LES OBJETS CONNECTES ET L'INTELLIGENCE ARTIFICIELLE

DESCRIPTION DU THÈME

Propriétés	Description
Intitulé long	Comprendre le fonctionnement des objets connectés et de l'intelligence artificielle
Formation(s) concernée(s)	Terminale STMG Système d'information de gestion (SIG)
Matière(s)	Terminale STMG Management, sciences de gestion et numérique Enseignement spécifique de SIG
Présentation	Découverte du fonctionnement des objets connectés et de l'IA, illustration par des exemples.
Savoirs	Intelligence artificielle : impact sur l'évolution des algorithmes.
Compétences	
Transversalité	Première STMG : sciences de gestion et numérique Terminale STMG : management, sciences de gestion et numérique Enseignement spécifique de SIG
Prérequis	Première STMG : sciences de gestion et numérique Thème 2 : Numérique et intelligence collective - Intelligence artificielle et automatisation de tâches organisationnelles.
Outils	
Mots-clés	Objets connectés, intelligence artificielle, algorithmes, protection des données personnelles, big data, adresse IP, protocoles, éthique.
Durée	3 heures
Auteur.e(s)	Estelle CYBULA-SORNETTE – Sébastien HENRIOT (relectures)
Version	v1.0
Date de publication	Avril 2023

DERNIÈRES RÉVISIONS

Ce tableau contient les modifications apportées au document après sa publication uniquement.

Date	Auteur.e	Description

LES OBJETS CONNECTES ET L'INTELLIGENCE ARTIFICIELLE

INTRODUCTION

Depuis les années 1990, les objets connectés sont de plus en plus présents dans notre quotidien. Du développement de leurs infrastructures techniques, que l'on appelle l'« Internet des objets », à celles de l'« Internet du tout connecté », les technologies convergent aujourd'hui avec l'intelligence artificielle et le big data vers un « Internet des comportements » dont l'enjeu est désormais l'analyse comportementale.

Le nombre d'objets connectés vendus pourrait augmenter de 50 à 200 milliards d'ici 2025. Ces nouveaux dispositifs, qui permettent de capter, d'analyser et de visualiser des données en temps réel, s'insèrent rapidement dans toutes les sphères de la vie quotidienne.

LES OBJETS CONNECTÉS

1 DÉFINITION

Les objets connectés sont des objets usuels, accessibles à tous, pilotables à distance via une application, auxquels on ajoute une connexion internet, ce qui les rend « connectés ».
C'est pourquoi, on distingue un objet connecté d'une interface d'accès au web, cette dernière pouvant cependant prendre la forme d'un objet du quotidien.

2 FONCTIONNEMENT

Les objets connectés sont reliés à Internet : ils peuvent donc communiquer avec d'autres systèmes pour obtenir ou fournir de l'information comme les *data marketing*[1]. Cela est rendu possible par la forte miniaturisation des composants électroniques, mais aussi par l'émergence de nouveaux réseaux de télécommunication (*voir ci-après*).

Les objets connectés pourront par exemple :

- ⇨ collecter et stocker des données en fonction de leur environnement : rythme cardiaque de l'utilisateur, hygrométrie d'une cave, etc.
- ⇨ traiter des données et informations recueillies sur le web et l'environnement de l'objet, puis déclencher des actions en conséquence, comme par exemple l'arrosage d'une pelouse à la veille d'une forte journée de sécheresse. ;
- ⇨ diffuser des informations, comme par exemple les lunettes connectées dédiées aux personnes malvoyantes ou aveugles, qui grâce à leurs caméras et leurs systèmes de reconnaissance faciale qui analysent les éléments environnants pour avertir leurs utilisateurs de ce qui les entoure. Ces informations, traduites en sons ou en paroles, les guident dans leur parcours, identifient les personnes qui les entourent (si les personnes sont déjà enregistrées dans le logiciel des lunettes).

TRAVAIL À FAIRE 1.

Rechercher un exemple d'objet connecté qui collecte, stocke, traite et diffuse des données.

