JUIN 2023 | NUMÉRO 1

LE LEXIQUE NUMÉRIQUE

CODE. X VERSE

BACLET SOPHIE
MOUTIER FRANÇOIS
DESCHAMPS NICOLAS
MORIO RAPHAEL
RECULET VALENTIN

Education
Citoyenneté
Numérique

Crajep Hauts-de-France

Financement dans le cadre de la réponse de l'Union à la pandémie de COVID-19

UNION EUROPÉENNE

l'Europe s'engage en Hauts-de-France avec le FEDER

RÉGION ACADÉMIQUE HAUTS-DE-FRANCE

À propos

Un lexique est un outil pratique pour trouver la définition d'un mot, comprendre sa signification ou aider à la traduction d'un mot d'une langue à une autre. On peut dès lors *a priori* s'étonner de la parution d'un lexique numérique. Il semble toutefois que le jargon numérique peut être apparenté à une nouvelle langue. En effet Internet a constitué une véritable révolution tant dans nos usages que dans notre langage. Si la viralité d'Internet n'est plus à prouver, c'est également une viralité des néologismes numériques qui doit être soulignée. Régulièrement de nouveaux termes apparaissent pour appréhender des usages et phénomènes qui souffraient jusqu'alors d'un manque de définition. La maîtrise de ces néologismes est toutefois un préalable à une participation active des individus aux nouveaux sujets de société que posent le numérique. En définitive **la mise en lumière de la culture numérique est susceptible de renforcer le pouvoir d'agir des citoyens.**

Ce lexique privilégie une approche critique du numérique. Ainsi l'horizontalité des échanges permis par la *blockchain* et la *cryptomonnaie*, la menace causée par la *censure* des *plateformes numériques* sur les activistes et les militants ou les contours possibles de la *surveillance* à l'ère du numérique constituent des enjeux éminemment démocratiques devant être compris et maîtrisés par les citoyens.

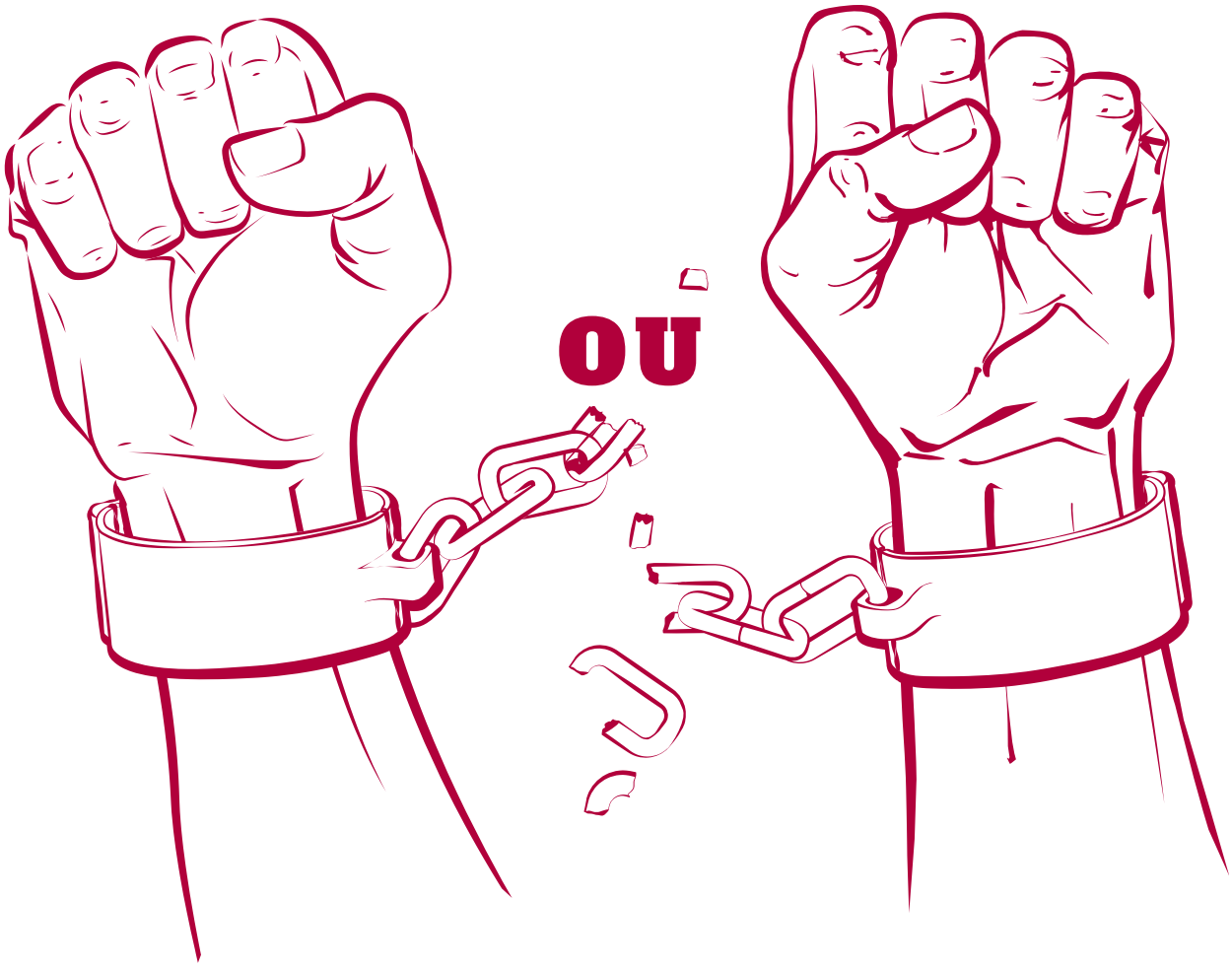
Le lexique numérique est basé sur la Recherche-Action du Projet Éducation à la Citoyenneté Numérique (ECN). Grâce à des entretiens et des actions expérimentales, les personnes rencontrées au cours d'une année et demie sur le territoire des Hauts-de-France ont eu à coeur de nous faire part de leurs difficultés à appréhender l'environnement numérique. Loin de se restreindre aux nouveaux termes et tendances émergentes, ces publics nous ont également pointé du doigt la difficulté de comprendre avec précision et clarté des notions employés quotidiennement par les médias tels que *données personnelles*, *hackeur* ou encore *cyberattaque*. Cet ouvrage leur est naturellement dédié.

Loin de se restreindre à une édition dans nos seules structures internes, l'équipe ECN a souhaité diffuser cet ouvrage largement. Qu'il s'agisse d'ouvrir le dialogue entre un parent et son enfant, de faciliter la compréhension d'une matière riche d'anglicisme pour un public non anglophone ou de présenter le numérique sous une autre acception que le caractère mathématique, analogique et technologique : il nous semble que ce lexique peut être placé entre les mains de toutes personnes ayant un intérêt pour le cyberespace.

SOMMAIRE

A

AFFRANCHISSEMENT



ASSERVISSEMENT

ABONNEMENT

\a.bɔn.mɑ̃\

Dans le domaine du numérique, les abonnements se sont démultipliés puisqu'ils constituent un moyen de monétisation pour les contenus en ligne.
Les abonnements peuvent être **payants** ou biens **gratuits**.

- Dans le cadre d'un abonnement payant, il s'agit d'apporter un financement direct en l'échange d'une prestation de services, d'actualités ou de produits. Les abonnements à la presse écrite libre relèvent généralement d'abonnements payants.

- Dans le cadre d'un abonnement gratuit, il s'agit de visibiliser l'adhésion d'une personne (abonné) à un contenu ou un service accessible en ligne. Sur la plateforme Youtube, il est par exemple possible de s'abonner à un certain nombre de chaînes sans pour autant souscrire à une contrepartie financière. Les abonnements gratuits ont largement transformé la logique marchande d'Internet en permettant de mesurer l'engagement des abonnés mais également de collecter leurs données personnelles afin de produire des recommandations de contenu ciblées. A l'inverse un viewer sera une personne qui regarde une vidéo sur une plateforme numérique sans toutefois s'y abonner.

ALGORITHME

\al.go.ʁitm\

Le concept d'algorithme provient du mathématicien persan du IXème siècle Al-Khwârizmî et définit une suite logique d'étapes et d'instructions à suivre dans l'objectif de résoudre un type de problème déterminé. Ainsi un algorithme fonctionnel produira systématiquement le résultat attendu.

Parfois les algorithmes sont illustrés à travers l'exemple d'une recette de cuisine : en suivant minutieusement les ingrédients et étapes de la recette, nous arriverions systématiquement au même résultat. Si suivre scrupuleusement la recette d'un gâteau au chocolat permettra toujours d'obtenir un gâteau au chocolat : son goût pourra néanmoins sensiblement différer en fonction de la qualité des ingrédients, du mode de cuisson...

C'est pourquoi il semble préférable de comparer un algorithme à la résolution d'un casse-tête.

La finalité n'est ici empreinte d'aucune subjectivité : si le casse-tête est résolu alors l'algorithme est fonctionnel. Un algorithme performant sera à la fois rapide et précis. Dans le domaine numérique, un programme est un algorithme qui indique à l'ordinateur sous forme de langage informatique les différentes étapes et tâches à suivre pour s'exécuter correctement. Il existe différents types de fonctionnement pour les algorithmes.

ALGORITHME

Un algorithme peut :

- sous-diviser un problème en plusieurs petits problèmes plus faciles à solutionner
- tester toutes les solutions possibles afin de trouver la meilleure
- apprendre à partir des données qui lui sont soumises afin de s'améliorer sans intervention humaine

Les réseaux sociaux ainsi que les services de streaming fonctionnent à l'aide d'algorithmes qui vont permettre la classification des contenus sur les pages d'accueil et le tri des recommandations pour chaque profil. Connaître la logique algorithmique constitue dès lors une forme d'empowerment à l'ère du numérique : une meilleure maîtrise des algorithmes permet en effet de basculer d'utilisateur passif auquel des contenus sont soumis à utilisateur actif ayant une influence et un contrôle sur ses recommandations.

La difficulté est toutefois matérialisée par le fait qu'aujourd'hui de nombreux algorithmes sont considérées comme des « boîtes noires » à propos desquels on ne connaît pas véritablement les étapes et instructions alors qu'ils sont susceptibles d'influencer les internautes économiquement, politiquement ou encore idéologiquement. Au delà des recommandations sur les plateformes numériques, les algorithmes sont également à l'origine de décisions en matière d'éducation, de santé, d'emploi ou encore de justice qui peuvent creuser les inégalités sociales, raciales ou encore sexistes. C'est pourquoi l'ethical by design vise à conférer plus de moralité et d'éthique aux décisions algorithmiques dès leur conception.

