CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

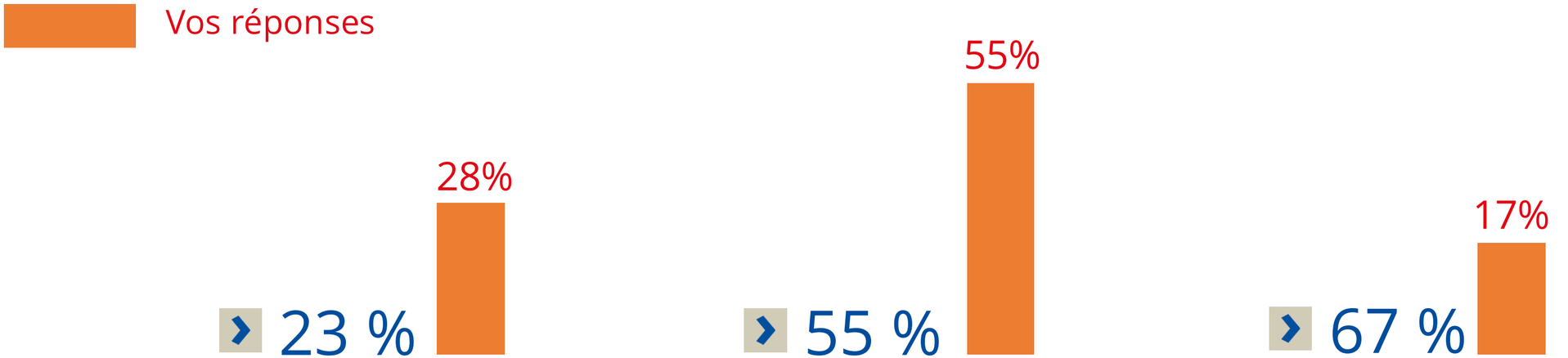
Protéger et accompagner ses enfants en ligne

Webinaire FCPE

Mardi 17 mars 2026

POUR COMMENCER : UN QUIZ

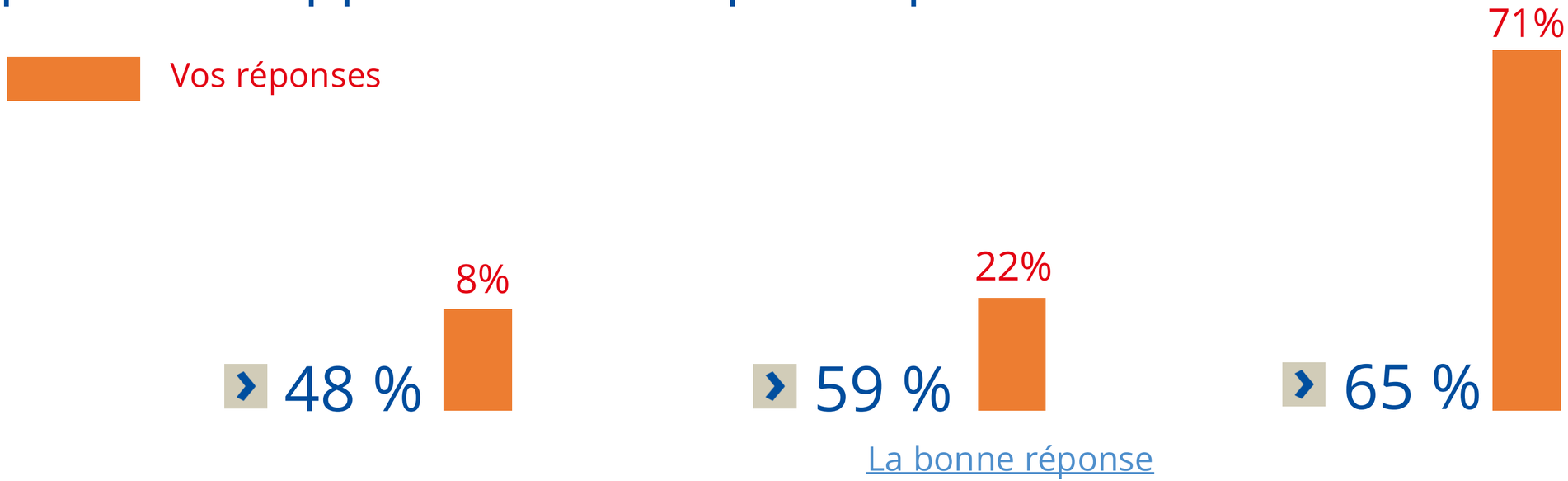
- Selon vous, quel est le pourcentage d'enfants âgés de 8-10 ans qui utilisent les réseaux sociaux ?



La bonne réponse

POUR COMMENCER : UN QUIZ

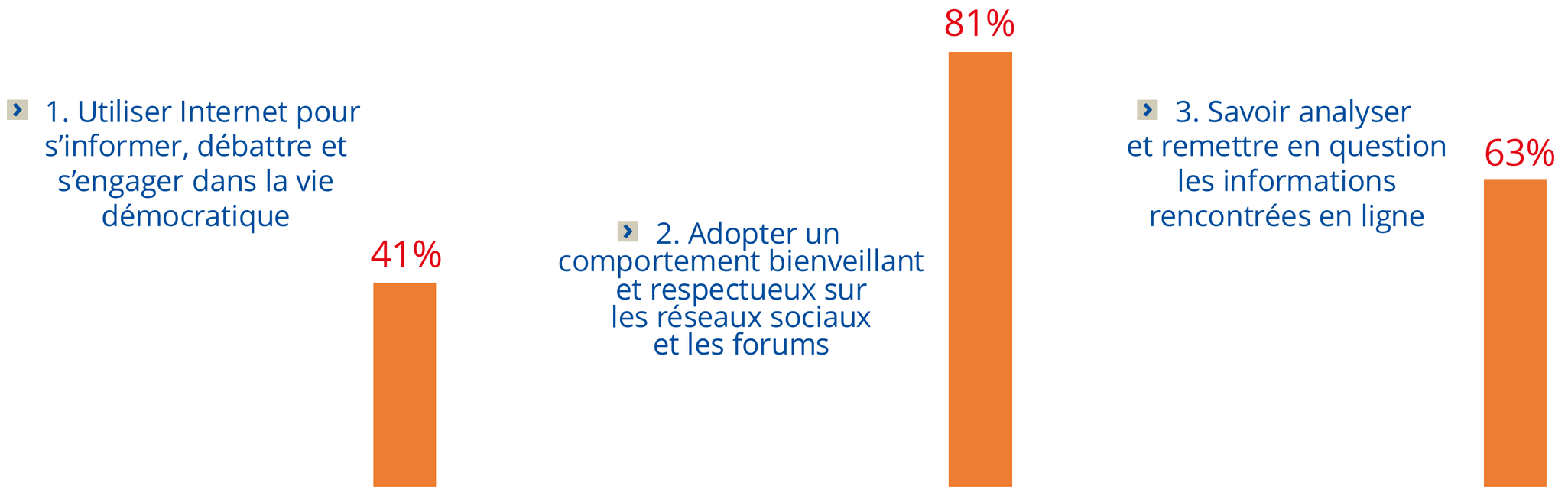
- Selon vous, quel est le pourcentage d'adolescents âgés de 11-14 ans qui ont un appareil numérique en permanence dans leur chambre ?



POUR COMMENCER : UN QUIZ

Comment définir la « citoyenneté numérique » ?

Vos réponses



Toutes ces réponses définissent la citoyenneté numérique.

Eléments de réponse

- Etude 2024 Caisse d'épargne, e-Enfance, 30/18 : **67 % des enfants de 8-10 ans** sont sur les réseaux sociaux
- Etude 2024 Génération Numérique (Les pratiques numériques des 11-18 ans) : **59 % des 11-14 ans** ont un appareil numérique en permanence dans leur chambre
- **Citoyenneté numérique** (définition du Conseil de l'Europe) :
  - Être en ligne : qui suis-je en ligne ? Comment suis-je avec les autres ? Comment je m'informe ?
  - Bien-être en ligne : comment je vais en ligne ? Est-ce-que je sais protéger ma vie privée ?
  - Droits en ligne : Je connais mes droits liés à ma vie numérique ? Je sais comment les exercer ?