[1] marketing fondé sur l'utilisation des données

Si certains objets connectés, de par leur nature, peuvent être raccordés à un réseau wifi domestique ou professionnel (par exemple une balance corporelle connectée), de nombreux autres sont destinés à être utilisés partout en mobilité. Une des problématiques va donc être de trouver un moyen de faire communiquer ces objets avec une autonomie énergétique suffisante, et pour un coût raisonnable.

On peut alors se demander quel réseau de communication utiliser ?

Les réseaux de télécommunication des objets :

La communication GSM directe : cette solution consiste à utiliser les réseaux de données existants (3G, 4G, etc.). Très peu adaptée dans la majorité des cas, elle nécessite une carte SIM, et utilise une technologie très consommatrice d'énergie. De plus, elle est relativement onéreuse.

L'utilisation du Bluetooth : cette solution consiste à se connecter à un smartphone équipé de Bluetooth pour se servir de la connexion de ce dernier au réseau Internet. Dans ce cas, la consommation énergétique est moindre, mais la dépendance au smartphone peut être problématique.

Les réseaux M2M et *IoT* dédiés : ces dernières années, on a vu apparaître des réseaux de télécommunication dédiés aux objets connectés. Ces derniers ne nécessitent pas de carte SIM et offrent des consommations très réduites. Ils sont conçus pour transmettre un volume restreint de données (quelques octets).

Les protocoles dédiés aux objets connectés :
Le Bluetooth à basse consommation : BLE (Bluetooth Low Energy) : portée courte mais faible consommation
LoRa (Long Range) (ou LoraWAN) est un protocole de communication sans fil développé pour les objets connectés. Il permet à de nombreux objets connectés différents de communiquer entre eux en utilisant une bande de fréquence dédiée. Il est conçu pour offrir une portée étendue et offre une faible consommation énergétique.
Le protocole radio de Sigfox (3D-UNB), utilise une technique d'émission appelée bande ultra-étroite (UNB pour Ultra Narrow Band en anglais), ce qui réduit significativement le bruit tout en permettant des communications longue distance.

Sigfox et LoRaWAN sont donc deux technologies très prometteuses pour le développement de l'Internet des objets. Basées sur le modèle de communication des réseaux étendus à faible puissance. Ces protocoles réseau permettent un déploiement à grande échelle et une couverture réseau étendue, pour une faible consommation énergétique et un coût économique très avantageux.

Zigbee est un protocole de communication sans fil qui se concentre sur la simplicité et la faible consommation d'énergie plutôt que sur la portée étendue.

L'acronyme **M2M** (*Machine to Machine*, communication de machine à machine, communication inter-machines…) est utilisé pour parler de l'ensemble des outils TIC (technologies de l'information et de la communication), déployés pour permettre à des machines de communiquer entre elles sans qu'il n'y ait une intervention humaine.

Dans un tel système, les équipements sont donc connectés en réseau et exécutent des opérations spécifiques sans avoir besoin d'opérateur.

On peut prendre l'exemple de capteurs de chaleur, d'humidité ou de vibrations qui envoient les données recueillies à un serveur. Ensuite, un logiciel se charge de les traiter et de les analyser pour, finalement, générer des alertes à l'adresse des utilisateurs.

L'*IoT* (*Internet of Things* - Internet des Objets) est assez proche du M2M. On peut considérer que l'IoT est une version plus étendue du *Machine to Machine* et surtout plus ouvert. Ouvert dans la mesure où le traitement et la transmission de données sont dématérialisés via Internet. Les données, captées en masses, sont envoyées sur une plateforme de type Cloud. Ici, donc, les objets (les machines) interagissent avec leur environnement et communiquent dans un réseau beaucoup plus élargi.
Au sein de ce système, les machines connectées sont généralement identifiées par une adresse IP, de la même manière qu'un ordinateur relié à internet.

TRAVAIL À FAIRE 2. À PARTIR DE RECHERCHES SUR INTERNET.

