4 MES DONNÉES, MON CHOIX !

Article 12 de la Déclaration universelle des droits de l'Homme (1948) :

Toute personne a droit au respect de sa vie privée et de sa réputation.

LE SAVIEZ-VOUS ?

Selon une étude de l'agence *Heaven* (2024), 42 % des 18-25 ans en France utilisent l'IA tous les jours, et 80 % au moins une fois par semaine. Et encore, ces chiffres ne tiennent pas compte de toutes les fois où ils utilisent l'IA… sans même le savoir.

Prenons quelques exemples fictifs d'une journée ordinaire.

- D'abord, on déverrouille son smartphone avec la reconnaissance faciale. Une IA analyse les traits du visage (distance entre les yeux, forme du nez, ligne de la mâchoire…). Ce sont des données biométriques, parmi les plus sensibles. D'après un rapport d'Europol (avril 2025), certaines IA sont désormais capables de générer de faux visages ou empreintes pour tromper ces systèmes. Un vrai risque pour notre sécurité et notre vie privée.
- Plus tard, on entre dans un bureau de tabac, et on croise peut-être le *MyCheckr Mini*, un petit boîtier équipé d'une caméra. Il utilise l'IA pour estimer l'âge des clients afin de limiter la vente aux mineurs de certains produits (alcool, tabac, produits de vapotage, jeux d'argent et de hasard). Lumière verte : c'est bon. Rouge : pièce d'identité exigée. Sauf que, selon la CNIL (Commission nationale de l'informatique et des libertés), l'appareil peut scanner tous les visages, même ceux venus acheter…des chewing-gums. Or, le droit européen interdit de collecter plus de données que nécessaire, afin de protéger la vie privée des citoyens et de limiter les abus.
- En fin de journée, on décide de poster une photo avec ses amis sur *Instagram*. Là encore, toutes les données, même les plus intimes, sont récupérées par *Meta*, la maison mère de *Facebook* et *Instagram*. Depuis le 27 mai 2025, l'entreprise récolte les données de ses usagers (à l'exception des comptes de mineurs et de ceux qui ont rempli un formulaire pour s'y opposer) pour entraîner ses programmes d'intelligence artificielle.

Ces exemples montrent que nos données personnelles ou notre sécurité ne sont pas toujours bien protégées.

Pour répondre à ces enjeux, la CNIL a publié en février 2025 de nouvelles recommandations. Objectif : garantir le respect du RGPD, le règlement européen qui protège les données personnelles. Elle propose par exemple d'informer clairement les personnes lorsque leurs données servent à entraîner une IA, et de leur permettre de les corriger ou les supprimer. Un véritable défi technique !

Au niveau international, face aux progrès rapides des entreprises privées du secteur, dont l'objectif principal reste le profit, la mise en place d'une réglementation devient essentielle. À ce jour, seule l'Europe a instauré un cadre législatif avec l'*Artificial Intelligence Act*, fondé sur le principe d'une IA digne de confiance. Ce texte ambitionne de faire de l'Union européenne la pionnière d'une intelligence artificielle légale, éthique et robuste.

4 MES DONNÉES, MON CHOIX !

Monstres et compagnie : Cherche et trouve

Pour mieux comprendre ce dessin, essaie de répondre aux questions suivantes :

Dlog (Tunisie) - 2024

1 – Que représentent les cinq têtes du monstre ?

.....

.....

.....

.....

.....

.....

.....

2 – Cherche dans ce dessin de Dlog :

2 symboles de l'argent

4 symboles liés aux utilisations d'internet et à la technologie

Le symbole de la censure (limitation de la liberté d'expression)

3 symboles de données personnelles des utilisateurs d'internet

3 – Que représente le quadrillage noir recouvrant la Terre dans le dessin ? À quoi cela fait-il référence ?

.....

.....

.....

4 – À partir de tes réponses, quelle est ton interprétation du dessin ?