ETRE PARENT EN 2026

De nombreux écrans dans nos foyers, une mauvaise connaissance des usages numériques de nos enfants :

- 1/3 des parents seulement activent le contrôle parental
- 1/3 des parents ne contrôlent pas les usages numériques de leurs enfants (réseaux sociaux, jeux vidéos…)
- Sentiment de culpabilité des parents

Des parents unanimes sur les risques auxquels sont exposés leurs enfants en ligne :

- Surexposition des enfants aux écrans, manque d'attention et de concentration
- Atteinte à la vie privée, usurpation d'identité, arnaques (jeux d'argent)
- Cyberharcèlement, moqueries
- Exposition à des contenus pornographiques et hyper violents
- Mauvaises rencontres en ligne

La CNIL

Un peu d'histoire

ARCHIVES

Une division de l'informatique est créée à la chancellerie " Safari " ou la chasse aux Français

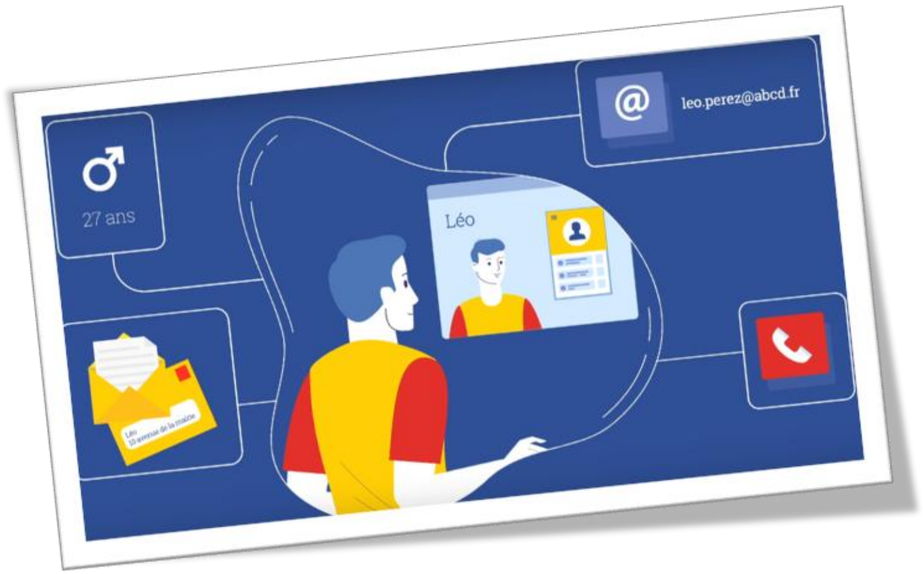
En ordre dispersé, les départements ministériels tentent de développer à leur profit, à leur seul usage, l'informatique et son outil, l'ordinateur. Ce n'est pas tout à fait un hasard si, à l'époque où le Journal officiel va publier un arrêté créant une " division de l'informatique " au ministère de la justice, celui de l'intérieur met la dernière main à la mise en route d'un ordinateur puissant destiné à rassembler la masse énorme des renseignements grappillés sur tout le territoire; pas un hasard non plus si le projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus) destiné à définir chaque Français par un " identifiant ", qui ne définisse que lui, maintenant terminé, est l'objet de convoitises ardentes; le ministère de l'intérieur y souhaite jouer le premier rôle. En effet, une telle banque de données, soubassement opérationnel de toute autre collecte de renseignements, donnera à qui la possédera, une puissance sans égale.Ainsi se trouve d'évidence posé un problème fondamental, même s'il est rebattu : celui des rapports des libertés publiques et de l'informatique. Son importance exigerait qu'il en fût, au Parlement, publiquement débattu. Tel ne parait pas être, pourtant, la solution envisagée par le premier ministre dans les directives qu'il vient d'adresser au ministère de la justice, intéressé au premier chef si l'on s'en rapporte à la Constitution qui dans son article 66 fait de l'autorité judiciaire le gardien des libertés individuelles.

Par PHILIPPE BOUCHER.

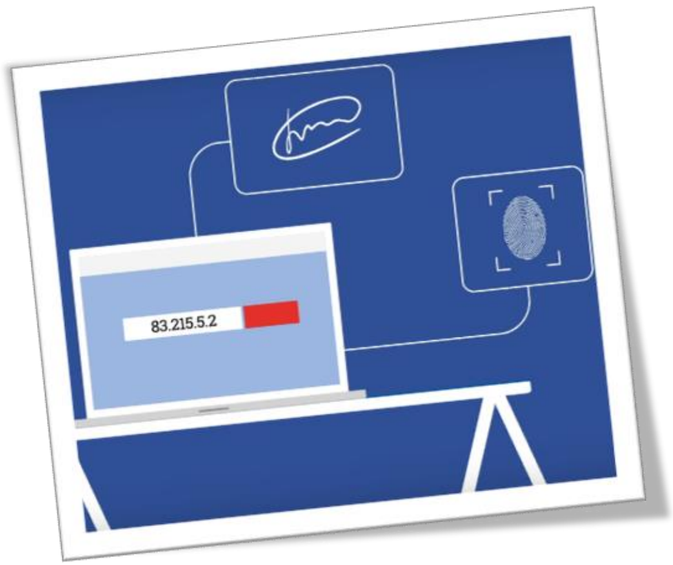
NOS 4 MISSIONS

LES DONNÉES PERSONNELLES

Une donnée personnelle est toute information se rapportant à une personne identifiée ou identifiable



Prénom, nom, adresse, téléphone



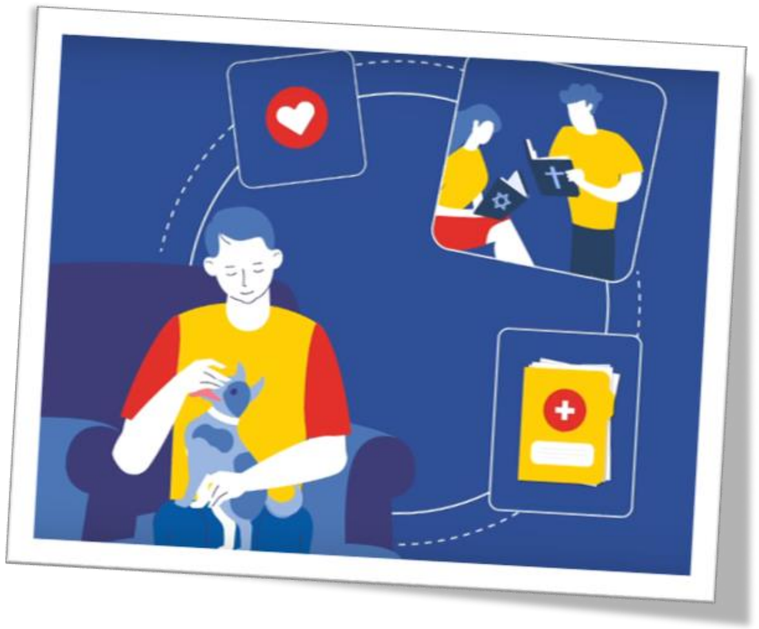
Adresse IP, numéro d'immatriculation

Voix, visage

LES DONNÉES PERSONNELLES

Certaines données sont « sensibles »

- Religion
- État de santé
- Appartenance syndicale
- Opinions politiques
- Origine ethnique
- Orientation sexuelle
- Données biométriques et génétiques



Eviter de les divulguer en ligne

- Risque de discrimination, cyberharcèlement

LE RGPD

- **Respect des droits et libertés fondamentales, socle des valeurs démocratiques de l'UE**
  - La Charte des droits fondamentaux de l'UE reconnaît le droit à la protection des données
- **Evolutions technologiques : usage et partage de données personnelles en forte hausse**
- **Point clé : confiance des utilisateurs**
- **Les personnes doivent avoir le contrôle des données les concernant**
- **Car les risques sont nombreux**
  - Atteinte à la vie privée, discriminations
  - Arnaques, usurpation d'identité
  - Manipulation, harcèlement
  - Négation des droits
  - Surveillance excessive

CNIL.

