

MILLIONdata_BABY

L'antisèche !

Je souhaite sensibiliser toutes personnes face à des services numériques pour donner autonomie et protection.

J'ATTIRE L'ATTENTION SUR...

La **lecture de certaines cartes** : inviter les participants à lire les cartes et laissez-les se poser des questions ou partager une expérience qui fait écho avec la situation décrite.

Puis **partager le principe de la carte**, rapportée au faits réels ou à la pratique en question et des impacts que ça peut avoir.

LES MESSAGES QUE JE PARTAGE

Nos données sont nos données : **les prendre sans autorisation, c'est voler** !

En Europe, **vendre des données est interdit**.

Internet est comme une plage : quand on marche dessus, nous laissons des traces. Il y a des **outils pour effacer ces traces**. Mais les données se récupèrent aussi sur papier.

À chaque donnée demandé, nous devons : **être informé** sur l'utilisation de ces données, exprimé clairement que nous sommes d'accord, **avoir accès** à ces informations pour les **consulter**, les **modifier**, ou demander de les **supprimer**.

Toujours **vérifier qui nous demande nos informations personnelles**. Si vous recevez un email d'un ami ou d'une banque : appelez-les avant de cliquer.

L'entreprise ou le service public a pour obligation de protéger les données personnelles de ses utilisateurs pour éviter qu'elles ne soient volées, revendues ou falsifiées pour utilisation.

PHASE	DURÉE	À FAIRE
INTRO	10'	Questionner sur les données personnelles
PRÉSENTATION DU JEU	10'	Expliquer le principe du jeu à l'aide des cartes du premier chapitre Poser une application pour chaque participant et distribuer les cartes aux participants
DÉMARRAGE	15'	Déterminer qui commence la partie Questionner les participants sur leur rapport au numérique et aux données personnelles
DÉCOUVERTE DES CHAPITRES	6x10'	Expliquer le concept du chapitre Faire jouer un ou deux tours. Quand les participants sont prêts : on passe au chapitre d'après.
DÉBRIEF	15'	Demander aux participants ce qu'ils ont compris, retenu, avec quoi ils repartent. Partager des recommandations et outils pour se protéger.



Certaines cartes peuvent faire peur. La peur favorise les stratégies d'évitement (je préfère faire l'autruche plutôt que m'angoisser).

Notre conseil : dédramatiser en apportant un ton léger, en rire, pour favoriser la prise de conscience qui entraînera un changement de comportement progressif et la construction d'un discours vis à vis de leurs proches.

Antisèches - Intro, présentation et démarrage

1 - Intro

Échange autour des données personnelles

Qu'est-ce qu'une donnée personnelle ?

Les données personnelles permettent de vous identifier : votre nom, votre email, votre numéro de plaque d'immatriculation, votre taille, la couleur de vos yeux, etc.

Uniquement internet ?

Non ! Vos données personnelles commencent à la naissance et peuvent circuler sur des formulaires papier.

Y a-t-il des données qui ont plus d'importance que d'autres ?

Les données qui touchent à l'intimité d'un individu, dont l'utilisation pour un mauvais usage représente un risque élevé pour les personnes. (croyances, religion, origine, santé, sexualité, genre, etc.).

- le numéro de sécurité sociale (NIR)
- les données personnelles relatives aux condamnations pénales, aux infractions et aux mesures de sûreté.
- Les données des personnes mineurs

Quelle est la différence entre des données personnelles récoltées en France et aux États-Unis ?

En Europe : la collecte de donnée est encadrée par le RGPD, il est interdit de les vendre (on ne revend pas la couleur des yeux). Aux États-Unis, les données se vendent comme votre t-shirt ou vos chaussures. Des entreprises ont donc décidé d'en faire un commerce.

2 - Présentation du jeu

Le jeu million Data_Baby a pour ambition de montrer ces pratiques, les impacts sur la société, les lois, le rôle des associations, et les enjeux de la cybersécurité en 6 chapitres.

L'animateur ou animatrice montre le principe du jeu avec les cartes en expliquant : pour collecter des données, il me faudra donc une application ou un site en ligne, sur laquelle j'ajoute des façons de collecter des données personnelles.