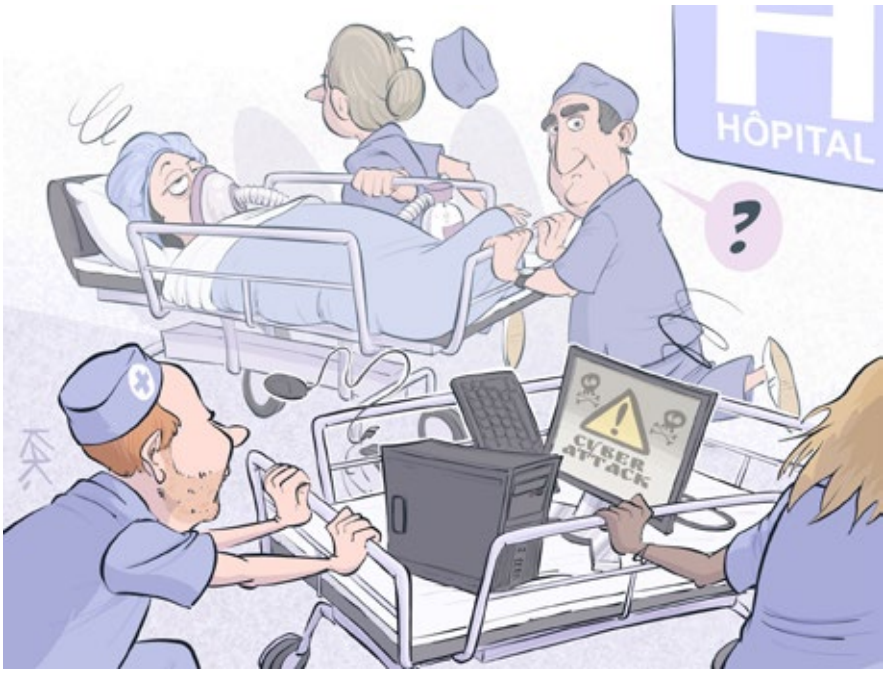
.....

.....

.....

4 MES DONNÉES, MON CHOIX !

Cyber-attaques : Quiz



Kak (France) - 2021

Dans un monde de plus en plus connecté, les données personnelles (par exemple, le nom et le prénom, le numéro de sécurité sociale, l'adresse postale ou mail, une empreinte, un identifiant de connexion informatique…) sont des trésors précieux, qui deviennent la cible de pirates informatiques. Les hôpitaux ont ainsi été victimes de cyberattaques ces dernières années, en France et ailleurs dans le monde, comme le montre ce dessin de Kak.

Réponds à ces questions pour en savoir plus sur le sujet :

1 – Entre 2021 et 2023, quel a été le pays européen le plus touché par des cyberattaques dans le secteur de la santé ?

La France | L'Allemagne | L'Italie

2 – Une des menaces les plus importantes en termes de cyberattaques est le rançongiciel.

À partir de quels mots ce terme a-t-il été créé ?

.....

.....

Peux-tu en déduire en quoi consiste ce type d'attaque ?

.....

.....

.....

.....

.....

.....

3 – Combien d'attaques par rançongiciels ont touché des établissements de santé en 2024 en France ?

13 | 40 | 71

4 – En 2024, le centre hospitalier d'Armentières, dans le Nord de la France, a été victime d'une cyberattaque. Combien de patients ont été concernés par la violation de leurs données ?

30 000 | 150 000 | 230 000

5 – D'après toi, quels peuvent être les risques pour les patients d'une violation de données, qui compromet l'intégrité, la confidentialité ou la disponibilité de leurs données personnelles ?

.....

.....

.....

.....

4 MES DONNÉES, MON CHOIX !

Tous surveillés ? Dessin sans bulle

D'après **Chappatte** (Suisse) - 2019

Imagine le texte de la bulle dans ce dessin de Chappatte :

.....

.....

.....

.....

4 MES DONNÉES, MON CHOIX !
FICHE RÉPONSES

Monstres et compagnie : Cherche et trouve

1 – Les cinq têtes du monstre représentent les **logos des GAFAM** (acronyme des géants du Web). De gauche à droite : le « G » de ***Google*** ; la pomme d'***Apple*** ; le « f » de ***Facebook*** (aujourd'hui *Meta*) ; la flèche jaune (représentant également un sourire) d'***Amazon*** ; les quatre carrés, rouge, vert, bleu et jaune de ***Microsoft***, surmontés d'une couronne en forme de « M ». Basées aux États-Unis, ces entreprises sont les plus puissantes du secteur du numérique mondial.