ANONYMAT

\a.nɔ.ni.ma\

L'anonymat sur Internet relève de la gageure tant il est difficile – pour ne pas dire impossible – de ne laisser aucune trace de sa navigation sur la toile. L'identification des internautes est en effet rendue possible par leurs adresses IP : une suite de chiffres qui est propre à chaque équipement informatique et attribué par un fournisseur d'accès à Internet.

Les enjeux liés à l'anonymat sur Internet sont très souvent au cœur des débats et polémiques liés au numérique. Généralement il est argué que sous couvert d'anonymat le cyberharcèlement, les discours de haine, l'apologie et la négation d'actes de terrorisme, l'incitation à la violence, la pédocriminalité ou encore la propagation de fausses informations sont largement facilités.

En France depuis la loi pour la confiance dans l'économie numérique (LCEN) - loi n°2004-575 du 21 juin 2004 et le code des postes et des communications électroniques : les fournisseurs d'accès à Internet sont tenus de détenir et de conserver les données permettant l'identification des individus afin de poursuivre et réprimer les individus ayant commis une infraction en ligne. En résumé les débats faisant état d'une levée nécessaire de l'anonymat sur Internet sont sujetd à controverse dans la mesure où la loi française prévoit déjà une identification possible des internautes.

Des procédés techniques peuvent toutefois être utilisés par les internautes pour rendre plus difficile cette identification. C'est notamment le cas des Virtual Private Network (VPN) puisque la localisation précise de l'internaute sera sensiblement entravée voir rendue impossible lorsque sont mis en place des no-logs signifiant que le prestataire ne collecte aucune donnée sur ses utilisateurs et ne peut donc matériellement pas les identifier.

Ces dispositifs constituent des atouts précieux pour les défenseurs des droits de l'homme, les journalistes ou encore les lanceurs d'alerte qui peuvent construire un plaidoyer en faveur des libertés individuelles ou faire exercice de leur liberté d'expression.

ANONYMOUS

\ə.ˈnɒ.nɪ.məs\

Le collectif Anonymous est un mouvement hacktiviste se qualifiant par la multitude "Nous sommes Anonymous. Nous sommes légion" qui débute sa première action militante officielle en 2008 en effectuant diverses actions contre l'Église de la Scientologie alliant manifestation de rue et attaque DDoS.

Dès la première apparition officielle du collectif, le mouvement se caractérise par le port du masque de Guy Fawkes, rebelle catholique anglais du XVIème siècle popularisée par la bande dessinée et le film « V pour Vendetta ». Depuis 2010 les actions du collectif sont dirigées contre les gouvernements exerçant une censure à l'encontre de leur population à l'instar des moyens mis en œuvre lors des Printemps arabes. Les discours gouvernementaux ont été tantôt approbateurs tantôt détracteurs à l'encontre du collectif qualifié de menace à la sécurité nationale par le directeur de la NSA en 2012 et largement salué suite à sa déclaration de guerre contre Daesh en 2015.

AUTOCENSURE

\o.to.sɑ̃.syʁ\

L'autocensure est une forme de censure qu'une personne s'applique à elle même par peur, crainte de représailles ou encore suite à la réception de menaces. A l'ère d'Internet l'autocensure s'est démultipliée pour plusieurs raisons :

- la crainte de fuite de données personnelles, de fuite de photos
- la crainte d'une cybersurveillance menée par les plateformes numériques ou les gouvernements
- la crainte d'une dénaturation des propos
- l'absence d'utilisation de pseudonymes
- la volonté de se conformer à l'opinion majoritaire
- la crainte de se faire punir, humilier ou insulter

Ce faisant ce sont bien majoritairement des personnes ayant subi auparavant une forme de cyberharcèlement ou d'injures et de menaces en ligne qui vont s'autocensurer par crainte que cette vague de haine ne se reproduise. Sur les réseaux sociaux les utilisateurs refusent parfois de porter un message en ligne reflétant leur opinion en considérant que le coût supporté de cette prise de position (haine, harcèlement) ne compensera pas le bénéfice (discours extrêmes sont plus relayés que les discours modérés). Cette majorité silencieuse des réseaux sociaux est parfois nommée « silent civic » : ce sont des citoyens silencieux qui suivent certaines pages, s'informent mais ne publient pas de messages engagés.

AVATAR

\a.va.taʁ\

Antérieurement l'avatar désignait le personnage joué par un individu dans un jeu. Désormais il désigne tout aussi bien le fait de dissimuler son identité derrière un pseudonyme que la représentation physique d'un individu sur Internet ou dans un jeu vidéo.

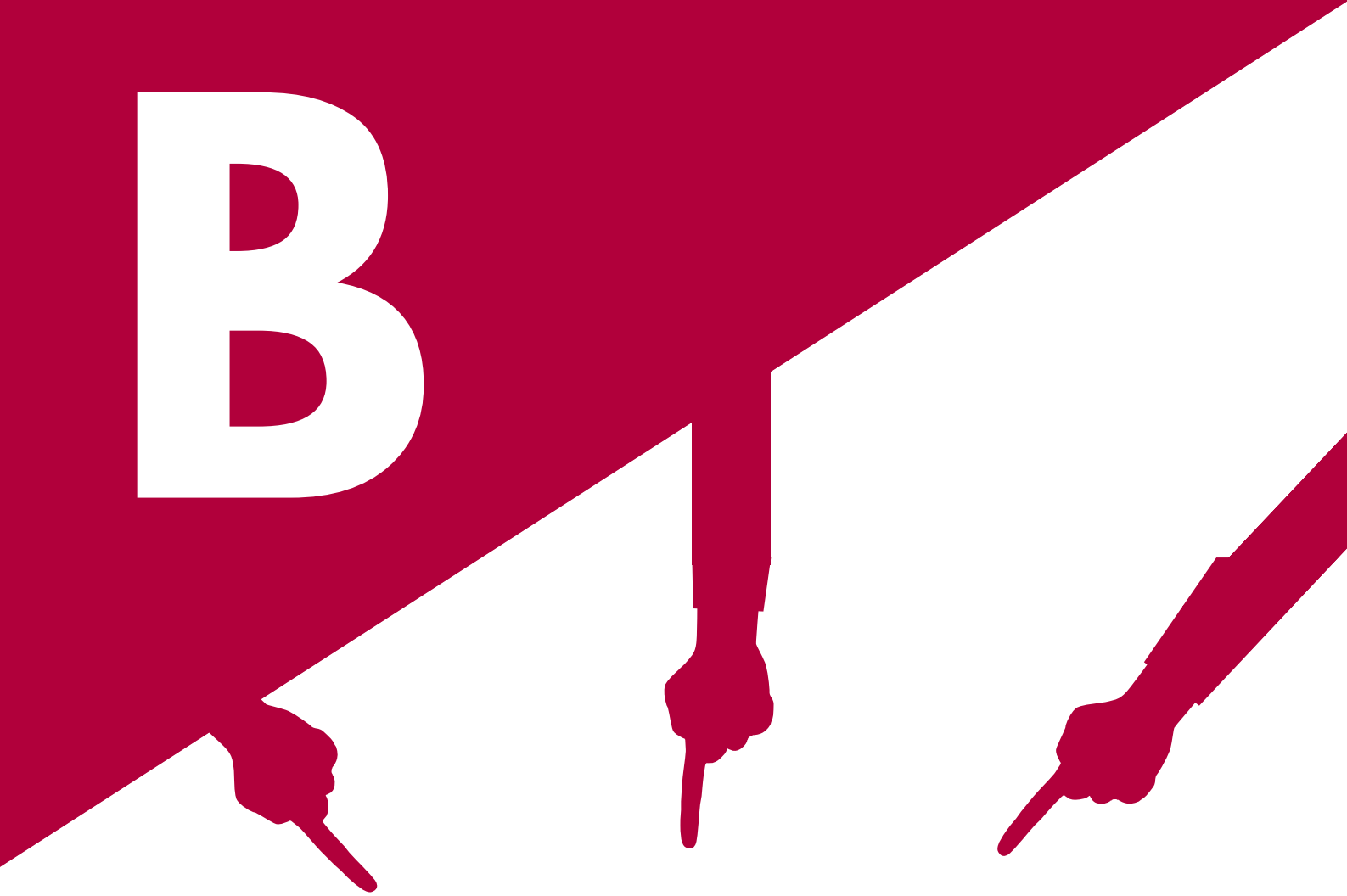
Il s'agit donc d'un double numérique. Les avatars sur les jeux vidéos permettent une liberté de customisation souvent plus large que dans le monde réel. Cette liberté est source d'émancipation pour les joueurs mais également source de compréhension en visibilisant les discriminations racistes ou sexistes auxquels sont confrontées les personnes dans le monde réel. Pour cette raison les personnes victimes de discrimination se refusent parfois à adopter un avatar leur ressemblant afin de ne pas être victime de discrimination sur une plateforme numérique.

La plateforme Horizon Worlds lancée par Méta permet aux personnes de visualiser leurs avatars grâce à la réalité virtuelle. Actuellement en bêta-test un avatar féminin d'une utilisatrice a été sexuellement agressé devant d'autres utilisateurs amenant à questionner les questions de responsabilité et de protection qui devront être mis en place sur ces nouvelles plateformes numériques – puisque le caractère immersif de la réalité virtuelle renforce l'insécurité des personnes l'utilisant.

L'apparence d'un avatar est susceptible d'influencer le mode de jeu ou la façon d'interagir des individus. Ce phénomène s'appelle l'effet Proteus. Lors de l'étude menée par Yee en 2009 sur le jeu de rôle massivement multi-joueurs World of Warcraft, il a été révélé que les avatars jugés attractifs et de grande taille selon les joueurs étaient les plus puissants en terme d'expériences sur le jeu et étaient plus écoutés au sein d'un groupe.

Les interactions entre les joueurs sont également à distinguer puisque les personnages masculins sont ressortis plus enclins à s'engager dans des combats tandis que les personnages féminins avaient plus tendance à soigner leurs coéquipiers.