"À quand remonte la dernière fois que vous avez donné votre adresse email ?"

3 - Démarrage

-> Questionner les participants sur leur rapport au numérique et aux données personnelles.

"Qu'est-ce que ça vous fait de savoir que des gens récupèrent vos données ?"

"En aviez-vous conscience ?"

-> Déterminer qui commence la partie : demander aux participants de regarder dans les smartphones (si participants équipés), pour déterminer qui a l'utilisation la plus importante.

Par exemple, regarder le temps journalier moyen passé la semaine dernière.

Chaque chapitre : une problématique

Chapitre 1 - Stage en vol de données personnelles

Facebook, Instagram, Tik Tok, Gmail, Candy crush, ChatGPT sont ils vraiment gratuits ? La réponse est Non. Pour financer la création de leur logiciels, les grands groupes se rémunèrent grâce aux données personnelles des utilisateurs : ils les collectent puis les revendent.

La collecte de donnée passent aussi par des objets connectés autre que le smartphone : la voix, les conversations, les heures à laquelle on utilise tel ou tel objet. Exemple : assistant vocal.

La responsabilité est bien celle de la personne qui demande aux machines de collecter et non la machine de la collecte des données. Si cet être humain est raciste, il va collecter les données en ce sens.

Chapitre 4 - Le réveil citoyen

Des personnes et organisations remettent en question ces pratiques et proposent des solutions : boycott, attaque en justice, défense des droits, outils et sensibilisation des publics, etc.

-> Certaines entreprises proposent des services pour enfants : les données des mineurs sont considérées comme les plus sensibles et nécessite une sécurité poussée.

-> Rendez-vous dans les antisèches des personnalités

Chapitre 2 - La concurrence fait rage

En l'absence de règles claires qui encadrent les pratiques commerciales, les entreprises vont utiliser leurs méthodes pour collecter des données et légitimer leur utilisation.

-> Interdire l'accès d'un site si la personne utilise un bloqueur de publicité

-> Utilisation de faux profils et de fake news

-> Faire de la recherche et développement sur des technologies permettant de collecter plus de données (5G, smart cities, etc)

Chapitre 5 - Bye Bye démocratie

La collecte des données intéressent aussi les gouvernements pour contrôler les populations, en utilisant des logiciels espions qui permettent de surveiller n'importe qui sans qu'il le sache, ou récupérer les données que les GAFAM collectent.

Les données sont partout. Les hackers utilisent leurs compétences pour identifier les failles de sécurité pour aller récupérer la donnée. Certains proposeront aux organismes de sécuriser leurs failles, d'autres feront du chantage et demanderont une rançon.

Une des méthodes pour sécuriser les données est de les chiffrer.

Chapitre 3 - La justice s'en mêle

Des lois régulent la collecte et la gestion des données personnelles depuis 1978 (la CNIL)

Pour les entreprises qui ne respectent pas les lois, des sanctions existent appliquées par la CNIL.

Là encore, des méthodes pour les contourner existent : corruption, lobbying pour faire évoluer les lois, paradis fiscaux.

Chapitre 6 - Wild Wild Web

Les avancées technologiques peuvent nous faire oublier que c'est bien l'être humain qui est responsable de sa folie et non la technologie.

Certaines personnes souhaitent transférer leurs cerveaux dans des super ordinateurs pour vivre éternellement, Microsoft qui propose un chatbot pour continuer à parler avec une personne décédée pour récupérer vos conversations, Elon Musk qui s'intéresse à la Lune pour y mettre ses data centers pour éviter les lois sur la protection des données personnelles ou souhaite intégrer des puces dans les cerveaux pour contrôler les émotions et les pensées.

Antisèches des personnalités

Lanceurs d'alertes

Surveillance de masse et contrôle des populations

Edouard Snowden, Brittany Kaiser, Sophie Zhang sont des lanceurs d'alertes : ils ont révélé au monde entier les pratiques des gouvernements qui collectent et utilisent les données des gens sans leur consentement, aidés par les réseaux sociaux entre autre, afin de surveiller et contrôler les populations.