Les enjeux

QUELQUES CHIFFRES

Etude 2024 de Génération numérique : enquête sur les pratiques numériques des 11-18 ans

- **59%** des 11-14 ans et **86%** des 15-18 ans ont un appareil numérique en permanence dans leur chambre
- **59%** des 11-14 ans et **95%** des 15-18 ans sont inscrits sur un ou plusieurs réseaux sociaux
- Les réseaux les plus utilisés : **Snapchat, Tiktok, Instagram**
- **Points positifs** : communiquer avec les amis ou la famille, apprendre de nouvelles choses, se divertir
- **Impacts négatifs** : on devient accro, les réseaux propagent des rumeurs, les réseaux contribuent au cyberharcèlement



Mes traces sur Internet

Les données traitées par défaut dans mes réglages :

Accès au micro, géolocalisation, partage d'informations, etc.

Les données que je donne de moi-même

- Prénom, Nom
- Adresse de messagerie
- Numéro de téléphone
- Date de naissance
- Géolocalisation
- Photographies
- Vidéos
- Carte de crédit

Les données interprétées de mes actions

- Goûts musicaux, vestimentaires…
- Désirs
- Religion, foi
- Orientation sexuelle
- Opinions politiques
- Temps passé sur une application

Les données de mon entourage

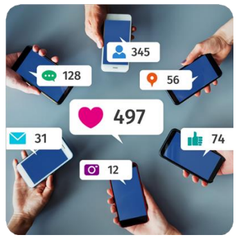
- Amis
- Famille, parents
- Situation amoureuse
- Goûts de mon entourage
- Photos / vidéos
- Domiciliation, lieux de vie et déplacements

CNIL.

Algorithmes et publicités ciblées

J'utilise un réseau social entièrement gratuit

Permet de **réunir un nombre** important d'utilisateurs



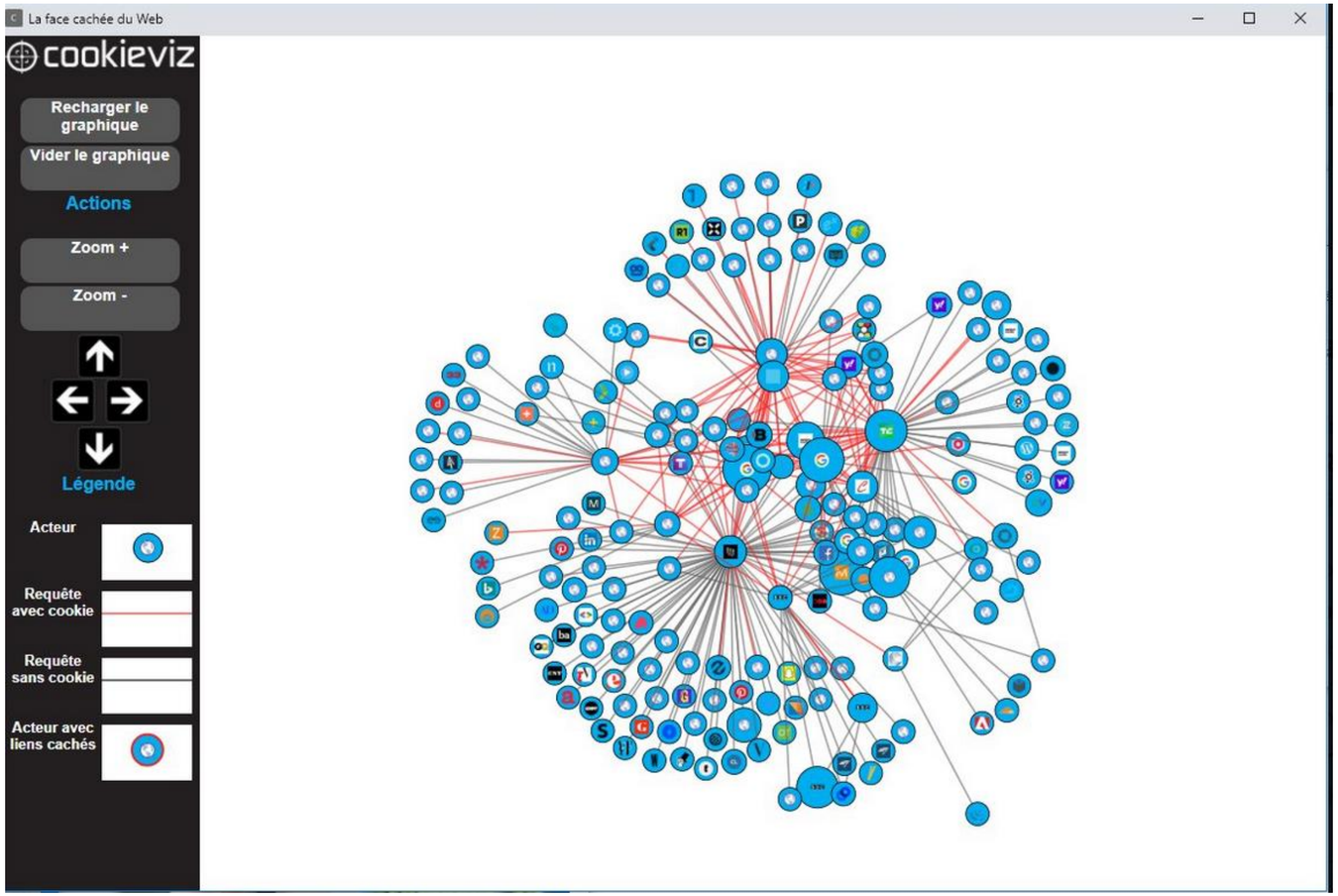
Il collecte mes données personnelles

Elles sont analysées pour être **monnayées à des fins publicitaires**. Plus elles sont nombreuses et précises, plus elles rapportent

Les entreprises paient le réseau pour afficher leur publicité ciblée

Mon profil établi à partir de mes données permet de m'afficher **des publicités personnalisées**

Cookieviz : dataviz en temps réel du tracking de votre navigation



Garder un esprit critique

Sur les réseaux sociaux :
Algorithmes dans les fils d’actualité
Proposition de contenus similaires, enfermement dans des bulles de filtre
Design des interfaces : influence sur nos choix et actions

Les droits numériques

NOS DROITS

Être informé

Savoir ce qui va être fait de mes données

Avoir accès à

Savoir quelles données me concernant sont détenues

Rectifier

Lorsque mes données sont erronées

S’opposer à

Je ne veux pas que mes données soient utilisées

Faire effacer

Mes données ne devraient pas ou plus être utilisées

Portabilité

Je veux déplacer mes données

NOS DROITS

COMMENT EXERCER SES DROITS ?

- Contacter celui qui détient vos données
- Délai de réponse légal : 1 mois
- En l’absence de réponse ou en cas de refus non motivé : plainte auprès de la CNIL

ET LES JEUNES ?