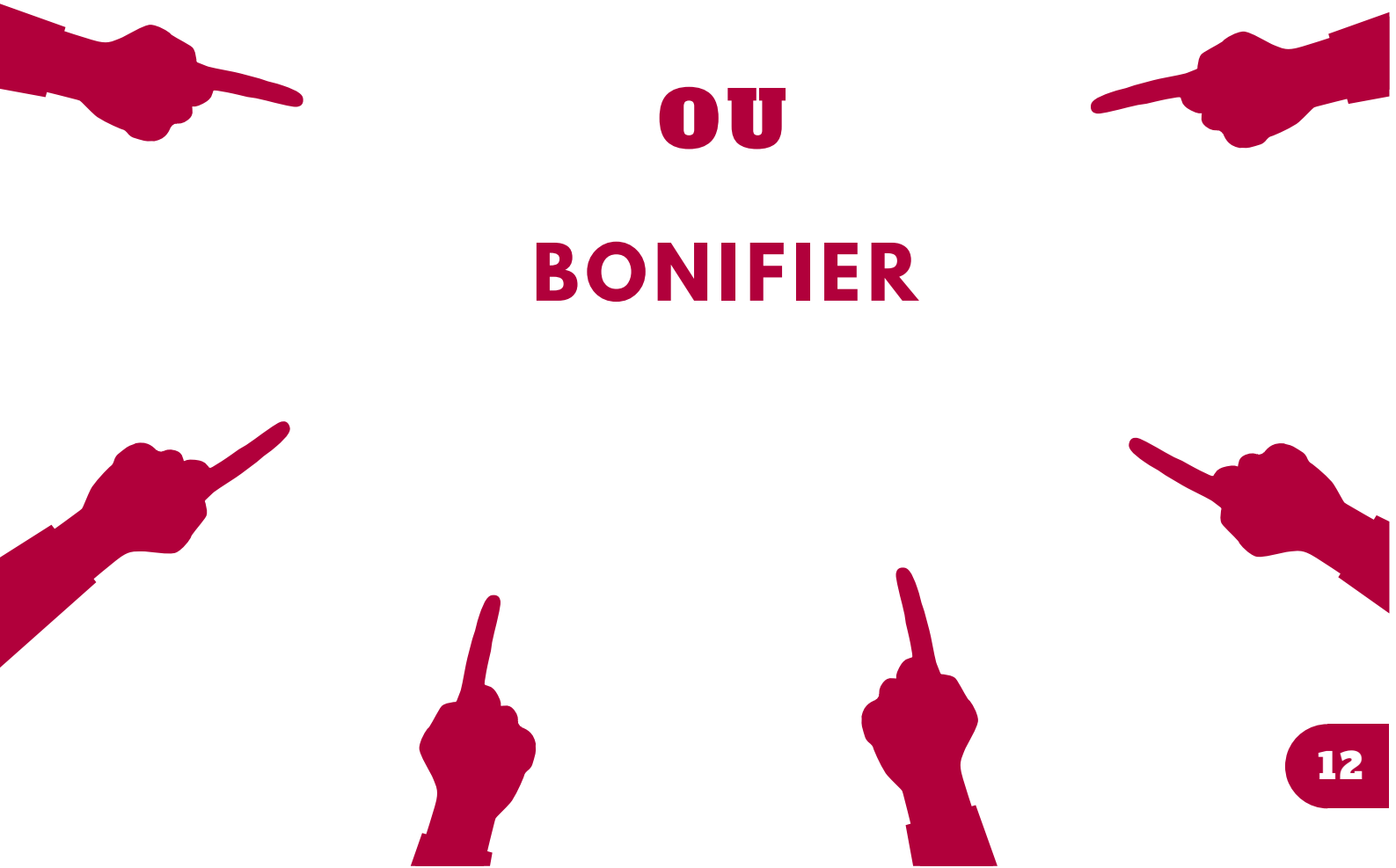
B



BLÂMER

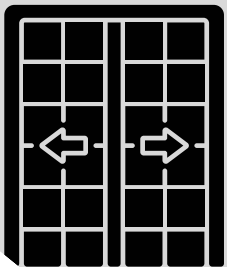
OU

BONIFIER



BACK DOOR

\blæk dɔɹ\



La porte dérobée (ou back door) est une fonctionnalité introduite dans un logiciel qui permet d'accéder secrètement aux activités du logiciel, d'en prendre le contrôle ou d'exercer une surveillance. Grâce à la mise en réseau des appareils connectés, une porte dérobée sur un logiciel permettra d'accéder aisément à l'ensemble des dispositifs d'une personne (ordinateur, smartphone, objets connectés...)

Utiliser à des fins malveillantes une porte dérobée permettra de dérober ou détruire les données des utilisateurs (mot de passe, coordonnées bancaires, secrets commerciaux, messages privés...) ou encore de contrôler à distance un ordinateur pour réaliser une cyberattaque. Parfois les développeurs insèrent une porte dérobée dans leurs logiciels pour réaliser aisément les actions de maintenance.

La question des back door a souvent été au cœur des débats entre les gouvernements et les entreprises privées : lorsqu'une entreprise propose l'envoi de messages chiffrés entre ses utilisateurs, les services de renseignements sollicitent la mise en place de porte dérobée permettant d'accéder aux messages dans le cadre d'enquêtes et de poursuites de crimes grave. Les entreprises privées y répondent bien souvent par la négative car l'installation d'une porte dérobée à destination des services de renseignement uniquement est impossible : la porte dérobée pourra également être utilisée à des fins malveillante par des tiers pour commettre une cyberattaque par exemple.

BATX / GAFAM / MAMMA / NATU

Ces différents sigles désignent des entreprises centrales dans le développement technologiques à travers le monde. Ces derniers ont bouleversé les habitudes de milliards d'être humains.

Les GAFAM désignent successivement Google, Apple, Facebook, Amazon et Microsoft. Suite au changement de Facebook à META nous passons de GAFAM à GAMAM - aussi dénommé MAMMA (Google étant remplacé par Alphabet - sa société mère).

Ces entreprises américaines sont majeures dans les champs économiques et politiques et sont concurrencées par les BATX en Chine. En effet dans ce pays une politique d'indépendance renforcée a fait naitre des équivalents aux grandes sociétés américaines à savoir Baidu (moteur de recherche) , Alibaba (site de e-commerce), Tencent (réseau social) et Xiaomi (entreprise technologie). Les BATX sont en situation monopolistique puisque les GAFAM sont strictement encadrés voir censurés dans cette région du monde.

NATU est un acronyme désignant Netflix, Airbnb, Tesla et Uber. Ces entreprises ont proposé des modèles économiques innovant avec de nouveaux produits/services plus accessibles et qui répondent à la nécessité d'un nouveau besoin pour les consommateurs jusqu'ici non comblé.

BIAIS ALGORITHMIQUE

\bjɛ al.gɔ.ʁit.mik\

Un biais algorithmique se définit comme l'absence d'éthique, de neutralité, de moralité ou d'équité dans le résultat produit par un algorithme. Un biais dans un algorithme mettra ainsi en relief les discriminations raciales, sociales ainsi que les discriminations liées au genre, à l'orientation sexuelle, à l'handicap et toutes formes de biais sociaux ou culturels présents dans la société. Ainsi un algorithme de traduction féminisera le terme neutre « nurse » en « infirmière » et masculinisera le terme neutre «doctor » en « docteur ».

Ces biais algorithmiques constituent le reflet d'une société discriminante puisque les algorithmes produisent des résultats à partir de base de données où sont compilées ces inégalités.

A titre d'exemple l'absence de représentativité de certaines catégories de population dans les bases de données a pu causer un taux d'erreur dans la reconnaissance faciale de 35 % pour les femmes noires contre 0,8 % pour les hommes blancs : cela s'explique par le fait que les bases de données sont majoritairement constituées d'hommes blancs.

L'existence de biais algorithmique s'explique notamment par la surreprésentation d'hommes blancs dans les développeurs à l'initiative de ces logiciels qui n'ont parfois pas une pleine conscience des discriminations potentielles et des privilèges dont ils bénéficient. L'un des moyens mis en place pour lutter contre ces biais algorithmiques est de créer des bases de données plus éthiques et représentatives de la société intégrant notamment des athlètes porteurs de handicap, des personnes racisées et des femmes chefs d'entreprises... Catherine d'Ignazio et Lauren F. Klein (Data Feminism, MIT Press, 2020) se refusent par exemple à parler de biais et préfèrent le terme d'« oppression algorithmique ».

BLOCKCHAIN

\blɔkkʃɛ̃\

La blockchain (chaîne de blocs) est une technologie de stockage et de transmission d'informations ayant été développée en 2008. Le principe de la blockchain est de fonctionner sans organe central de contrôle – autrement dit sans intermédiaire. Cette base de données a pour particularité d'être partagée entre tous ses utilisateurs et d'être sécurisée grâce au chiffrement. Ainsi la sécurité de la blockchain repose sur la certification effectuée par tous ses utilisateurs répartis dans le monde. Ce système décentralisé permet l'envoi de données à l'ensemble des ordinateurs et équipements composant la chaîne de blocs.

En ce sens la blockchain doit être envisagée comme un système technique démocratique plaçant les utilisateurs en position de propriétaires des informations échangés. La sécurisation garantie par les équipements de tous les utilisateurs – grâce à son caractère décentralisé - rend le système assez fiable puisque chaque opération est automatiquement hachée sous une forme cryptée. Si la blockchain a pu être présentée comme une solution optimale en terme de fiabilité, il convient de constater que ce n'est que le lien de confiance qui a été déplacé : basculant de la confiance accordée à un organe centralisé (gouvernement, établissement monétaire et financière, compagnie d'assurance) à la confiance dans le code et dans les personnes qui élaborent ce code. Ce faisant une erreur dans le code pourrait engendrer des vols et piratages. L'absence d'organe centralisé a également pu faciliter la matérialisation de fraude fiscale ou de financement du terrorisme.

BOT
\bɔt\

Un bot est une application logicielle qui interagit avec des serveurs informatiques pouvant être automatisé ou semi-automatisé : son but est de simuler le comportement d'une personne humaine ou bien d'effectuer des tâches répétitives. Pour effectuer ces tâches répétitives les bots sont programmés à partir d'algorithmes.