1. Trouvez des exemples d'objets connectés et compléter le tableau ci-dessous.

Catégories	Exemples	Usage
Pour les particuliers	La montre connectée	La « montre intelligente » est une montre électronique qui intègre des fonctions de communication élaborées : réception-émission d'appels téléphoniques, notifications provenant d'un téléphone mobile, envoi et réception de messages, reconnaissance vocale. Elle est connectée à un smartphone via une liaison Bluetooth. En général elle est équipée d'un écran tactile qui permet de personnaliser l'affichage en changeant le cadran.
Dans la maison	Le thermostat connecté	Il règle automatiquement votre température de maison ou alors de façon manuelle grâce à un smartphone.
En ville (smart city)		
Dans le commerce		
Dans les industries		
Dans l'agriculture		
Dans la santé		

3 LES DANGERS

Selon le ministère de l'Economie, "le développement des objets connectés expose principalement les consommateurs à deux types de risques : l'utilisation commerciale des données personnelles/sensibles et le piratage". Se pose également le problème de l'atteinte à la vie privée des utilisateurs.

TRAVAIL À FAIRE 3. À PARTIR DE LA LECTURE DES LIENS CI-DESSOUS

https://linc.cnil.fr/fr/risques-des-objets-connectes-sur-la-vie-privee-lanalyse-de-doctorants-en-securite-redocs
https://www.lexpress.fr/economie/high-tech/piratage-des-jouets-vtech-des-millions-de-donnees-parents-et-enfants-recuperees_1741350.html

Expliquez en quoi la vie privée des utilisateurs des objets connectés peut être exposée ?

TRAVAIL À FAIRE 4. À PARTIR DE RECHERCHES SUR INTERNET.

Trouvez des exemples concrets de dangers liés à l'usage des objets connectés.

4 COMMENT SE PROTÉGER ?

Après l'achat, sécurisez bien la connexion aux autres appareils communicants, en procédant régulièrement aux mises à jour de sécurité et mises à jour logicielles. L'idée est de limiter les vulnérabilités connues qui pourraient être exploitées par des personnes ou des organisations malveillantes.
Changez fréquemment le nom et le mot de passe par défaut de chaque objet connecté : la faille qu'exploitent les pirates est encore trop souvent l'absence de vigilance des utilisateurs !
Limitez l'accès de l'objet connecté aux autres appareils électroniques ou informatiques.
Par exemple, si vous avez une TV connectée, vous devrez vous assurer de modifier le mot de passe par défaut et choisir un réseau personnel, sécurisé, avec une clé de protection adéquate pour le Wifi et le routeur.
Même chose pour les mots de passe des services et sites internet. Il faut éviter la redondance et utiliser des mots de passe robustes. N'oubliez pas de restreindre l'accès à votre réseau personnel et d'isoler son accès à internet des autres éléments connectés au réseau (il n'est pas vraiment nécessaire que votre imprimante soit connectée à votre TV, par exemple).

L'INTELLIGENCE ARTIFICIELLE

5 DÉFINITION

L'intelligence artificielle représente tout outil utilisé par une machine afin de *« reproduire des comportements liés aux humains (ou dépasser les capacités humaines), tels que le raisonnement, la planification et la créativité* ».
On utilise le terme "d'intelligence artificielle" pour désigner les ordinateurs et programmes informatiques capables de performances habituellement associées à l'intelligence humaine. Par exemple, la capacité à interagir avec l'homme, à traiter de grandes quantités de données ou encore à apprendre progressivement et donc, à s'améliorer de manière continue.

6 FONCTIONNEMENT

L'intelligence artificielle est rendue possible par une combinaison de 3 facteurs : une vaste quantité de données, une puissance informatique extraordinaire, notamment grâce au cloud et des algorithmes révolutionnaires, basés sur l'apprentissage profond (*deep-learning*).

Tout comme l'intelligence humaine, l'intelligence artificielle fonctionne grâce à l'interconnexion d'un réseau de neurones. Les experts ont créé des équations avec des paramètres variables. Les équations sont interconnectées ce qui permet alors une stimulation intellectuelle artificielle. Concrètement, le savoir de l'IA résulte de ces équations, que l'on appelle aussi unités de fonctionnements. Celles-ci s'enrichissent constamment et fonctionnent entre elles. Ainsi, ce réseau de neurones artificiels intègre les données que l'humain souhaite traiter.