- **Avant ses 15 ans, c’est vous qui exercez ses droits pour lui**

Conseils pratiques

5 CONSEILS POUR LES PARENTS

- **Garder le lien avec nos enfants** : échanger, être à l'écoute en cas de problème
- **Se mettre d'accord sur des règles** : temps d'écran/autres activités
- **Accompagner nos enfants dans la protection de leur vie privée** : paramétrer son téléphone et les services en ligne (pseudo, compte en privé, photo non identifiante)
- **Promouvoir le civisme en ligne** : respect des autres, bienveillance
- **Respecter la vie privée des enfants** : les accompagner sans être intru

POINTS DE VIGILANCE

Risques d'une surveillance excessive des enfants en ligne :

- Rupture du lien de confiance parents-enfants
- Difficulté à grandir avec le numérique

S'interroger sur nos pratiques en tant que parents :

- Quelles actions pour protéger nos données personnelles ?
- *Sharenting* : publication de photos de mon enfant sur les réseaux sociaux

[Vidéo CNIL et DPC]

Accompagner et protéger son enfant

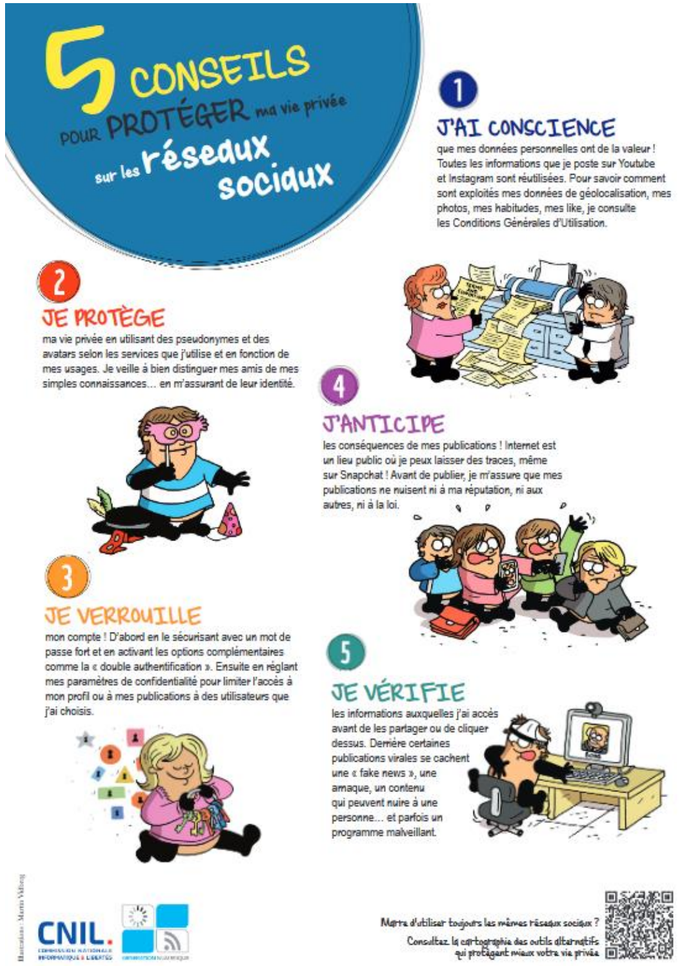
- **Discutez avec votre enfant et paramétrez avec lui les fonctionnalités**

Exemples de questions

- Que peux-tu faire avec ? Quelles règles décidées ensemble ?
- Il y a des choses qui te déplaisent ? Lesquelles ?
- Quelles sont tes applis préférées ? Pourquoi ?
- Quelles sont tes vidéos préférées ? Pourquoi ?
- Avec qui es-tu en relation ?
- As-tu déjà vu des vidéos en ligne qui t'ont choqué ? Qu'as-tu ressenti ?
- Si tu étais une appli, laquelle serais-tu ?

SUR LES RÉSEAUX SOCIAUX

- Naviguer en mode privé
- Désactiver ou ne pas activer la localisation permanente
- Utiliser un pseudonyme
- Mettre ses comptes sur les réseaux sociaux en mode « privé »
- Avoir des mots de passe solides et différents par service
- Utiliser un moteur de recherche respectueux de nos données



1 DES MOTS DE PASSE SOLIDES ET DIFFÉRENTS POUR CHAQUE COMPTE TU CHOISIRAS

Un mot de passe c'est comme une clé propre à chaque porte, elle te protège de l'intrusion. Si tu te fais voler un mot de passe que tu utilises pour différents sites web ou applications, ils pourront tous être piratés !

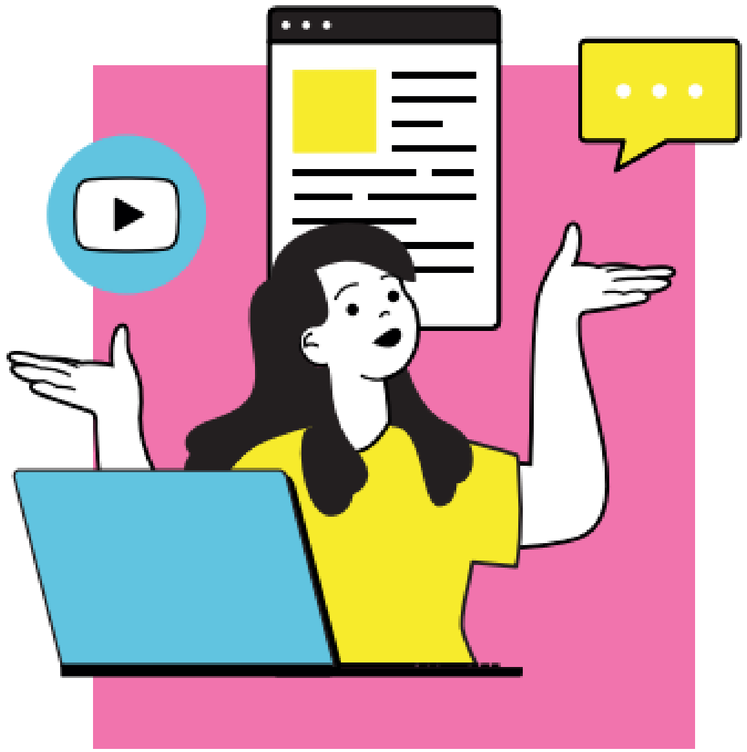
BONNES PRATIQUES

- Utiliser des mots de passe suffisamment longs, complexes et surtout différents pour chaque compte.
- Les garder secrets et privilégier un gestionnaire de mots de passe sécurisé pour les conserver.

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

3 EN LIGNE, LE MOINS POSSIBLE SUR TON IDENTITÉ TU DIRAS



Publier et partager tes données personnelles sur Internet (nom, prénom, adresse mail, photos, vidéos, vocaux…) peut les exposer à une utilisation malveillante.

BONNES PRATIQUES

- Éviter de divulguer tes données personnelles et celles de tes connaissances.
- Vérifier les paramètres de confidentialité de tes comptes pour définir ce qui peut être visible par les autres.

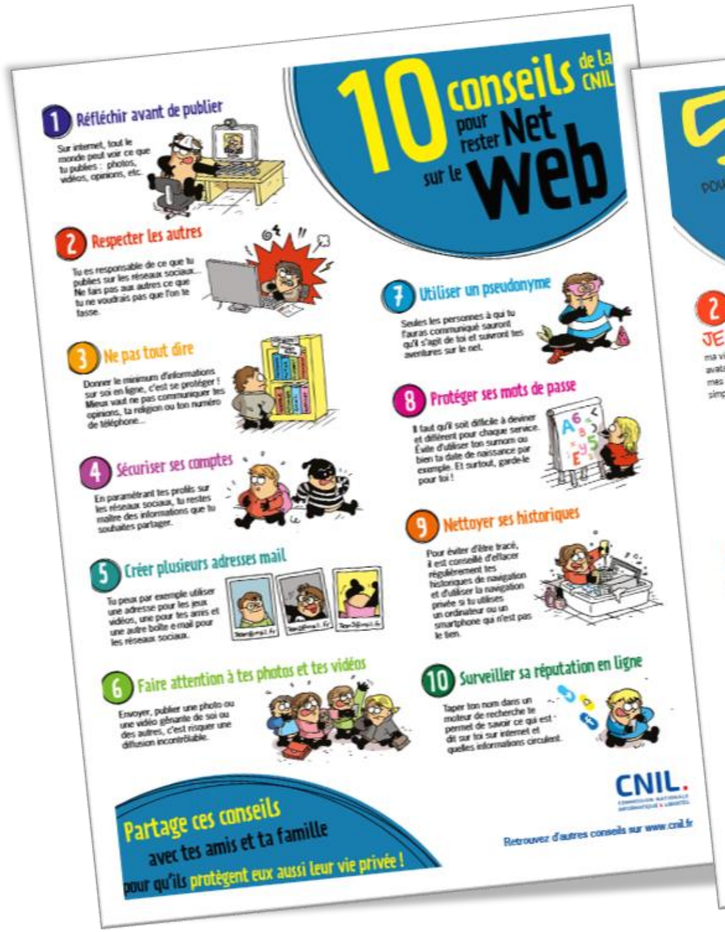
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