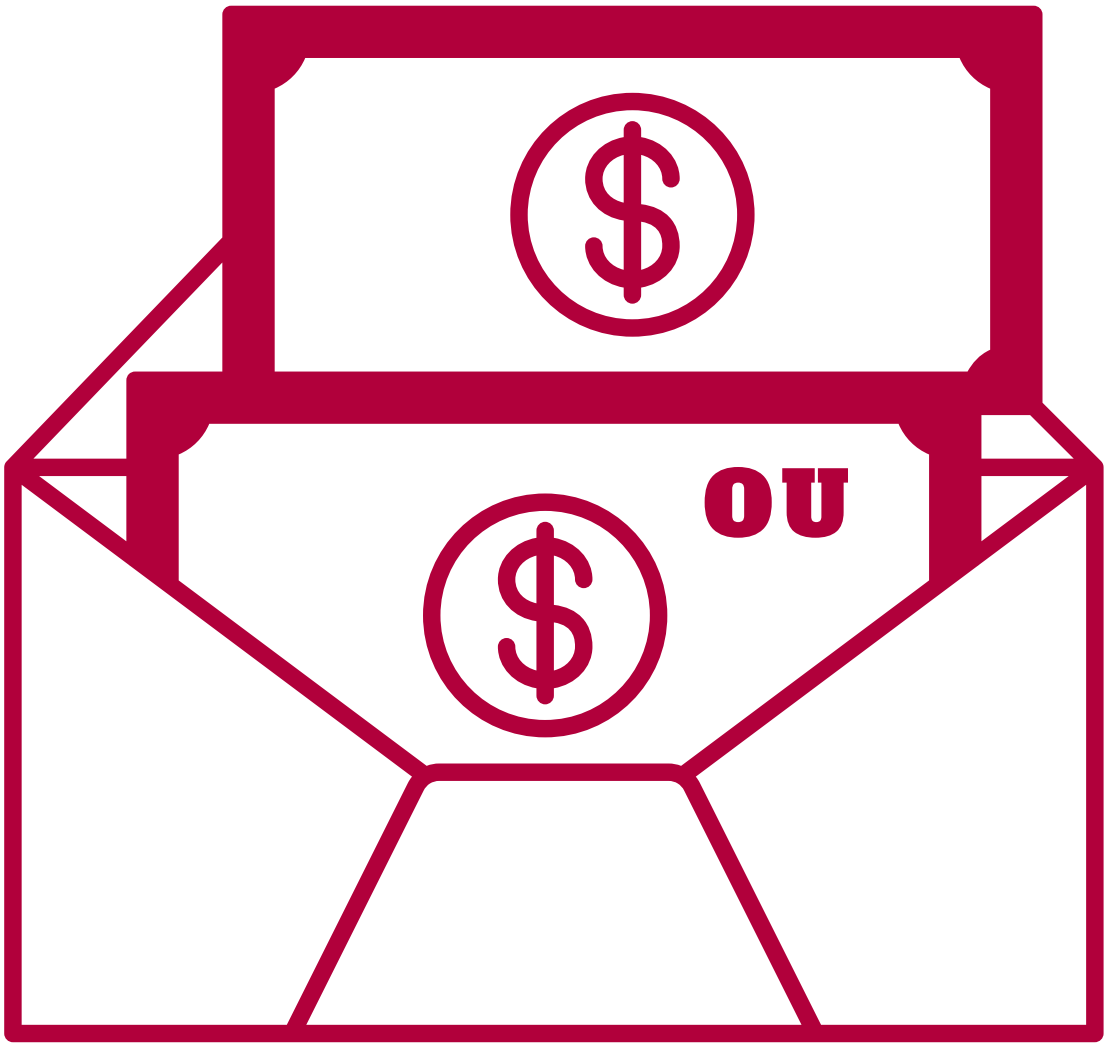
Sur Internet environ la moitié du trafic est géré par des bots : sur un moteur de recherche le bot va par exemple procéder à l'indexation des contenus pour fluidifier et faciliter les recherches, sur les messageries instantanés les bots peuvent gérer le canal de discussion, tenir des statistiques ou encore proposer des jeux. Les bots peuvent également être employés à des fins malveillantes en permettant la réalisation de cyberattaques, en facilitant la distribution de spam ou de commentaires malveillants.

Ce détournement de l'usage des bots est permis par leur multiplicité : ce sont donc plusieurs applications logicielles qui vont être utilisées au même moment dans un dessein frauduleux. Lorsque plusieurs bots communiquent entre eux, on parle alors d'un réseau de bots ou botnet.

Un chatbot est un bot ayant pour unique but de dialoguer avec des personnes et donc de simuler une interaction avec un autre individu. Les entreprises ont développé des chatbot ces dernières années dans le but d'assurer un service commercial ou un support client sur les réseaux sociaux.
L'avantage offert par les chatbot est leur disponibilité 24 heures sur 24, 7 jours sur 7.
Dans ce cas de figure les utilisateurs sont parfaitement conscients que leur conversation n'est pas avec un être humain. En 2016 Microsoft a crée un chatbot nommé « Tay » destiné à discuter avec les utilisateurs de Twitter. Afin de répondre aux questions des utilisateurs du réseau social, Tay a accéder aux données accessibles publiquement et a consolidé son apprentissage au fil des interactions avec les utilisateurs. Au bout de 8 heures le chatbot a toutefois tenu des propos racistes, négationnistes et misogynes menant à sa disparition du réseau social.
Dernièrement le grand public a découvert le chatbot ChatGPT qui a pu soulevé des inquiétudes en matière de droit d'auteur, de désinformation et de biais algorithmiques.

C

CONTESTER



CONCÉDER

CENSURE

\sɑ̃.syʁ\

En droit la censure est une atteinte portée à la liberté d'expression et d'opinion ainsi qu'à l'accès libre à l'information. L'atteinte portée à ces libertés fondamentales ne pourra être justifiée que dans le cadre de lutte contre des crimes graves comme par exemple l'apologie de crime contre l'humanité, la provocation au terrorisme, l'incitation à la haine raciale, l'incitation à la haine envers les personnes handicapées, l'incitation à la haine envers des individus en raison de leur orientation sexuelle, la pornographie infantile, l'incitation à la violence ou encore l'atteinte à la dignité humaine.

En ligne cette censure est toutefois rendue possible grâce à la mise en place de procédés techniques qui pourront entraver les libertés fondamentales des internautes : c'est le cas du retrait et du blocage.

Souvent employés sans distinction, le blocage et le retrait recouvrent des réalités bien différentes : le retrait ne peut être réalisé que sur un contenu particulier (un commentaire, une photo par exemple) alors que le blocage est beaucoup plus invasif puisque c'est un site Internet dans son ensemble qui sera rendu inaccessible. Du fait de la censure chinoise par exemple les sites de Google, Facebook ou encore Twitter sont bloqués afin que les internautes se dirigent vers des plateformes numériques chinoises largement contrôlées par l'État. Cette censure peut être réalisée sur le fondement de la loi ou bien des conditions générales d'utilisation d'une plateforme.

Les conditions générales d'utilisation des plateformes numériques ont rendu possible le retrait de :

- Contenus militants émanant de communautés lesbiennes, gays, bisexuelles, transgenres et queers
- Plaidoyers formulés contre des gouvernements répressifs
- Documentaires sur les nettoyages ethniques
- Critiques sur la discrimination raciale
- Représentation de la nudité ayant une valeur historique, culturelle ou éducative
- Documentaire de conflits et récits historiques
- Preuves de crimes de guerre

Cette distinction est importante car la censure n'aura pas la même portée : lorsque la loi est mobilisée la censure se limitera au territoire de l'État en ayant fait la demande tandis que l'application des conditions générales d'utilisation permettra une censure mondiale.

COMMUNS NUMÉRIQUE

\bɭɔkkʃɛ̃\

Les communs numériques constituent l'intégralité des ressources numériques qui sont créées et gérées collectivement par une communauté. Les communs numériques se caractérisent par leur non-rivalité (plusieurs personnes peuvent utiliser la ressource en même temps) et leur non-exclusivité (tous les internautes peuvent y avoir accès sans restriction au droit d'usage). Considérer les ressources numériques au travers de dispositifs collaboratifs amène à promouvoir la libre circulation des biens numériques. Ainsi les communs numériques sont parfois envisagées comme une alternative au capitalisme et au mouvement de privatisation qui irrigue le numérique.

En effet les communs numériques reposent sur le lien de confiance entre les membres de la communauté et sur leur autogouvernance. Le régime juridique des creative commons s'applique tout particulièrement aux communs numériques. Il s'agit de permettre une mutualisation des connaissances, des ressources tout en favorisant l'innovation et la libre concurrence. En définitive les communs numériques s'imbriquent parfaitement dans l'histoire d'Internet qui, dès ses débuts, a été le fruit d'une co-construction d'acteurs militant pour son ouverture et son esprit collaboratif. Dans la pratique les communs numériques souffrent toutefois d'une absence de réciprocité face aux plateformes numériques à l'exemple du moteur de recherche Google bénéficiant de revenus importants grâce aux contenus de l'encyclopédie Wikipédia - qui à l'inverse est peu rétribuée en contrepartie.

COOKIE

\ku.ki\

Un cookie informatique est une trace numérique enregistrée sur l'équipement des internautes et est associé à un site web ou à un domaine web. Le cookie permet d'associer les identifiants des internautes à leur navigation : c'est notamment grâce à ce stockage d'informations qu'un panier d'achat est conservé sur un site marchand.

Les cookies assurent le bon fonctionnement d'un site web mais peuvent également servir à des fins publicitaires et plus largement à collecter des données personnelles sur les internautes.

Auparavant ces cookies étaient acceptés par défaut par les utilisateurs sans que leur consentement ne soit expressément demandé. Progressivement les enjeux liés au pistage des internautes par le stockage de données personnelles - grâce aux cookies - a toutefois fait évolué le droit au respect de la vie privée. C'est pourquoi l'utilisateur doit désormais être informé des données collectées le concernant, de la raison justifiant cette collecte et de la durée de conservation des informations personnelles. Le consentement explicite des internautes est également requis bien qu'en pratique il peut encore être mal appliqué par certains sites web.

CROWDSOURCING

\kʁɔd.suʁ.siŋ\

Le crowdsourcing (ou production participative) désigne le travail collaboratif ou cumulatif d'une foule de personnes que l'ère du numérique a grandement facilité. Il s'agit notamment d'atteindre des objectifs scientifiques, culturels, sociaux ou encore économiques qu'un groupe de personnes restreint n'aurait pu atteindre.

C'est notamment le cas du projet OpenStreetMap qui compte sur la participation de l'ensemble des internautes pour constituer une base de données géographique mondiale.

A priori le crowdsourcing permet une participation de l'ensemble des individus sans aucune discrimination grâce à son caractère "ouvert". Pour autant certains initiatives de crowdsourcing ont pu reproduire des schémas discriminants à l'instar de l'application StreetBump permettant aux utilisateurs de signaler l'état des routes pour mettre en oeuvre les réparations nécessaires et sur laquelle les classes populaires ont moins pu participer car elles sont moins nombreuses à posséder un smartphone

CRYPTOMONNAIE

\kʁip.tɔ.mɔ.nɛ\

La cryptomonnaie est une monnaie numérique transitant en peer-to-peer (de pair à pair) sans qu'une banque ne centralise les échanges théorisée par la communauté cypherpunk de 1980 en alternative au capitalisme. Il s'agit donc d'un système décentralisé permettant la distribution d'actifs numériques grâce à la blockchain. Ce faisant l'ensemble des transactions encadrant les cryptomonnaies sont publiques et transparentes et peuvent n'être contrefaites que très difficilement grâce au protocole de chiffrement les encadrant.

