



Visioconférence : ayez les bons réflexes pour choisir et utiliser vos logiciels

Publié le 15 avril 2020 - Direction de l'information légale et administrative (Premier ministre)

Vous êtes en télétravail, vous participez à des réunions, des formations, des cours en ligne... Pendant la période de confinement vous utilisez certainement des outils gratuits de discussion et de visioconférence et vous vous demandez si ces logiciels sont fiables. La Commission nationale de l'informatique et des libertés (Cnil) répond à vos interrogations et rappelle quelques règles de vigilance.

Ayez les bons réflexes

- lisez toujours les conditions générales d'utilisation ou la politique de confidentialité/de protection des données des outils de visioconférence pour vérifier leur fiabilité ;
- utilisez des applications qui vous garantissent la confidentialité des communications (pas d'enregistrement ou de stockage des conversations et pas de réutilisation des conversations) ;
- vérifiez que vos données personnelles ne sont pas utilisées pour d'autres finalités ;
- limitez le nombre d'informations à fournir (utiliser un pseudonyme et une adresse mail dédiée, par exemple) ;
- utilisez un mot de passe différent de ceux utilisés sur d'autres services ;
- fermez l'application lorsque vous ne l'utilisez plus ;
- désactivez le micro et la webcam quand ils ne sont pas nécessaires.

➔ **À savoir** : Vous devez être informé de l'usage de vos données. Les informations fournies peuvent s'étendre à d'autres types de données techniques permettant une ré-identification (adresse IP, identifiant de l'appareil, cookies ou technologies analogues).

Conseils et protection de la vie privée

- privilégiez les solutions qui protègent la vie privée (par exemple Tixeo, certifiée par l'Agence nationale de la sécurité des systèmes d'information (Anssi) ;
- évitez de télécharger l'application depuis un site web ou une source inconnus ;
- n'utilisez que les applications pour lesquelles l'éditeur indique clairement comment les données sont réutilisées (dans l'application elle-même ou sur son site web, par exemple) ;
- lisez les commentaires des utilisateurs sur des forums de discussion ;
- vérifiez que l'éditeur a mis en place des mesures de sécurité essentielles, comme le chiffrement des communications de bout en bout ;
- sécurisez le réseau Wi-Fi avec un mot de passe robuste, en activant le chiffrement WPA2 ou WPA3 ;
- assurez-vous que l'antivirus et le pare-feu sont à jour.

⚠ **Attention** : certaines applications gratuites peuvent rentabiliser leur service en traitant des informations personnelles. Vos conversations privées ou professionnelles, peuvent révéler beaucoup d'informations, soit intimes, soit protégées par une obligation de confidentialité par rapport à vos activités professionnelles.

➔ **À savoir** : Pour les usages professionnels, les points de vérification doivent être renforcés (notamment par la signature d'un accord de sous-traitance avec l'éditeur de l'outil). Le recours à un fournisseur de solutions certifié par l'Agence nationale de la sécurité des systèmes d'information (Anssi) [\(https://www.ssi.gouv.fr/entreprise/certification_cspn/tixeoserver-version-11-5-2-0/\)](https://www.ssi.gouv.fr/entreprise/certification_cspn/tixeoserver-version-11-5-2-0/) est conseillé en cas d'activité sensible ou soumise au secret professionnel.

Et aussi

- Fichiers informatiques et données personnelles (<https://www.service-public.fr/particuliers/vosdroits/F2024>)

Pour en savoir plus

- Covid-19 : les conseils de la Cnil pour utiliser les outils de visioconférence [🔗 \(https://www.cnil.fr/fr/covid-19-les-conseils-de-la-cnil-pour-utiliser-les-outils-de-visioconference\)](https://www.cnil.fr/fr/covid-19-les-conseils-de-la-cnil-pour-utiliser-les-outils-de-visioconference)
Commission nationale de l'informatique et des libertés (Cnil)
- Les outils de visioconférence avec la Cnil [🔗 \(http://www.jeunes.gouv.fr/spip.php?article9219\)](http://www.jeunes.gouv.fr/spip.php?article9219)
Ministère chargé de l'éducation