Les équations permettent d'extraire les informations les plus importantes. Avec cette interconnexion de neurones artificiels, l'intelligence artificielle s'apparente au fonctionnement du cerveau humain. L'avantage, c'est que l'IA devient de plus en plus performante à mesure qu'elle expérimente, recense et analyse les données. Chaque seconde écoulée lui permet d'affiner ses capacités sensorielles ou motrices. C'est le principe même du *Machine Learning*, on parle alors d'apprentissage autonome.

TRAVAIL À FAIRE 5. À PARTIR DE RECHERCHES SUR INTERNET.

Trouvez des exemples de technologies basées sur l'intelligence artificielle.

TRAVAIL À FAIRE 6. A PARTIR D'INTERNET

Tester le ChatBOT de la page ci-dessous. Qu'apporte-t'il aux utilisateurs ? Quelles en sont les limites ?

http://bacstmg.fr/auxjardinsfleury/

Trouvez des exemples d'utilisation de l'intelligence artificielle dans différents secteurs d'activités.

7 LE CAS CHATGPT

TRAVAIL À FAIRE 7. TEST DU CHATBOT

Posez une question à propos de « l'intelligence de ChatGPT ».
Demander au ChatBot ce qu'il peut vous apprendre.
Comparer vos résultats avec ceux d'un autre compte (si possible). Que pouvez-vous en conclure ?

Posez une question 'non éthique' au ChatBot. Quelle réponse apporte-t-il ?

Comment fonctionne cet outil ? Ce ChatBot est-il différent des ChatBot 'classiques' ?

Qu'est-ce que 'l'alignement de l'intelligence artificielle' ?

8 LES DANGERS DE L'IA.

À mesure que l'IA progresse, certains voient en elle une menace montante. Et il ne s'agit pas uniquement de l'avis du public, mais aussi des experts et des scientifiques. En effet, selon eux, sa capacité grandissante fait que l'intelligence artificielle est capable de faire beaucoup plus que ce que les gens pensent. D'une certaine manière, cela signifierait que les systèmes dits intelligents le sont plus encore. Autrement dit, les humains risquent de perdre le contrôle face à son évolution rapide.

L'IA pourrait d'abord être programmée pour une tâche potentiellement dangereuse. Dans un deuxième cas de figure, elle pourrait être conçue pour une tâche bénéfique, mais en employant des méthodes dévastatrices pour y parvenir.

Alors que l'intelligence artificielle permet d'obtenir des résultats plus précis et plus rapides à un moindre coût, elle met en danger certains emplois. D'après une étude, elle serait en mesure d'effectuer au moins **70 % des tâches des travailleurs humains**. Cela signifie que plus les solutions d'IA deviendront performantes, plus elles menacent de réduire le nombre d'emplois.

L'intelligence artificielle présente l'avantage de contribuer à la **cybersécurité**. Toutefois, elle est elle-même un vecteur des attaques malveillantes. Si elle est un moyen pour les entreprises d'atteindre plus facilement leur objectif, ça l'est aussi pour les malfaiteurs. Nous savons que l'IA implique le traitement d'une quantité massive de données. Cela offre un plus grand champ d'attaque pour les pirates et les hackers. D'autres criminels utilisent des *bots* alimentés par l'IA pour perpétrer des attaques en ligne.

D'autre part, le danger de l'intelligence artificielle concerne aussi la **confidentialité**. Les gouvernements et les forces de l'ordre de plusieurs pays tirent profit de la technologie pour une surveillance de masse. Par exemple, ils utilisent la reconnaissance faciale en s'appuyant sur les données collectées dans les espaces publics à la recherche de criminels.

On peut alors classer les attaques en trois niveaux, du plus faible au plus grave.