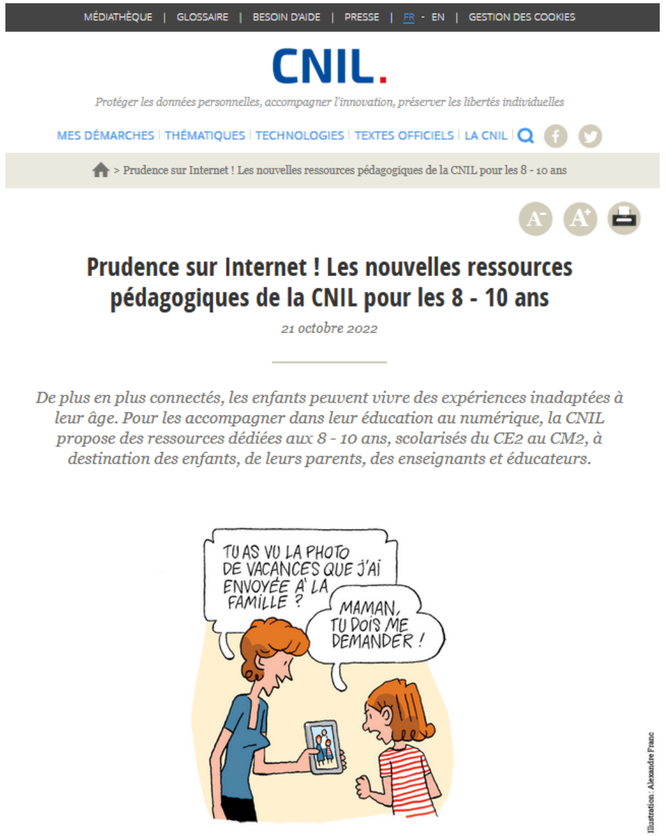
Ressources pédagogiques

NOS RESSOURCES PÉDAGOGIQUES

- Une rubrique « Enfants et ados » sur cnil.fr



LES RESSOURCES 8-10 ans



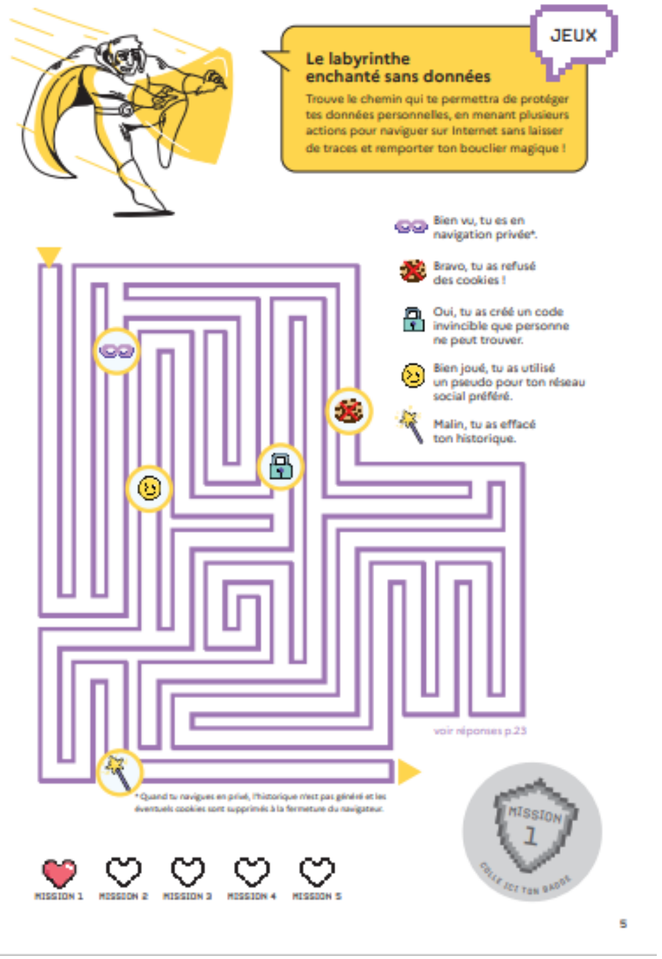
- 4 vidéos
- Poster/glossaire
- Quiz
- Jeu de cartes
- Diplôme
- Livret enseignants
- Livret parents

https://www.cnil.fr/fr/prudence-sur-internet-les-nouvelles-ressources-pedagogiques-de-la-cnil-pour-les-8-10-ans