La distribution de cette monnaie virtuelle est rendue possible par le "minage" lors duquel chaque individu ayant participé se voit attribué le montant de l'effort fourni de manière graduelle. Créer de la cryptomonnaie se fait par la résolution de problème cryptographiques élevés exigeant du temps et des ressources numériques (processeurs de carte graphique) ayant un fort impact énergétique. Contrairement à son origine cryptoanarchiste et issu des communautés cypherpunk, il convient aujourd'hui de constater que les cryptomonnaies ont été largement récupérées ou créées par les grandes entreprises numériques ainsi que certains gouvernements dans un dessein capitaliste, c'est le cas de la cryptomonnaie Libra crée Facebook/Méta.

CYBERATTAQUE

\si.bɛ.ʁa.tak\

Une cyberattaque est un acte malveillant dirigé vers un dispositif informatique pouvant être commis par un individu seul, un groupe de personne structurées, une entreprise ou encore un gouvernement. La finalité d'une cyberattaque peut être de paralyser l'accès à un service ou à un système informatique, de voler des données personnelles, d'altérer ou de détruire des informations dans un système informatique.

La cyberattaque peut par exemple prendre la forme d'une attaque par force brute : il s'agit de tester toutes les combinaisons possibles jusqu'à le trouver le mot de passe d'une personne. La cyberattaque peut également prendre la forme d'une attaque par déni de service (DDoS).

Une attaque DdoS consiste à envoyer de nombreuses requêtes sur un seul et même service pour en empêcher le fonctionnement normal. Par sa forme « distribuée » cette cyberattaque est plus difficile à stopper dans la mesure où ce sont plusieurs machines qui se coordonnent et envoient simultanément les requêtes.

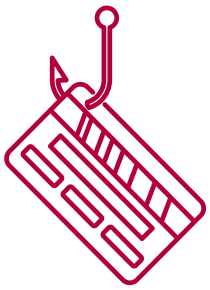
L'objectif est de rendre inaccessible un site Internet, un service ou encore un serveur de fichier à une large échelle. Les attaques DdoS peuvent occasionner d'importantes pertes financières lorsque l'accès à un site commercial est entravé à l'image de l'attaque réalisée contre Amazon ayant entraîné une perte de 600 000$ en dix heures durant les années 2000. Pour se prémunir contre les cyberattaques de nombreux sites web proposent une prime aux bugs (bug bounty) qui consiste à repérer les vulnérabilités d'un site pour les corriger avant qu'une cyberattaque ne soit commise.

Ces attaques malveillantes peuvent également être le fruit d'un malware (logiciel malveillant) développé dans le but d'endommager ou de corrompre l'ordinateur d'un utilisateur.

CYBERATTAQUE

Ces malware seront notamment localisés dans la pièce jointe dans un e-mail ou dans un logiciel frauduleux que l'utilisateur téléchargera en pensant qu'il s'agit d'un logiciel authentique.

Les spyware (programme espions) peuvent aussi porter atteinte à la sécurité d'un système informatique en enregistrement secrètement les actions émises sur un matériel informatique. Les ransomware sont des malware qui ont la particularité de demander une rançon aux utilisateurs pour pouvoir de nouveau accéder aux données personnelles. L'attaque peut également être réalisée par un hameçonnage (phishing) qui consiste à se faire passer pour une entreprise légitime pour demander des informations sensibles aux victimes.



CYBERSÉCURITÉ

\si.bɛʁ.se.ky.ʁi.te\

La cybersécurité désigne l'ensemble des dispositifs, outils, concepts et règlementations visant à protéger les personnes, les serveurs, les ordinateurs, les appareils mobiles, les réseaux ou encore les données contre des attaques malveillantes ou cyberattaques. Le chiffrement est une technique de sécurisation des données visant à rendre le contenu des informations compréhensible uniquement par les personnes autorisées (détenant la clé de déchiffrement).
Le chiffrement assure la confidentialité et la sécurité des données.

Ce faisant les informations ne pourront être consultées par un tiers, une entreprise ou un Etat.

Pour approfondir :Tribune de la Quadrature du Net pour défendre le droit au chiffrement, 15 juin 2023.

Dans le cas du chiffrement de bout en tout : seuls deux personnes peuvent déchiffrer les données. Ainsi le fournisseur de service ne sera pas en mesure d'accéder aux informations échangées entre les personnes.
Le déchiffrement consiste à donner un sens aux informations chiffrées grâce à une clé de déchiffrement, à l'inverse du décryptage qui consiste à casser le chiffrement sans avoir obtenu au préalable la clé.

L'authentification permet également à un utilisateur d'accéder à une ressource de manière fiable et sécurisée - notamment grâce à un mot de passe solide. Cette authentification est dite à « double-facteur » lorsque l'intéressé doit prouver à deux reprises son identité pour accéder à une ressource. L'authentification est « multi-facteurs » lorsque plus de deux preuves d'identité sont requises. Le terme anglais back-up signifie une sauvegarde de données en anglais. Il s'agit de dupliquer ces données de sorte à ne pas les stocker sur un seul système informatique pour parer à l'éventualité d'une perte de données. Ces copies permettent la bonne restauration du système informatique ayant pu être corrompu.

D

DÉMOCRATIE

DICTATURE

DARKNET

\daʁk.nɛt\

Un darknet est un réseau de partage dont les protocoles contiennent des fonctions d'anonymat (à l'inverse des autres réseaux peer-to-peer). Ce faisant les réseaux darknet peuvent être utilisées pour communiquer sans subir une ingérence de la part des entreprises ou des gouvernements. C'est pour cette raison que les darknets sont souvent présenté comme des réseaux facilitant la réalisation d'activités illégales (vente de virus, de données à caractère personnel, échange de contenus à caractère pédopornographique ou réalisation de cyberattaque).

De nombreux sites webs hébergeant des contenus pédocriminels ont été démantelés sur le darknet par le collectif Anonymous ou le FBI.

Le discours médiatique diabolisant le darknet a pu être contesté par des associations telles que la Quadrature du Net dans la mesure où le Darknet peut offrir une réelle alternative à la surveillance de masse. En effet les darknets doivent également être envisagés comme des réseaux permettant la libération de la parole de dissidents politiques ou de communautés homosexuelles dans des États autoritaires, facilitant l'échange de communications en marge de grandes entreprises collectant des données personnelles à l'instar de Facebook ou Google ou rendant possible la diffusion d'informations sensibles par les lanceurs d'alerte. En définitive les principaux utilisateurs du darknet sont aujourd'hui les journalistes d'investigation et les dissidents politiques. Parmi les principaux darknets on peut citer le réseau Tor, Freenet ou encore GNUnet. Le darknet est parfois confondu avec le deepweb alors que ce sont deux termes distincts : si le darknet est un réseau de partage, le deepweb ne constitue pas un réseau mais désigne uniquement les sites web qui ne sont pas indexés par les moteurs de recherche.

DEEPFAKE

\ di:pfeɪk\

Un deepfake est une superposition d'images, de vidéos ou de fichiers audios existants à d'autres images, vidéos ou fichiers audios de sorte à changer le visage ou encore la voix d'une personne.

La technologie deepfake a pu être employée pour réaliser des canulars ou des fausses informations. C'est en 2018 que le monde a découvert la porté des deepfake lorsque que Jordan Peele et Jonah Peretti ont créés de toute pièce une vidéo de Barack Obama faisant une annonce publique. Depuis lors l'utilisation de deepfake est croissante dans le milieu de la pornographie mettant en scène quasi-exclusivement des femmes célèbres. Ce sont également les personnes politiques qui ont pu être la cible de deepfake. La technologie deepfake consiste en une atteinte au droit à l'image.

Pour approfondir : Quelques exemples et conseils de détection, Internet sans craintes.

DONNÉE PERSONNELLE

\dɔ.ne pɛʁ.sɔ.nɛl\

Une donnée à caractère personnel se définit par l'ensemble des informations qui se rapporte à une personne physique identifiée ou identifiable. Ainsi les données personnelles recouvrent tout aussi bien des informations directement identifiantes (nom, prénom) et des informations indirectement identifiante (date de naissance, numéro de téléphone, adresse postale, photo...).

L'enfermement progressif induit par le numérique présente un décalage certain avec la vision qu'on avait du web à sa création présenté comme une immense bibliothèque. Les contenus recommandés aux internautes viennent donc essentiellement conforter leurs opinions, représentations et croyances sans permettre la mise en questionnement.

Parmi les données personnelles certaines données bénéficient d'une protection renforcée, ce sont les données sensibles (concernant les mineurs, liées à l'orientation sexuelle, à l'appartenance syndicale, à l'opinion religieuse, données de santé, données génétiques et biométriques...)

Les données personnelles sont protégées par le droit français depuis 1978 avec la loi Informatique & Liberté.

Le cadre juridique entourant les données personnelles a toutefois été modernisé avec le Règlement général sur la protection des données personnelles (RGPD) adopté en droit de l'Union européenne et entré en vigueur en 2018. Le droit à la protection des données personnelles constitue un droit fondamental étroitement lié au droit au respect de la vie privée. Conformément au droit à la protection des données personnelles, les individus sont par exemple tenus de savoir quelles données sont collectées les concernant, dans quel but ces données sont collectées et pour combien de temps ces données seront conservées.

DOXING

\dɔk.siŋ\

Le doxing est une pratique consistant à divulguer les données à caractère personnel d'un individu sur Internet dans l'intention de nuire à sa vie privée. Il sagit plus précisément de rendre public l'adresse postale d'une personne ou encore son identité.

En France, depuis le 26 août 2021, le fait de révéler l'identité, et des informations personnelles dans le but de nuire est puni pénalement par l'amendement "Samuel Paty", à l'article 223-1-1 du Code pénal.

Ce nom ne doit rien au hasard, puisque des informations concernant le nom et l'adresse de l'établissement scolaire où Samuel Paty exerçait ont été exposé en ligne par des parents d'élèves.

Les femmes journalistes sont particulièrement sujettes aux pratiques de doxxing de sorte à limiter l'exercice de leurs droits à la liberté d'expression.

DYSMORPHIE

\dis.mɔʁ.fi\

L'utilisation d'applications numériques comme Zoom ou encore Snapchat a pu susciter un trouble de limage corporelle encourageant les internautes à modifier leurs images en recourant notamment à la chirurgie esthétique.