8.1 Intelligence artificielle : les menaces de faible intensité.

- ⇨ **Exploitation de préjugés :** tirer profit des biais existants des algorithmes, par exemple les recommandations de YouTube pour canaliser les spectateurs ou les classements de Google pour améliorer le profil des produits ou dénigrer les concurrents.

- ⇨ **Robots cambrioleurs** : utiliser des petits robots autonomes se glissant dans les boîtes aux lettres ou les fenêtres pour récupérer des clés ou ouvrir des portes. Les dommages sont faibles potentiellement, car très localisés à petite échelle.
- ⇨ **Blocage de détection par IA** : déjouer le tri et la collecte de données par IA afin d'effacer des preuves ou de dissimuler des informations criminelles (pornographie par exemple)
- ⇨ **Fausses critiques rédigées par IA** : générer des faux avis sur des sites tels que Amazon ou TripAdvisor pour nuire ou favoriser un produit.
- ⇨ **Traque assistée par IA** : utiliser les systèmes d'apprentissage pour pister l'emplacement et l'activité d'un individu.
- ⇨ **Contrefaçon** : fabriquer de faux contenus, comme des tableaux ou de la musique, pouvant être vendus sous une fausse paternité. Le potentiel de nuisance demeure assez faible dans la mesure où les tableaux ou musiques connus sont peu nombreux.

8.2 Intelligence artificielle : les menaces d'intensité moyenne.

- ⇨ **Robots militaires** : prendre le contrôle de robots ou armes à des fins criminelles. Une menace potentiellement très dangereuse mais difficile à mettre en œuvre, le matériel militaire étant généralement très protégé.
- ⇨ **Escroquerie** : vendre des services frauduleux en utilisant l'IA. Il existe de nombreux exemples historiques notoires d'escrocs qui ont réussi à vendre de coûteuses fausses technologiques à de grandes organisations, y compris des gouvernements nationaux et l'armée.
- ⇨ **Corruption de données** : modifier ou introduire délibérément de fausses données pour induire des biais spécifiques. Par exemple, rendre un détecteur insensible aux armes ou encourager un algorithme à investir dans tel ou tel marché.
- ⇨ **Cyberattaque basée sur l'apprentissage** : perpétrer des attaques à la fois spécifiques et massives, par exemple en utilisant l'IA pour sonder les faiblesses des systèmes avant de lancer plusieurs attaques simultanées.
- ⇨ **Drones d'attaque autonomes** : détourner des drones autonomes ou s'en servir pour s'attaquer à une cible. Ces drones pourraient être particulièrement menaçants s'ils agissent en masse dans des essaims auto-organisés.
- ⇨ **Refus d'accès :** endommager ou priver des utilisateurs d'un accès à un service financier, à l'emploi, à un service public ou une activité sociale. Non rentable en soi, cette technique peut être utilisée comme chantage.
- ⇨ **Reconnaissance faciale** : détourner les systèmes de reconnaissance faciale, par exemple en fabriquant de fausses photos d'identité (accès à un smartphone, caméras de surveillance, contrôle de passagers...)
- ⇨ **Manipulation de marchés financiers** : corrompre des algorithmes afin de nuire à des concurrents, de faire baisser ou monter une valeur artificiellement, de provoquer un crash financier...

8.3 Intelligence artificielle : les menaces graves.

- ⇨ **Fausses vidéos** : usurper l'identité d'une personne en lui faisant dire ou faire des choses qu'elle n'a jamais dite ou faites, dans le but de demander un accès à des données sécurisées, de manipuler l'opinion ou de nuire à réputation de quelqu'un...Ces vidéos truquées sont quasi indétectables.
- ⇨ **Piratage de voitures autonomes** : s'emparer des commandes d'un véhicule autonome pour s'en servir comme arme (par exemple perpétrer une attaque terroriste, provoquer un accident, etc).