2 –

- 2 symboles de l'argent
  Plusieurs réponses sont possibles. Le monstre tient une **liasse de billets** dans sa main gauche, et une autre est plantée dans les dents de la tête « *Google* ». En haut à droite, le serpent dont la langue représente le logo « *Amazon* » tient un **sac de billets**. La tête « *Facebook* » tient dans son bec un **emoji « dollars »**. Sur chacun de ces éléments, on remarque le symbole du dollar américain.
- 4 symboles liés aux utilisations d'internet et à la technologie
  Les têtes et les bras des monstres tiennent plusieurs icônes ou objets liés à internet et à la technologie. Un **chargeur de téléphone** sort de la bouche de la pomme représentant « *Apple* », de laquelle pend aussi l'**icône rouge** de la localisation. En haut à gauche, au sommet du « G », on peut voir un **curseur**, ou flèche de navigation. À droite, le monstre tient dans sa main le **symbole USB**.
- Le symbole de la censure (limitation de la liberté d'expression)
  La tête « *Facebook* » tient une **paire de ciseaux**, généralement représentée par les dessinateurs et dessinatrices de presse pour symboliser la censure. Au XIXe siècle, le personnage d'Anastasie, une dame portant de grands ciseaux, était justement utilisé par les dessinateurs pour représenter la censure. Son nom vient du pape Anastase Ier, qui a interdit plusieurs livres car ils ne correspondaient pas à la pensée chrétienne.
- 3 symboles de données personnelles des utilisateurs d'internet
  Au centre, un tentacule du monstre tient le symbole de la protection des données : un **cadenas sur fond bleu**. En bas à gauche, le monstre tient entre ses griffes un **smartphone** avec une silhouette représentée sur l'écran (pouvant être une photo ou un contact). En bas à droite, il tient un **dossier sur lequel est écrit « data »**, qui signifie « données » en anglais.

3 – La Terre est recouverte par **un cercle contenant des lignes horizontales et verticales : cela représente les méridiens et parallèles** du globe, image également utilisée comme symbole du ***World Wide Web***, aussi appelé la toile (le système permettant d'accéder aux ressources d'Internet, qui sont interconnectées entre elles). La façon dont il est dessiné peut par exemple faire penser aux barreaux d'une cage.

4 – La dessinatrice évoque dans ce dessin le **pouvoir économique des GAFAM et leur emprise sur les données personnelles des utilisateurs**.
En choisissant la figure du monstre, elle peut vouloir faire passer l'idée de peur, de danger.
Mais à partir des éléments que tu as trouvés, tu es libre d'avoir ta propre interprétation du dessin.

4 MES DONNÉES, MON CHOIX !
FICHE RÉPONSES

Cyber-attaques : Quiz

1 – Selon l'ENISA (agence de l'Union européenne pour la cybersécurité), entre 2021 et 2023, **la France** a été le pays européen le plus touché par des cyberattaques dans le secteur de la santé (dans les hôpitaux, les laboratoires, les mutuelles de santé, les organismes publics de santé et les industries pharmaceutiques). Viennent ensuite l'Espagne et l'Allemagne. L'Italie est en 5e position.

Cela s'explique notamment par le fait qu'en France, les établissements de santé doivent obligatoirement déclarer les incidents de sécurité qui touchent leur système d'information (l'ensemble des ressources et outils qui permettent de collecter, stocker, traiter et diffuser les informations au sein d'un établissement). Ceux-ci sont donc davantage comptabilisés que dans d'autres pays européens.

2 – Le terme « rançongiciel » est une contraction des mots « **rançon** » et « **logiciel** ».