La dysmorphie Zoom est née suite au confinement et s'applique aux personnes ayant consulté un chirurgien esthétique alors qu'ils n'avaient jusqu'ici jamais souffert de leur apparence dans le monde réel. C'est en effet la confrontation régulière à leur propre image renvoyée par leurs écrans d'ordinateurs qui a encouragé ses personnes à se plaindre systématiquement d'un teint blafard suite aux nombreuses visioconférences.

La dysmorphie Snapchat quant à elle caractérise les personnes qui souhaitent reproduire sur leurs visages les filtres proposés par l'application lissant la peau, amincissant le nez et augmentant la taille des yeux.

E-G-H

ELDORADO, GAGEURE

OU

HANTISE

ECONOMIE DE L'ATTENTION

\ekɔnɔmi a.tɑ̃.sjɔ̃\

L'économie de l'attention est une branche des sciences économiques qui considère que l'attention est une ressource rare en raison de l'offre abondante d'informations à laquelle sont confrontés les consommateurs. La captation de l'attention n'est toutefois pas inhérente au numérique, dès l'Antiquité l'art de la rhétorique visait à capter l'attention des foules et manipuler les esprits.

C'est à l'apparition de l'imprimerie que l'attention devient un enjeu de marché ayant des finalités économiques et commerciales. Avec le numérique les consommateurs ont basculé dans une ère où l'immédiateté, l'immersion, les recommandations algorithmiques et le flux continu d'informations sont la norme. Ainsi l'économie de l'attention recouvre tout aussi bien les enjeux liés aux nouvelles opportunités de marché des entreprises que ceux liés à la captation de l'attention des internautes au moyen de leurs données personnelles.

La collecte de données personnelles permet de prédire les comportements et habitudes de consommation ou encore de navigation des internautes.

C'est ce que Shoshana Zuboff nomme le "capitalisme de surveillance ". Il s'agit d'établir des profils précis des utilisateurs pour générer des publicités ciblées, des recommandations conformes à leurs habitudes et ainsi maintenir les utilisateurs attentifs - captifs sur une plateforme.

Les data broker sont les entreprises qui agrègent les données à caractère personnel collectées par des entreprises privées et les revendent sur un marché de gros à d'autres entreprises spécialisées dans la publicité, le marketing ou l'analyse de données.

Les data broker amènent à envisager l'agrégation de données puisque ces entreprises sont en mesure de dresser un profil extrêmement ciblé des personnes grâce à l'immensité des informations personnelles détenues. Autrement dit les data broker sont des courtiers de données personnelles).

ECONOMIE DE L'ATTENTION

Dans l'économie de l'attention ce sont les données comportementales qui présentent un intérêt particulier : durée de la connexion, nombre de clics, nombre d'amis, de like ou encore de commentaires...

La FOMO (fear of missing out) définit la peur de manquer quelque-chose : c'est pour cette raison qu'un internaute se connecte sur un réseau social pour vérifier les nouveaux contenus mis en ligne sans avoir nécessairement reçu de notification. Sur une plateforme numérique l'utilisateur fait défiler les contenus jusqu'à en trouver un qui le satisfasse et crée un sentiment immédiat de récompense : comme une machine à sous.

L'économie de l'attention pourrait à terme engendrer de l'isolement social et un renforcement des comportements de consommation. Historiquement Internet n'a toutefois été pensé au travers de l'économie de l'attention mais bien autour du partage de savoir, de la libre circulation de l'information et de la collaboration : ce sont ces différents enjeux qui pourraient aujourd'hui être valorisés pour contrer les risques de l'économie de l'attention en alertant les utilisateurs des procédés mis en place à leur encontre pour les garder captif sur une plateforme numérique.

GAMEUR.SE

\gɛ.mœʁ\

Un gameur ou une gameuse est une personne qui joue fréquemment aux jeux vidéos. Peuvent être distingués les casual gamer (joueurs occasionnels) des hardcore gamer (joueurs compétitifs).

En raison de la place centrale accordée aux garçons dans les publicités de jeux vidéo, la figure de la gameuse a pu être contestée par des vagues de violence dirigées contre les filles et femmes joueuses mais également rendue possible par les nombreux stéréotypes prêtées aux femmes dans le domaine du jeu vidéo. Le terme « e-girl » a par exemple longtemps été employée afin de dénigrer les gameuses puisqu'il décrit une femme souhaitant uniquement attirer l'attention des hommes en ligne, de sorte à ostraciser les gameuses des communautés liées aux jeux vidéos. Les campagnes de cyberharcèlement, les menaces de viol, de mort ou encore le doxing consistant à révéler les informations personnelles telles que l'adresse postale d'une personne sont essentiellement dirigées contre les gameuses.

HACKEUR.SE

/'hæk3ˠz/

Un hackeur ou une hackeuse est une personne qui est un programmeur expérimenté et qui a plus largement une connaissance fine et précise des infrastructures technologiques. Les hackeurs font parti intégrante de l'histoire d'Internet puisqu'ils ont participé à sa création et à celle du World Wide Web. La mouvance hackeur se caractérise par l'accès libre à l'information grâce au contournement des protections logicielles et matérielles

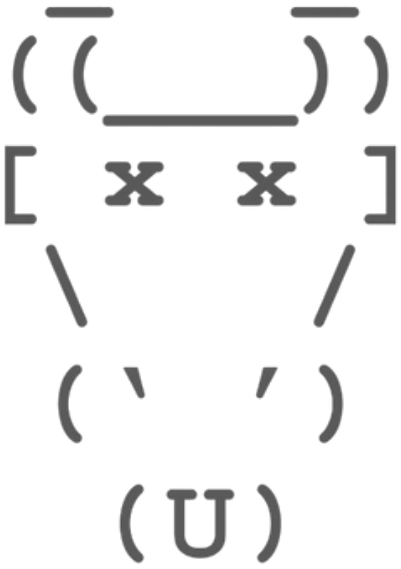
L'intention du hackeur a permis une classification de ces derniers à travers les termes : white hat, black hat, grey hat et hacktiviste. Les white et black hat sont une référence aux films de western où les bandits portent un chapeau noir contrairement aux héros qui portent un chapeau blanc.

Transposé dans l'environnement numérique le black hat désigne un hacker qui use ses compétences techniques pour mener des actions illégales dans un dessein criminel (création de virus ou logiciel espion, revente de données personnelles) tandis que le black hat usent de leur compétence avec bienveillance (en faisant remonter les vulnérabilités d'un système d'information pour éviter toute intrusion). Les grey hat au contraire laisseront un délai pour corriger une vulnérabilité mais la rendront publique si elle n'est pas corrigée dans le délai imparti ou bien agiront dans l'illégalité sans intention de nuire à autrui.

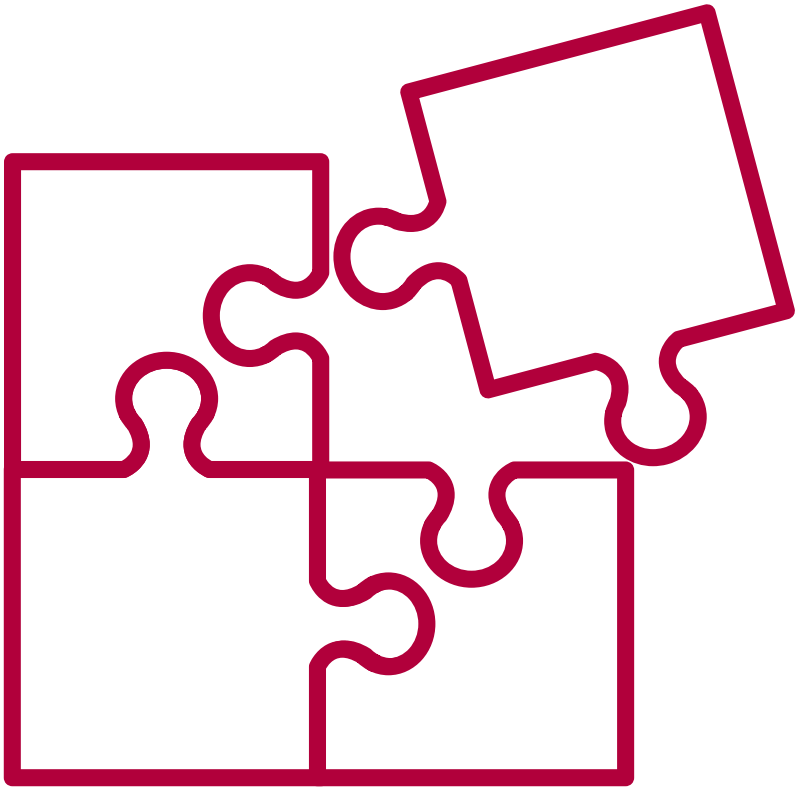
Les hackeuses ont tenu une large part dans l'histoire d'Internet à l'image d'Ada Lovelace à l'initiative du programme informatique ou de Grace Hopper ayant crée le terme de « bug » informatique.

La place de ces femmes a toutefois été largement invisibilisée dans l'histoire du numérique, puisque le nom d'Alain Turing est bien plus souvent cité que celui de Grace Hopper lorsqu'il s'agit d'envisager la culture hacker.

L'hacktivisme désigne un militantisme qui fait appel à des compétences en piratage informatique pour favoriser les changements politiques ou sociétaux. C'est en 1994 que le premier groupe de hackers est apparu, les Cult of the Dead Cow connu pour son engagement en faveur de la liberté d'expression sur Internet et pour son soutien aux mouvements de liberté numérique. L'"hacktiviste" utilise des opérations technologiques comme du piratages, du détournements de serveurs, du remplacement de pages d'accueil, du vol de données, de la diffusion de données confidentielles, etc.



INSTRUMENT D'INCLUSION



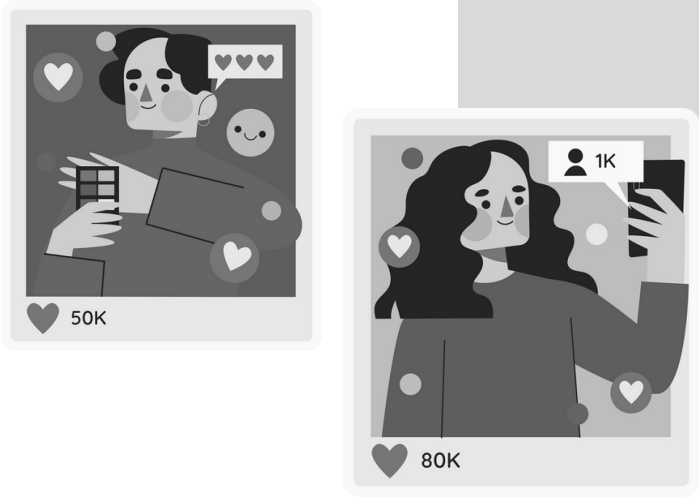
OU

D'ISOLEMENT

INFLUENCEURE.SE

\ɛ̃.fly.ɑ̃.sœʁ\

Un influenceur tout comme une influenceuse sont des individus qui utilisent leur popularité, leur taux d'engagement et leur audience médiatique pour orienter les tendances, les modes de consommations ou encore les opinions de leurs communautés en ligne.