- ⇨ **Hameçonnage sur mesure** : générer des massages personnalisés et automatisés afin d'augmenter l'efficacité du phishing visant à collecter des informations sécurisées ou installer des logiciels malveillants.
- ⇨ **Piratage des systèmes contrôlés par l'IA** : perturber les infrastructures en causant par exemple une panne d'électricité généralisée, un engorgement du trafic ou la rupture de la logistique alimentaire.
- ⇨ **Chantage à grande échelle** : recueillir des données personnelles afin d'envoyer des messages de menace automatisés. L'IA pourrait également être utilisée pour générer de fausses preuves (par exemple l'extorsion à l'aide d'images à caractère sexuel).
- ⇨ **Fausses informations rédigées par IA** : écrire des articles de propagande semblant être émises par une source fiable. L'IA pourrait également être utilisée pour générer de nombreuses versions d'un contenu particulier afin d'accroître sa visibilité et sa crédibilité.

8.4 Une technologie émergente de l'intelligence artificielle : le *deepfake*

TRAVAIL À FAIRE 8. FAITES DES RECHERCHES SUR INTERNET AFIN D'EXPLIQUER CETTE NOUVELLE TECHNOLOGIE

9 COMMENT SE PROTÉGER DU DANGER DE L'INTELLIGENCE ARTIFICIELLE ?

Plus l'intelligence devient sophistiquée et performante, plus le danger qu'elle représente s'agrandit. Et cela peut nous affecter tous sans exception, voire mettre notre vie en péril.

Il faudrait prendre le temps d'évaluer les risques et les avantages avant de la déployer à grande échelle. D'une certaine manière, toutes ces menaces pourraient être évitées avec un **développement éthique et responsable de l'IA**. Cela implique avant tout une approche centrée sur l'humain et non sur les avantages technologiques et économiques.

Il est aussi important de définir les limites de l'utilisation des systèmes intelligents en imposant des réglementations plus strictes. De telles initiatives existent déjà, comme le RGPD (règlement général sur la protection des données) et l'*AI Act* (Artificial Intelligence Act), approche réglementaire européenne de l'IA basée sur les risques, sans entraver abusivement le développement technologique.

Nous ne sommes peut-être pas directement menacées par une intelligence surhumaine, mais nous sommes exposés à un risque non négligeable. Aussi, bien que l'intelligence artificielle soit conçue pour être autonome, la supervision humaine reste essentielle pour éviter tout incident pouvant entraîner des conséquences désastreuses.

https://intelligence-artificielle.com/intelligence-artificielle-danger/
https://www.sia-partners.com/fr/perspectives/artificial-intelligence-act-que-faut-il-savoir

La CNIL a publié un rapport de synthèse du débat public qu'elle a animé sur les enjeux éthiques des algorithmes et de l'intelligence artificielle.
Quelles réponses éthiques au développement des algorithmes et de l'intelligence artificielle ?
Deux principes fondateurs ressortent : loyauté et vigilance

Un principe de *loyauté* appliqué à tous les algorithmes et intégrant les impacts collectifs, et pas seulement personnels, de ces derniers. Tout algorithme, qu'il traite ou non des données personnelles, doit être loyal envers ses utilisateurs, non pas seulement en tant que consommateurs, mais également en tant que citoyens, voire envers des communautés ou de grands intérêts collectifs dont l'existence pourrait être directement affectée. **L'intérêt des utilisateurs doit primer**.

Un principe de *vigilance/réflexivité* : il s'agit d'organiser une forme de questionnement régulier, méthodique et délibératif à l'égard de ces objets mouvants. Ce principe constitue une réponse directe aux exigences qu'imposent ces objets technologiques du fait de leur nature imprévisible (inhérente au *machine learning*), du caractère très compartimenté des chaînes algorithmiques au sein desquels ils s'insèrent et, enfin, de la confiance excessive à laquelle ils donnent souvent lieu.

TRAVAIL À FAIRE 9. A PARTIR DU LIEN SUIVANT

https://www.cnil.fr/fr/comment-permettre-lhomme-de-garder-la-main-rapport-sur-les-enjeux-ethiques-des-algorithmes-et-de

Quelles recommandations ont été proposées pour mettre en application les principes cités ci-dessus ?