Bruce Shneier, Shoshana Zuboff, Aaron Swartz : cryptologue, spécialiste en sécurité informatique, chercheurs, écrivains engagés dans la protection des données personnelles et des libertés. Tous et toutes, à leur échelle, ont participé à des recherches sur l'impact des données personnelles, qu'ils défendent fermement.

IDFright, institut des droits fondamentaux numériques

Défendre la liberté des citoyens lors des décisions politiques

L'institut des droits fondamentaux numériques travaille sur la protection de la liberté des citoyens, intervient en accompagnant des décisions politiques pour une gestion éthique des données en faveur des citoyens et de l'intérêt général, et en réalisant des publications issues de recherche.

UFC que choisir, 60 millions de consommateurs, etc...

Dénoncer les pratiques illégales et trainer les entreprises devant les tribunaux

UFC que choisir et 60 millions de consommateurs sont des associations qui ont pour but de dénoncer les pratiques illégales, non conformes au RGPD, et porter plainte pour protéger les intérêts des citoyens.

Julian Assange et Wikileaks

Libération des informations contrôlées par les États

Julian Assange, informaticien, hacker éthique, cybermilitant et journaliste

Il défend l'idée que les États sont, d'une part, en mesure de contrôler une grande partie des communications de leurs citoyens, et qu'ils tentent, d'autre part, de garder secrets de larges pans de l'information dont ils disposent.

Alors il fonde Wikileaks, plateforme pour partager ces informations confidentielles, dont des révélations sur la manière dont les États-Unis et leurs alliés mènent la guerre en Irak et en Afghanistan.

Il était jusqu'à récemment prisonnier politique en Angleterre. Les États-Unis souhaitent une extradition afin de lui faire sa fête, mais il est libre !

La quadrature du net, NOYB

Protéger les données personnelles face aux lois liberticides

Association composée d'avocats, juristes et bénévoles qui luttent depuis quinze ans pour protéger les libertés et les droits fondamentaux à l'ère du numérique.

Elle intervient lors d'examen de lois et dépose des plaintes à l'encontre d'entreprises qui ne respectent pas le RGPD.

Elle a déposé plainte contre les GAFAM a été déposé en 2018, une amende de 746 millions d'euros a été appliqué à l'encontre d'Amazon.

Antisèches des outils numériques

Un cookie : qu'est-ce que c'est ?

Un cookie est un petit fichier informatique, un traceur.

Il est déposé sur votre ordinateur et peut être lu par exemple lors de la consultation d'un site internet, de la lecture d'un courrier électronique, de l'installation ou de l'utilisation d'un logiciel ou d'une application mobile.

Les cookies existent pour tous les types de terminaux utilisés (ordinateur, smartphone, liseuse numérique, console de jeux vidéos connectée à Internet, etc.).

L'utilisation de ces outils est en principe soumise à votre consentement car il permet de vous tracer et donc d'obtenir des données sur vous et sur vos comportements.

Seuls certains cookies strictement nécessaires au fonctionnement du site peuvent être déposés sans consentement (source : [CNIL](#)).

Réseaux sociaux : comment supprimer mon compte ?

En principe, tous les sites internet vous proposant de créer un compte doivent également vous proposer une procédure pour le supprimer et donc supprimer vos données.

Si après un délai d'un mois, votre compte n'a pas été supprimé, vous pouvez adresser une plainte à la CNIL. Joignez à notre formulaire de plainte la copie de votre au courrier au responsable du réseau social et sa réponse éventuelle (source : [CNIL](#)).

Internet est un environnement dangereux

Vous méritez le respect. Vous devez faire passer votre sécurité avant tout le reste.

N'ajoutez que des gens que vous connaissez, ne prenez aucun risque, recoupez les informations qu'on vous donne, ne faites pas confiance.

N'envoyez pas d'informations sur vous à des inconnus. N'envoyez pas de photos de vous, elles pourraient être utilisées pour vous nuire et seront presque impossibles à faire supprimer ensuite. Suivez votre instinct, si quelque chose cloche, coupez tout contact.

Réseaux sociaux : comment limiter les risques pour ma vie privée ?