Il s'agit d'implanter un logiciel malveillant dans un système d'information, qui chiffre les données (c'est-à-dire qui les rend illisibles), puis de réclamer une rançon pour rendre les données de nouveau lisibles, et/ou pour ne pas les divulguer. Au-delà de la rançon, le but des personnes menant ces attaques est souvent de voler des données médicales et personnelles dans le but de les revendre, notamment sur les darknets (réseaux volontairement anonymisés, non indexés par les logiciels de référencement et les moteurs de recherche).

3 – Selon un rapport de l'Agence du numérique en santé, **40** attaques par rançongiciels ont touché des établissements de santé français en 2024. Ce chiffre est en hausse par rapport à 2023, mais les capacités de surveillance et de réponse des hôpitaux s'améliorent.

S'ils ne sont pas des cibles privilégiées par les pirates, les hôpitaux s'avèrent plus vulnérables aux cyberattaques que d'autres types d'établissements, notamment parce que leur système d'information est complexe et interconnecté. Les hôpitaux utilisant de plus en plus le numérique, de nombreuses applications échangent des informations entre elles pour gérer la comptabilité, les dossiers de patients informatisés, la prise de rendez-vous en ligne, etc. Cela pourrait être accentué par le développement de l'usage d'objets connectés pour la surveillance des patients (objets qui collectent, échangent et analysent des données pour automatiser des tâches).

4 – Dans la nuit du 10 février 2024, dix gigaoctets de données concernant **230 000** patients ont été dérobés au centre hospitalier d'Armentières (59). L'hôpital a notamment dû fermer le service des urgences durant trois jours pour garantir la sécurité des patients et rétablir le système d'information.

Les cyberattaques ont régulièrement un impact sur le bon fonctionnement des hôpitaux qui en sont victimes (opérations retardées, personnel ne pouvant plus accéder aux dossiers des patients, retour aux tâches manuelles en remplacement de celles habituellement automatisées et informatisées…).

5 – Les établissements de santé gèrent des données de santé très sensibles, à caractère personnel (des informations sur l'identité des patients, leur numéro de sécurité sociale, des résultats d'analyse…). L'un des principaux buts des cyberattaques est donc de **voler ces données pour les revendre**. Des pirates peuvent ensuite les utiliser pour faire du hameçonnage, c'est-à-dire envoyer un message frauduleux à une personne, qui lui paraîtra réaliste (car il viendra soi-disant de son médecin par exemple), dans le but de l'arnaquer. Ces données peuvent aussi être utilisées pour des usurpations d'identité.

4 MES DONNÉES, MON CHOIX !
FICHE RÉPONSES

Tous surveillés ? Dessin sans bulle

Chappatte (Suisse) - 2019
(« ça fait une paye » : expression signifiant « ça fait longtemps »)

Appliqué aux caméras de surveillance, un système de reconnaissance faciale a pour but de rechercher et identifier en direct une personne en particulier, dans la rue par exemple. Cela est déjà une réalité dans certains pays du monde, principalement dans des régimes autoritaires (Russie, Iran, Ouganda, Venezuela…). En Chine par exemple, cette technologie est utilisée par le gouvernement pour contrôler au quotidien la population, notamment la minorité ouïghoure.

En France, ce type de dispositif est actuellement interdit. Durant la période des Jeux olympiques et paralympiques de Paris en 2024, des caméras pilotées par un système d'intelligence artificielle ont été testées dans la capitale et dans des villes d'Île-de-France, notamment près des lieux de compétition ou dans le métro. Cela s'appelle la vidéosurveillance algorithmique. La très grande quantité d'images filmées par les caméras est analysée par des algorithmes entraînés à détecter des comportements ou situations définis comme pouvant être suspects (personnes au sol, objets abandonnés, mouvements de foule, présence d'une arme…), et non directement des personnes, comme c'est le cas pour la reconnaissance faciale.

L'organisation *Amnesty international* a néanmoins alerté sur l'usage de la vidéosurveillance algorithmique, notamment concernant les biais discriminatoires des données utilisées pour entraîner les algorithmes : comment est défini un comportement « anormal » ou « suspect » ? Cela pourrait-il concerner une personne sans abri allongée dans la rue, ou une personne en situation de handicap ayant une démarche différente ?