LES RESSOURCES 11-15 ANS

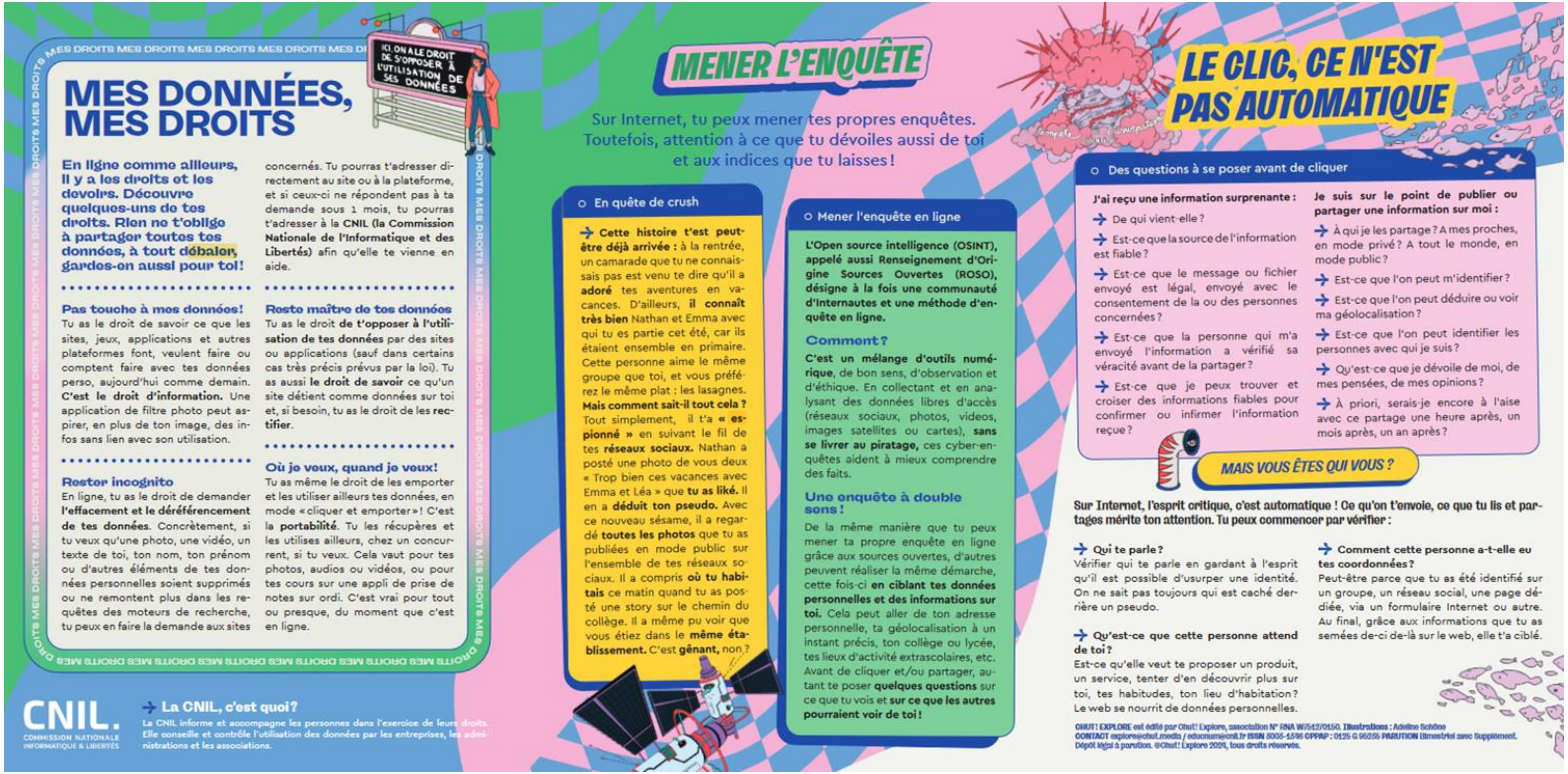
TOUS ENSEMBLE PRUDENCE SUR INTERNET

NOS RESSOURCES PÉDAGOGIQUES



UN OCÉAN DE DONNÉES

UN OCÉAN DE DONNÉES



MES DONNÉES, MES DROITS

En ligne comme ailleurs, il y a les droits et les devoirs. Découvre quelques-uns de tes droits. Rien ne t'oblige à partager toutes tes données, à tout déballer, gardes-en aussi pour toi !

Pas touche à mes données !

Tu as le droit de savoir ce que les sites, jeux, applications et autres plateformes font, veulent faire ou comptent faire avec tes données perso, aujourd'hui comme demain. **C'est le droit d'information.** Une application de filtre photo peut aspirer, en plus de ton image, des infos sans lien avec son utilisation.

Rester incognito

En ligne, tu as le droit de demander **l'effacement et le déréférencement de tes données.** Concrètement, si tu veux qu'une photo, une vidéo, un texte de toi, ton nom, ton prénom ou d'autres éléments de tes données personnelles soient supprimés ou ne remontent plus dans les requêtes des moteurs de recherche, tu peux en faire la demande aux sites concernés. Tu pourras t'adresser directement au site ou à la plateforme, et si ceux-ci ne répondent pas à ta demande sous 1 mois, tu pourras t'adresser à la **CNIL (la Commission Nationale de l'Informatique et des Libertés)** afin qu'elle te vienne en aide.

Reste maître de tes données

Tu as le droit **de t'opposer à l'utilisation de tes données** par des sites ou applications (sauf dans certains cas très précis prévus par la loi). Tu as aussi **le droit de savoir** ce qu'un site détient comme données sur toi et, si besoin, tu as le droit de les **rectifier.**

Où je veux, quand je veux !

Tu as même le droit de les emporter et les utiliser ailleurs tes données, en mode « cliquer et emporter » ! C'est la **portabilité**. Tu les récupères et les utilises ailleurs, chez un concurrent, si tu veux. Cela vaut pour tes photos, audios ou vidéos, ou pour tes cours sur une appli de prise de notes sur ordi. C'est vrai pour tout ou presque, du moment que c'est en ligne.

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

→ La CNIL, c'est quoi ?

La CNIL informe et accompagne les personnes dans l'exercice de leurs droits. Elle conseille et contrôle l'utilisation des données par les entreprises, les administrations et les associations.

MENER L'ENQUÊTE

Sur Internet, tu peux mener tes propres enquêtes. Toutefois, attention à ce que tu dévoiles aussi de toi et aux indices que tu laisses !

En quête de crush

→ **Cette histoire t'est peut-être déjà arrivée :** à la rentrée, un camarade que tu ne connaissais pas est venu te dire qu'il a **adoré** tes aventures en vacances. D'ailleurs, **il connaît très bien** Nathan et Emma avec qui tu es partie cet été, car ils étaient ensemble en primaire. Cette personne aime le même groupe que toi, et vous préférez le même plat : les lasagnes. **Mais comment sait-il tout cela ?** Tout simplement, il t'a **« espionné »** en suivant le fil de tes **réseaux sociaux.** Nathan a posté une photo de vous deux « Trop bien ces vacances avec Emma et Léa » que **tu as liké.** Il en a **déduit ton pseudo.** Avec ce nouveau sésame, il a regardé **toutes les photos** que tu as publiées en mode public sur l'ensemble de tes réseaux sociaux. Il a compris **où tu habitais** ce matin quand tu as posté une story sur le chemin du collège. Il a même pu voir que vous étiez dans le **même établissement.** C'est **gênant,** non ?

Mener l'enquête en ligne

L'Open source intelligence (OSINT), appelé aussi Renseignement d'Origine Sources Ouvertes (ROSO), désigne à la fois une communauté d'internautes et une méthode d'enquête en ligne.

Comment ?

C'est un mélange d'outils numérique, de bon sens, d'observation et d'éthique. En collectant et en analysant des données libres d'accès (réseaux sociaux, photos, videos, images satellites ou cartes), **sans se livrer au piratage,** ces cyber-enquêtes aident à mieux comprendre des faits.

Une enquête à double sens !

De la même manière que tu peux mener ta propre enquête en ligne grâce aux sources ouvertes, d'autres peuvent réaliser la même démarche, cette fois-ci **en ciblant tes données personnelles et des informations sur toi.** Cela peut aller de ton adresse personnelle, ta géolocalisation à un instant précis, ton collège ou lycée, tes lieux d'activité extrascolaires, etc. Avant de cliquer et/ou partager, autant te poser **quelques questions** sur ce que tu vois et **sur ce que les autres pourraient voir de toi !**

LE CLIC, CE N'EST PAS AUTOMATIQUE

Des questions à se poser avant de cliquer

J'ai reçu une information surprenante :

→ De qui vient-elle ?

→ Est-ce que la source de l'information est fiable ?

→ Est-ce que le message ou fichier envoyé est légal, envoyé avec le consentement de la ou des personnes concernées ?

→ Est-ce que la personne qui m'a envoyé l'information a vérifié sa véracité avant de la partager ?

→ Est-ce que je peux trouver et croiser des informations fiables pour confirmer ou infirmer l'information reçue ?

Je suis sur le point de publier ou partager une information sur moi :

→ À qui je les partage ? À mes proches, en mode privé ? À tout le monde, en mode public ?

→ Est-ce que l'on peut m'identifier ?

→ Est-ce que l'on peut déduire ou voir ma géolocalisation ?

→ Est-ce que l'on peut identifier les personnes avec qui je suis ?

→ Qu'est-ce que je dévoile de moi, de mes pensées, de mes opinions ?

→ À priori, serais-je encore à l'aise avec ce partage une heure après, un mois après, un an après ?

MAIS VOUS ÊTES QUI VOUS ?

Sur Internet, l'esprit critique, c'est automatique ! Ce qu'on t'envoie, ce que tu lis et partages mérite ton attention. Tu peux commencer par vérifier :

→ **Qui te parle ?**

Vérifier qui te parle en gardant à l'esprit qu'il est possible d'usurper une identité. On ne sait pas toujours qui est caché derrière un pseudo.

→ **Qu'est-ce que cette personne attend de toi ?**

Est-ce qu'elle veut te proposer un produit, un service, tenter d'en découvrir plus sur toi, tes habitudes, ton lieu d'habitation ? Le web se nourrit de données personnelles.

→ **Comment cette personne a-t-elle eu tes coordonnées ?**

Peut-être parce que tu as été identifié sur un groupe, un réseau social, une page dédiée, via un formulaire Internet ou autre. Au final, grâce aux informations que tu as semées de-ci de-là sur le web, elle t'a ciblé.