Sur un réseau social, il est souvent difficile de distinguer ce qui est public de ce qui reste privé, voici quelques conseils :

Soyez méfiants et gardez certaines informations absolument confidentielles : ne dévoilez pas trop de votre vie privée sur internet, ne partagez pas vos informations avec n'importe qui ;

Prenez le temps de régler les paramètres de confidentialité de votre profil : empêchez l'apparition de votre profil dans les moteurs de recherches, limitez ou compartimentez vos "amis" (vos contacts).

ne restez pas connecté quand vous quittez un site, pensez à cliquer sur "Déconnexion". Supprimer les profils que vous n'utilisez plus depuis plusieurs années (source : [CNIL](#)).

Publicités et spams

Règle de base pour recevoir moins de publicités : lors d'un achat, d'un abonnement, d'une demande de catalogue ou d'un devis etc., ne communiquez que des informations indispensables.

Par exemple, pour un achat d'électroménager, rien ne vous oblige à donner votre date de naissance, votre profession, votre numéro de téléphone ou l'identité des personnes qui vivent chez vous.

Inscrivez vous sur des listes d'opposition à la publicité (source : [CNIL](#)).

Conclusion et conversation avec les sceptiques

Conclusion : actions et outils

VPN et adresse IP : ProtonVPN

Navigateurs : Firefox, firefox focus, brave

Messageries : Signal, protonmail, infomaniak

Moteur de recherche : Duckduckgo

Envoyer des documents : Securedrop

Bloqueur de pub : U block, adnauseam

Cartes : Open Street Map

Visioconférence : Big Blue Button

Réseaux sociaux : Mastodon

Mot de passe : changer régulièrement, en créer des différents et des compliqués, et utiliser un gestionnaire de mot de passe libre : Keepass

// La meilleure donnée, c'est celle qu'on ne fabrique pas : il n'appartient qu'à vous de changer d'outil, et d'en consommer moins.

- Je désactive la géolocalisation
- J'active le chiffrement de mes données
- Je supprime mes données si elles n'ont pas d'intérêt à être stockées
- Je renforce les paramètres de confidentialités de mes comptes et de mon mobile
- Je me demande à quels intérêts je sers en utilisant telle ou telle application ?
- Je regarde les outils open source (qui appartiennent aux populations)

“De toute façon ça change rien de partager ses données, c'est pas moi qui vaît avoir un impact sur les GAFAM...”

Ça change tout !

Les données personnelles sont considérées comme le nouveau pétrole, avec l'idée qu'on a juste à se servir et à les revendre pour gagner de l'argent.

Cette idée est dangereuse.

Si le modèle d'affaire des Gafams est basé sur la collecte de données, moins on leur donne, plus on leur met des bâtons dans les roues.

C'est vraiment efficace ! La preuve ?

- Ils dépensent des millions d'euros et de dollars en lobbying.
- Ils menacent de couper l'accès en Europe dès que l'Union Européenne veut créer de nouvelles lois.
- Ils se croient au dessus des lois.

Les Gafams sont tellement puissants qu'ils dictent leur façon de voir le monde (Un Monde de Mâles blancs), et nous imposent leur vision de l'égalité, de l'écologie, d'une société qui autorise les armes et accepte la très grande pauvreté...

Utilisez ou non leurs APPLIS devient un acte politique.

“Moi je n'ai rien à cacher...”

Prétendre que votre droit à une sphère privée n'est pas important parce que vous n'avez rien à cacher n'est rien d'autre que de dire que la liberté d'expression n'est pas essentielle car vous n'avez rien à dire.

“T'es un peu alarmiste il faut se détendre”

N'oublions pas que les lois peuvent changer selon l'évolution des mentalités ou l'arrivée d'un nouvel acteur au pouvoir.

Des lois, aujourd'hui centrées sur la sécurité, qui autorisent une surveillance de masse pour se protéger d'actions terroristes, pourraient demain devenir des outils dans les mains d'un dirigeant politique souhaitant surveiller une minorité religieuse, ethnique, sexuelle et ou des opposants politiques.

Exemple : qui aurait cru que les USA pourraient revenir sur le droit à l'IVG ? Et que la police américaine utiliserait les nouvelles technologies pour empêcher les femmes de disposer de leur corps ? Quand bien même cela provoque la mort.