Le marketing d'influence a largement renouvelé les stratégies commerciales des entreprises puisque la relation de proximité d'un influenceur et de ses abonnés peut donner une autre dynamique aux publicités. C'est en effet l'influenceur ou l'influenceuse qui donnera un style, une patte à la publicité afin que sa communauté continue de s'identifier aux contenus crées. Afin d'être associé à des entreprises certaines personnes tentent de se faire passer pour des influenceurs en achetant de faux abonnés ou de faux likes pour se créer une communauté en ligne.

Il existe plusieurs catégories d'influenceurs qui peuvent être distinguées : les macro-influenceurs (plus de 50 000 abonnés), les micro-influenceurs (moins de 50 000 abonnés), les nano-influenceurs (centaines à millier d'abonné). L'influenceur ou l'influenceuse ne doit toutefois pas être considéré comme une agence de publicité, c'est pour cette raison qu'il bénéficie d'une plus grande liberté artistique. Cependant les influenceurs ont l'obligation de rendre leur publicité identifiable puisque le droit interdit la publicité cachée.

INTELLIGENCE ARTIFICIELLE

\ɛ̃.tɛ.li.ʒɑ̃s aʁ.ti.fi.sjɛl\

L'intelligence artificielle regroupe les procédés et techniques qui reproduisent ou surpassent des comportements humains. Il s'agit plus simplement de simuler l'intelligence humaine. Parmi les grands domaines de l'intelligence artificielle on trouve la traduction automatique, la reconnaissance vocale, la conversation automatique, la composition musciale automatique, la reconnaissance faciale ou encore la classification d'images.

C'est en 1956 que l'intelligence artificelle devient une discipline académique, après qu'Alan Turing est envisagé la possibilité de créer des machines douées d'intelligence en 1950 à travers le test de Turing consistant à ce qu'une machine puisse interagir à l'aveugle avec un humain sans être identifié en tant que machine. Depuis le début des années 2000 et l'avènement du big data les puissances de calcul et les flux d'informations sont sans précédent ce qui permet un renouveau de l'intelligence artificielle grâce au machine learning

Le machine learning (ou apprentissage automatique) désigne une technologie liée à l'intelligence artificielle qui permet aux ordinateurs et logiciels d'apprendre par eux mêmes à partir des données qui leurs sont accessibles.

Le machine learning a pu permettre la création d'une intelligence artificielle dénommée Eugene Goostman dialoguant avec les internautes. A l'issue d'une conversation avec Eugene Goostamn 33% des internautes pensaient avoir dialogué avec un garçon ukrainien de 13 ans et non pas un ordinateur : l'intelligence artificielle ayant réussi à reproduire les schéma d'une véritable conversation humaine. C'est grâce au machine learning que l'ordinateur développé par IBM nommé Deep Blue a pu vaincre le champion mondial d'échecs Garry Kasparov en 1997. Le machine learning est étroitement lié au Big Data (à l'immense flux de données accessibles sur le web). En 2016, AlphaGo développé par Google est parvenu à vaincre le plus grand champion de Go au monde. Plus récemment, c'est ChatGPT qui a passé le bac philosophie face à Raphaël Enthoven. Si le philosophe a obtenu la note de 20/20, l'IA a quant à elle eu 11/20... pour une rédaction effectuée en 90 secondes contre 90 minutes.

INTERNET

\ɛ̃.tɛʁ.nɛt\

Internet est un réseau informatique mondial reliant plusieurs réseaux informatiques et utilisant le protocole TCP/IP (Transmission Control Protocol / Internet Protocol). C'est à partir des années 1960 que la connexion informatique à longue distance est envisagée afin de permettre à des ordinateurs de travailler ensemble à distance. Il s'agissait toutefois de l'ARPANET créée dans le cadre de la DARPA (organisme de recherche pour la défense américaine) à des fins militaires puis pour faciliter les communications entre les chercheurs. En 1969 ARPANET relie l'Université de Californie à Los Angeles (UCLA), à l'Institut de Recherche de Stanford (SRI), l'Université d'Utah et l'Université de Santa Barbara. La question s'est toutefois posée par la suite de relier ARPANET à d'autres réseaux de communications par radio ou satellite : c'est ce qui a donné la création du protocole TCP/IP et donc d'Internet.

Ce sont par suite différentes applications qui se sont liées à Internet telles que le web (world wide web). Le web est donc bien distinct d'Internet : le web est un système de pages qui sont interconnectées et fonctionnent à travers Internet. Le web a été crée au laboratoire du CERN en 1989 par Tim Berners-Lee. Pour le dire plus simplement Internet est le réseau mondial sur lequel les ordinateurs s'échangent des informations alors que le web est l'immense bibliothèque qui rend possible la navigation de pages en pages. Internet comme le web relève dès lors de projets collaboratifs mêlant les mouvances hackers, les communautés hippies, les gouvernements et les entreprises tendant vers l'objectif de libre circulation de l'information

INTERNET

Jusqu'aux années 80 les programmeurs et usagers d'Internet avaient accès aux codes sources des logiciels et pouvaient améliorer les programmes informatiques. Progressivement le code informatique se transforme toutefois en bien marchand protégé par des contrats de licences. La montée en puissance des droits de propriété intellectuelle appliqué au domaine de l'informatique va dès lors créer un mouvement de privatisation d'Internet où les grandes entreprises numériques vont largement dominer le marché en tant qu'acteurs oligopolistiques.

Cette ascension des plateformes numériques est notamment visible dans les grandes phases de l'Internet : du web 1.0 au web 3.0.

Le web 1.0 désigne le web statique dans laquelle les utilisateurs peuvent aisément accéder aux contenus mis en place mais ne peuvent interagir entre eux (1990-2000). Le web 2.0 s'applique au web social où Internet s'est transformé en espace de socialisation permettant aux utilisateurs d'échanger et de produire des contenus à travers les blogs, les forums ou encore les réseaux sociaux (2000-2010). Le web 3.0 ou web sémantique caractérise l'enfermement progressif des utilisateurs dans une navigation strictement personnalisée grâce au profilage des individus permis par la collecte de leurs données personnelles. (depuis 2010).

L

LIBÉRALISER

OU

LÉGIFÉRER

LOGICIEL PROPRIÉTAIRE ET LIBRE

\lɔ.ʒi.sjɛl pʁɔ. pʁi. je. tɛʁ libʁ\

La culture Internet ou culture libre s'est fondée sur la promotion d'une liberté de diffusion et de modification des informations. Ce faisant le code source d'un logiciel était accessible aux utilisateurs pour qu'ils en modifient les bugs sans dépendre de l'éditeur du logiciel. C'est dans cette optique que les logiciels propriétaires et les logiciels libres doivent être opposées. Les licences libres s'appliquent aux oeuvres à propos desquelles les auteurs ont concédé leurs droits d'auteurs aux utilisateurs pour qu'ils puissent faire usage de l'oeuvre, connaître le code source, modifier l'oeuvre ou encore la diffuser. Les logiciels libres offrent dès lors une plus grande liberté à leurs utilisateurs.

A l'inverse les licences propriétaires sont celles qui contraignent la connaissance du code source, l'utilisation, la modification et la distribution des oeuvres. Dans la communauté des libristes (en faveur des licences libres) l'utilisation de logiciels propriétaires est décriée en raison de la menace pouvant être causée à la vie privée et de l'opacité du code source qui pourrait faciliter l'espionnage et la surveillance. Plusieurs logiciels libres peuvent être cités tels que le navigateur web Mozilla Firefox, les systèmes d'exploitation GNU, Linux ou de la famille BSD, les suites bureautiques OpenOffice et LibreOffice. Le réseau Framasoft référence les logiciels libres dans son annuaire Framalibre

LOIS DE LA ROBOTIQUE

\lwa ʁo.bo.tik\

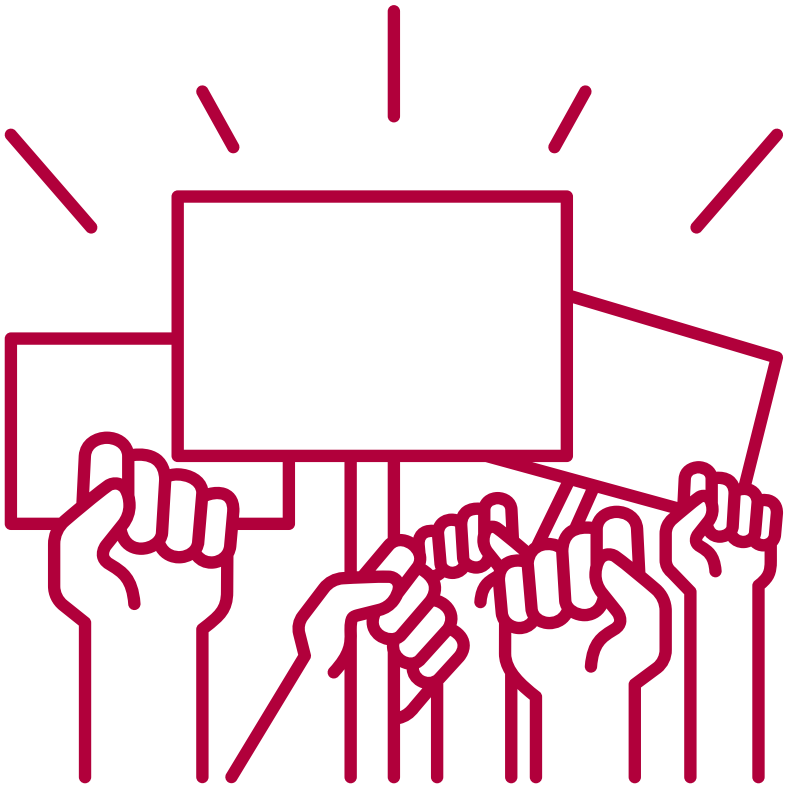
Les 3 Lois d'Asimov :

- Un robot ne peut porter atteinte à un être humain ni, restant passif, laisser cet être humain exposé au danger
- Un robot doit obéir aux ordres donnés par les êtres humains, sauf si de tels ordres entrent en contradiction avec la première loi
- Un robot doit protéger son existence dans la mesure où cette protection n'entre pas en contradiction avec la première ou la deuxième loi

C'est en 1942 qu'Isaac Asimov formule ces trois lois de la robotique dans sa nouvelle Cercle vicieux. Elles sont donc parues dans un ouvrage fictionnel. Aujourd'hui ces lois sont parfois considérées comme un idéal auquel tendre en matière d'avancées concernant l'intelligence artificielle. Les chartes de l'intelligence artificielle ou de l'éthique des robots adoptées ou en cours d'adoption mobilisent les termes des trois lois de la robotique (Corée du Sud en 2007, Proposition de loi française en 2020).