CHUT! EXPLORE est édité par Chut! Explore, association N° RNA W7512/0150. **Illustrations :** Adeline Schöne
CONTACT explore@chut.media / educnum@cnil.fr **ISSN** 3003-1596 **CPPAP :** 0125 G 96255 **PARUTION** Bimestriel avec Supplément.

CNIL.

UN OCÉAN DE DONNÉES

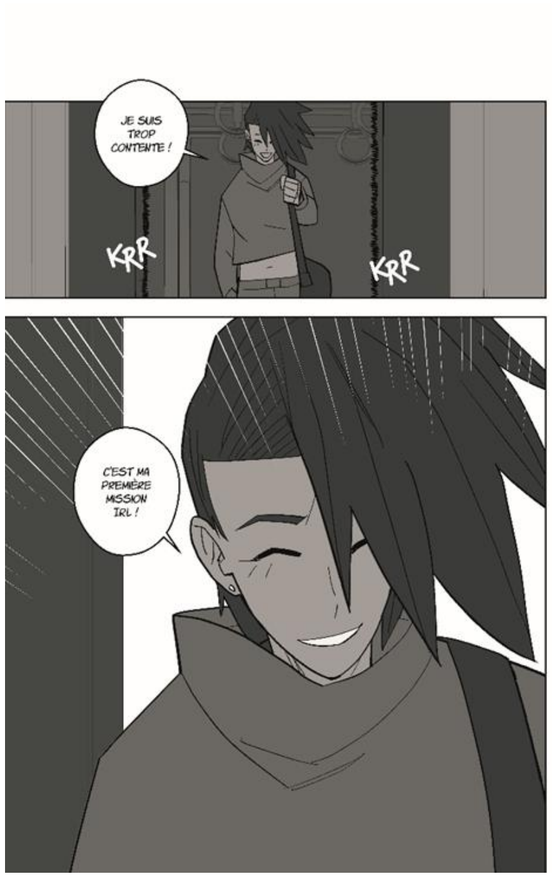
Livret

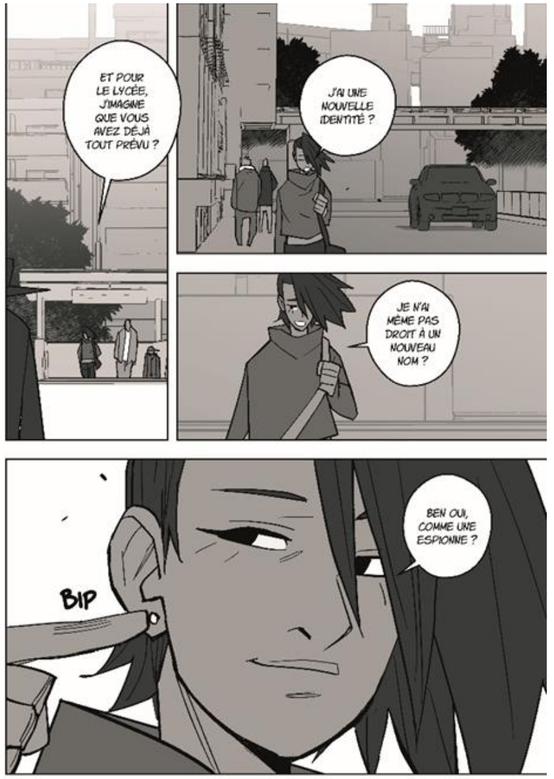
- Son 1er smartphone
- Géolocalisation
- Cyberharcèlement
- Service en ligne
- Cybersécurité
- Conseils parents
- Conseils enseignants

UN MANGA

- Manga type shonen
- Illustrateur : Grelin
- Scénariste : Faouzi Boughida
- Enquête menée auprès de lycéens : comment penser sa vie en ligne, protéger sa vie privée, construire son rapport aux autres…

- Sortie en 2025
- En français et en anglais





LA REVUE DES PARENTS

- Nos données personnelles valent de l'or pour les réseaux sociaux, et leur circulation met en danger enfants et adolescents. Comment reprendre le contrôle et mieux protéger leur vie privée ? Enquête.

- Retrouvez le dernier numéro de *la Revue des parents*, auquel la CNIL a participé. Le lien pour la consulter vous sera envoyé à l'issue du webinaire.

FantomApp

Se protéger sur les réseaux

CNIL.

Financé par l'Union européenne

UNE APPLICATION CONÇUE POUR ET AVEC LES ADOLESCENTS

→ Allers-retours dans les classes de collèges : écouter et prendre en compte la parole des adolescents

→ Choix du design et des fonctionnalités par les adolescents

CNIL.

3 FONCTIONNALITÉS

1. **Outils**

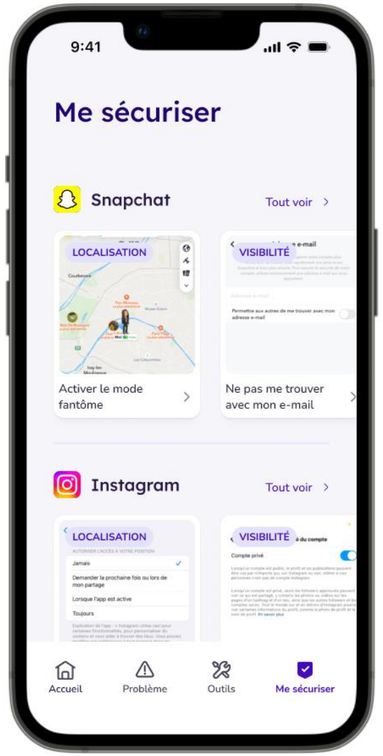
Tester son mot de passe
Flouter sa photo de profil
Tester son pseudo & sa bio

2. **Résolution de problèmes**

Effacer un contenu
Cyberharcèlement
Usurpation d'identité
Chantage sexuel
Piratage de compte
Arnaque

