'auteur.
- Evaluer avec lui l'ampleur de la diffusion et ce qu'il redoute le plus. Lui présenter les démarches possibles et proposer un soutien psychologique si la peur devient envahissante. Il faut l'associer autant que possible aux décisions qui le concernent.
- Ne pas négocier directement avec l'auteur.
- Accompagner le mineur dans les démarches de signalement et le dépôt de plainte.
- Continuer à prendre régulièrement des nouvelles de la victime et veiller à préserver une relation de confiance.

PREMIER RÉFLEXE



3018

Le dispositif national pour les jeunes victimes, témoins, auteurs, leurs familles et les professionnels sur les questions de harcèlement et de violences numériques.

Ouvert 7j/7, de 9h à 23h

- ✓ Une **écoute** gratuite, anonyme et confidentielle
- ✓ Un **accompagnement** des jeunes et leurs familles
- ✓ Une **orientation** vers les services compétents
- ✓ Des **signalements transmis et traités en priorité par les plateformes,** afin d'obtenir le retrait rapide des comptes et contenus préjudiciables, grâce au statut de **signaleur de confiance**

Par téléphone

Par tchat sur l'App 3018

Télécharger l'App 3018

En cas de danger immédiat, contactez les secours au 17 (police) ou 18 (pompiers)

e-Enfance 3018 OBSERVATOIRE