M

MILITANTISME



OU

MUTISME

METAVERS

\me.ta.vɛʁ\

Le métavers souffre d'un manque de définitions qui occasionne de vrais difficultés pour le public de le circonscrire, toutefois un métavers peut être défini comme un espace virtuel immersif connecté à Internet et accessible au travers de la réalité augmentée - ou de la réalité virtuelle - par un nombre illimité d'utilisateurs. La réalité augmentée (RA) allie en effet environnement réel à des éléments virtuels tels que les Google glass. A l'inverse la réalité virtuelle (RV) repose sur un environnement exclusivement artificiel tel que le Vision Pro.

Autrement dit la technologie peut venir se superposer à la réalité (RA) ou bien la remplacer (RV). Le principe du métavers a pour la première fois été rendu largement visible au travers du jeu en ligne massivement multijoueur "Second Life" en 2003.

Depuis 2021 l'entreprise Facebook a été renommée Meta et développe son propre métavers appelé "Horizon Worlds". En tant que monde virtuel chaque métavers possède sa propre monnaie permettant l'achat d'articles, d'objets et de services pour son avatar. Ainsi le métavers est indissociablement lié à la blockchain, aux cryptomonnaie et aux NFT. Par son caractère novateur, le métavers échappe encore très largement aux règlementations juridiques qui régissent la protection des données, la responsabilité des plateformes ou la modération des contenus. Si le métavers peut exacerber les phénomènes déjà présents sur les réseaux sociaux (désinformation, harcèlement, doxing) ce sont toutefois de nouveaux phénomènes qui peuvent également survenir. Les casques de réalité virtuelle sont en effet susceptibles de produire des effets de déréalisation et de dépersonnalisation ou rendent possible la collecte de données sensibles jusqu'alors non prévues par le droit telles que l'analyse de regard. Toutefois ces données personnelles émotionnelles ne sont pas encore appréhendées par les instruments juridiques applicables à la protection des données comme le RGPD.

NFT

\ɛn.ɛf.te\

Les NFT (pour non fungible token ou jeton non fongible) désignent un fichier numérique rattaché à un certificat d'authenticité. Plus simplement un NFT est un titre de propriété unique stocké et authentifié grâce à la blockchain.

Le principe de la blockchain est de fonctionner sans organe central de contrôle – autrement dit sans intermédiaire. Le NFT va donc prouver la rareté et le caractère unique d'un objet numérique (art crypto, objet de collection crypto, crypto jeu…)

Si une vidéo, une photo, un fichier audio, un élément de jeu vidéo mis en ligne peuvent donc être acheté avec les NFT, c'est également le cas d'objet virtuel tel qu'une paire de chaussure de designers qui pourra être visualisée avec un casque de réalité virtuelle.

NUDE

\nju:d\

Un nude est une photographie ou un film d'une personne dénudée. L'image même obtenue avec l'accord préalable de l'intéressée (sexting) ne peut être diffusée sans son consentement.

Le fait de porter à la connaissance du public ou d'une tierce personne un nude se nomme Revenge Porn.

C'est un délit.

Sont qualifiées de Dick pic les photographies de pénis en érection transmises sans sollicitation des personnes le recevant.

P-S-T

PANACÉE, SCIENCE-FICTION

OU

TYRANNIE

PLATEFORME NUMÉRIQUE

\pla.tə.fɔʁ.mə ny.me. ʁik\

Les plateformes numériques peuvent être distinguées entre d'une part les éditeurs de contenus et d'autre part les hébergeurs de contenus.

ÉDITEUR DE CONTENUS

\e. di. tœʁ kɔ̃tɑ̃ny\

Les journalistes faisant partis d'un organe de presse de même que les plateformes numériques comme Netflix doivent être considérées comme des éditeurs de contenu. Un éditeur contrôle les contenus qui seront accessibles et diffusés sur son site.

Il a donc connaissance des contenus avant qu'ils ne soient mis en ligne par sa maîtrise éditoriale. En droit l'éditeur est responsable de tous les contenus diffusés sur son site ou sa plateforme parce qu'il est soumis à une obligation de contrôle. L'éditeur ne peut pas attendre le signalement d'un contenu pour le retirer : il est responsable dès la mise en ligne du contenu.

HÉBÉRGEUR DE CONTENUS

\e.bɛʁ.ʒœʁ kɔ̃tɑ̃ny\

Facebook (Méta), Instagram, Snapchat et Tik Tok sont tous des réseaux sociaux. En tant que réseaux sociaux, ils doivent être considérés comme des hébergeurs de contenus. Un hébergeur permet la diffusion et le stockage d'écrit, d'image, de vidéo, de son ou encore de message par ces utilisateurs.

HÉBÉRGEUR DE CONTENUS

\e.bɛʁ.ʒœʁ kɔ̃təny\

IEn droit les hébergeurs sont irresponsables des contenus mis en ligne par leurs utilisateurs, ils sont cependant obligés de retirer un contenu dès qu'ils ont connaissance de leur caractère illicite dans un délai de 24 heures. Auparavant les réseaux sociaux procédaient au retrait des contenus suite au signalement fait par leurs utilisateurs.

Depuis que les délais de retrait ont été largement raccourcis (24 heures pour les contenus illicites, 1 heure pour les contenus de nature terroriste) : les réseaux sociaux privilégient la détection automatique de contenus illicites.

C'est à dire qu'ils misent sur l'intelligence artificielle et leurs règles de modération contenues dans leurs conditions générales d'utilisation. La difficulté est constituée par le fait que les conditions générales d'utilisation ne sont pas toujours rédigées en adéquation avec le droit national ou international.

Les conditions générales d'utilisation et les décisions automatiques ont permis le retrait :

- De contenus militant émanant de communautés LBTQI+
- De plaidoyers contre des gouvernements répressifs
- De représentations de la nudité ayant valeur historique, culturelle ou éducative
- D'informations sur les nettoyages ethniques

SURVEILLANCE

\syʁ.vɛ.jɑ̃s\

La surveillance n'est pas apparue avec le numérique, elle a toutefois reçu une nouvelle ampleur et de nouveaux moyens avec les outils électroniques. Il y a 2500 ans, l'Art de la guerre de Sun Tzu faisait d'ores et déjà état de l'intérêt d'observer secrètement ses ennemis en recourant à des espions.

Aujourd'hui ses espions sont susceptibles de se dissimuler dans notre poche eu égard aux nombreuses données collectées par nos smartphones. A l'ère du numérique ce sont tout aussi bien les gouvernements que des entreprises privées qui peuvent mettre en place cette surveillance à l'aide d'outils numériques. En 2013 le lanceur d'alerte Edward Snowden a révélé la mise en place du programme PRISM ciblant les personnes situées hors des Etats Unis par les services de renseignement américains ayant notamment collecté l'ensemble des données personnelles transitant par les câbles sous-marins reliant les Etats-Unis d'Amérique et l'Europe.

C'est une surveillance globale qui s'est dès lors déployée sur l'ensemble des internautes. Plus récemment - en 2021 - des révélations ont été faites concernant le projet Pegasus et la surveillance mise en place par les gouvernements en coopération avec la société israélienne NSO Group à l'encontre des défenseurs des droits de l'homme, d'avocats, d'opposants politiques et des journalistes au moyen de leurs téléphones portables.

A l'ère du numérique cette surveillance peut également être déployée à l'aide de dispositifs de télésurveillance tels que des caméras disposées dans l'espace public : il s'agit de vidéosurveillance.

Depuis 2011 la loi sur la sécurité intérieure la qualifie toutefois de vidéoprotection, bien qu'il s'agisse des mêmes procédés mis en oeuvre. Aujourd'hui les dispositifs de vidéosurveillance sont additionnés aux systèmes de reconnaissance faciale, ce qui engendre d'importants enjeux en lien avec la protection des données personnelles et le droit au respect de la vie privée.

La logique prédictive addosée à la vidéosurveillance et plus largement aux dispositifs de surveillance dans leur ensemble emporte des risques importants pour la société civile allant de la préservation des libertés fondamentales au vol de données, au risque de hacking ou d'erreur dans la reconnaissance faciale.

TROLL

\trəʊl\

Un troll est un individu qui crée une controverse, irrite ses interlocuteurs ou perturbe des conversations sur un réseau social. Ainsi le troll vient bouleverser les échanges au sein d'une communauté. Initialement dans la culture Internet le troll visait à créer une perte de temps pour les autres internautes en les redirigeant par exemple vers une autre page web que celle sollicitée. Se faire troller relevait donc d'une blague. Trollface est d'ailleurs un « meme »,
c'est à dire que c'est l'image qu'on donne aux trolls dans la communauté Internet : elle est symbolisée par un visage avec un immense sourire largement teinté d'ironie.

La communauté Internet a d'ailleurs considéré que l'un des premiers trolls était l'interprète russe Eduard Khil qui après s'être vu refusé l'interprétation d'une chanson américaine est monté sur scène afin de faire des vocalises sans parole accompagnées d'une gestuelle exagérée en 1966 . C'est en 2009 que le monde redécouvre cette vidéo, désormais numérisée : ce qui a donné «Trololo » (contraction de troll, Lol et des nombreuses vocalises « lololo ») Pour exister le troll doit toujours être intégré dans une communauté en ligne, en avoir acquis les codes ainsi que les normes et règles de modération : le troll se fait donc passer pour un membre honnête de la communauté en ligne afin de lancer un nouveau débat, une nouvelle pratique qui fera dévier les membres de la communauté de leurs habitudes. Dans certaines communautés en ligne, les membres imitent à leur tour les trolls pour qu'ils cessent les perturbations : c'est ce qu'on appelle « troller les trolls».

INDEX

ecn@crajephdf.org