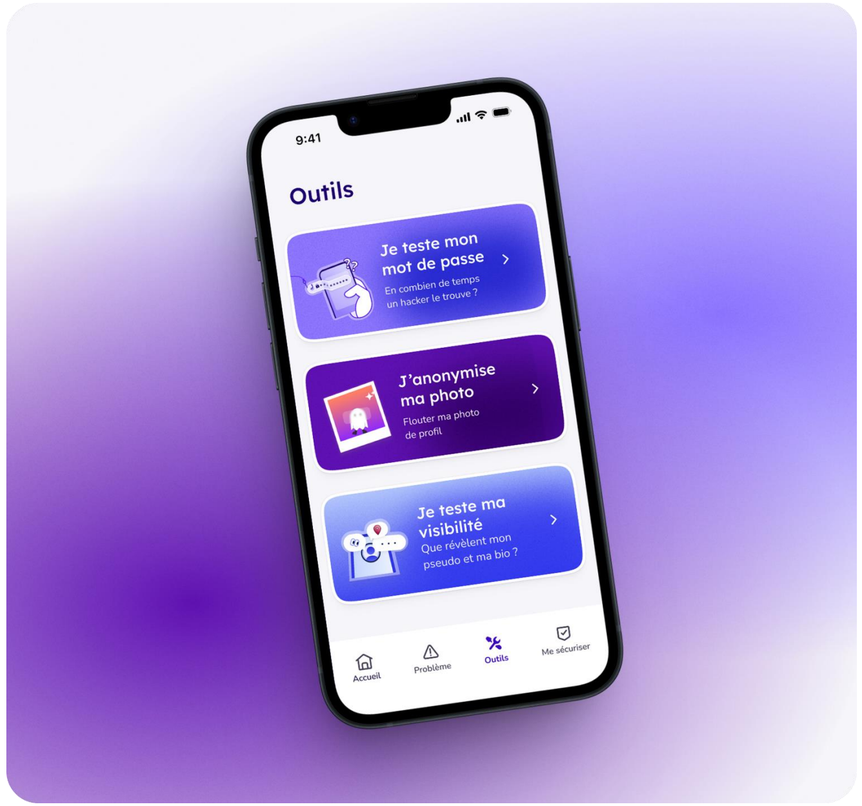
3. **Tutos paramètres**

Snapchat
X
Instagram
Whatsapp
Tiktok

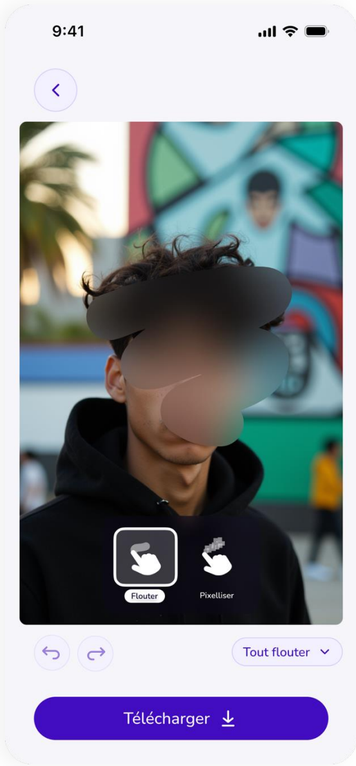


CNIL.

OUTILS



Tester mon mot de passe de manière ludique



Flouter ou pixeliser ma photo de manière ultra simple

Est-ce que mon pseudo ou ma bio contiennent des données personnelles ?

CNIL.

SOLUTIONS

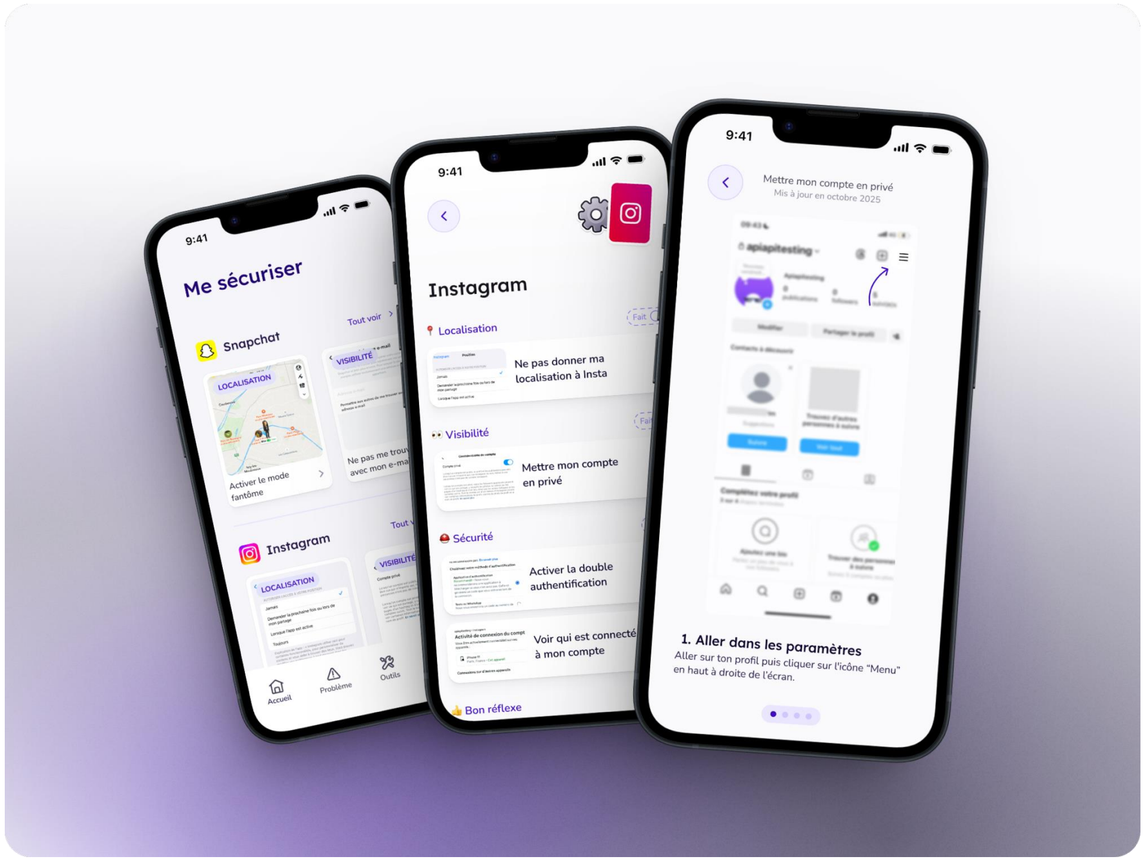
Pour chaque sujet :

- Définition : valider la situation vécue
- Message pour rassurer
- Pistes de solutions, détaillées

Les parcours prennent en compte les multiples situations dans lesquelles les adolescents peuvent se trouver. A chaque fois, c'est un chemin d'accès vers une résolution de problème.

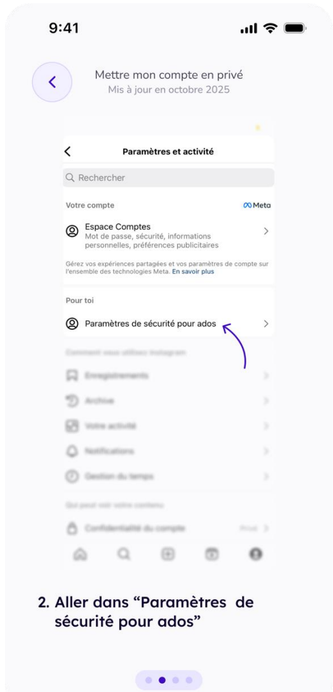
CNIL.

TUTOS

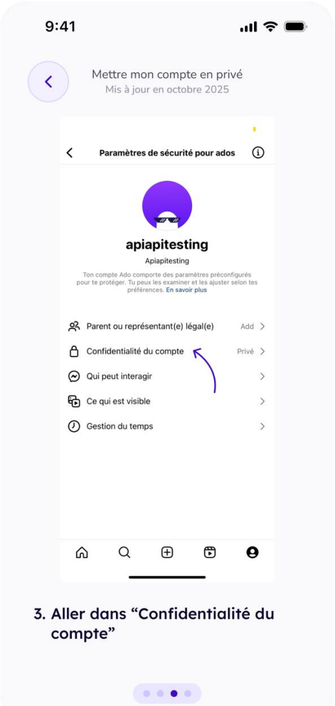


Pour chaque réseau social, le parcours « pas à pas » pour protéger sa vie privée en ligne

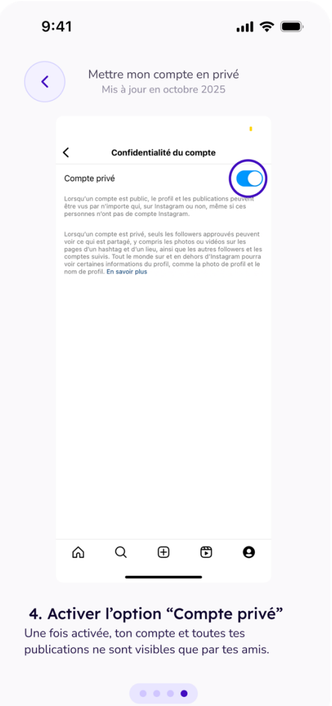
Possibilité de « checker » les étapes de protection lorsqu'elles sont activées



2. Aller dans "Paramètres de sécurité pour ados"



3. Aller dans "Confidentialité du compte"



4. Activer l'option "Compte privé"
Une fois activée, ton compte et toutes tes publications ne sont visibles que par tes amis.

CNIL.

Disponibilité

En ligne, sur le web
https://fantomapp.fr/

Disponible sur Google play

Disponible sur App Store