### République Algérienne Démocratique et Populaire

Ministère de l'enseignement Supérieur et de la Recherche Scientifique

### Université des Sciences et de la Technologie Houari Boumediene

Faculté Informatique

Département IA et SD

### Mémoire de Licence

Filière Informatique Spécialité Académique

Thème:

### la détection de fausses informations (fake news) par Machine learning sous python

Soutenu le :19/06/2022.

Sujet Proposé par :

M.BOURAOUI Seyfalah

Présenté par :

KERROUCHE Rayane

REMILI Karima

Devant le jury composé de : Mr GUERROUMI Mohamed

Mr BERBER Ahmed

Binôme : 154  $^{\rm 0}$ 

2021 / 2022

### Remerciements

Nous tenons premièrement à prosterner remerciant Allah le tout puissant de nous avoir donné le courage et la patience pour terminer ce travail. Nous voudrons tout d'abord remercier notre encadreur de mémoire, Monsieur Bouraoui Seyfallah, de nous avoir encadré, orienté, aidé et conseillé. Nous adressons nos sinceres remerciements aux membres du jury qui ont accepté d'évaluer notre travail.

Nous tenons à remercier nos familles qui ont contribué à alimenter notre réflexion ainsi les maintes conseils proposés qui nous ont aidé à atteindre l'objectif voulu.

### Table des matières

In	trodu	iction	générale	6
1	État	d'art		8
	1.1	Introd	uction	9
	1.2	Défini	ition des fakes news	9
	1.3		vpes des fakes news	9
		1.3.1	Information fabriquée	9
		1.3.2	Propagande numérique	9
		1.3.3	Théories	10
		1.3.4	Canulars	10
		1.3.5	Information biaisée ou unilatérale	10
		1.3.6	Rumeur	10
		1.3.7	Titres accrocheurs	10
		1.3.8	Nouvelles satiriques	10
		1.3.9	Publicités trompeuses (misleading ads)	10
		1.3.10	Mendicité en ligne (online begging)	10
	1.4	Les co	omposants des fausses nouvelles	11
		1.4.1	Créateur/Diffuseur de fausses nouvelles	11
		1.4.2	Contenu d'actualité	11
		1.4.3	Contexte sociale	11
	1.5	Les im	pacts des fausses nouvelles	12
	1.6		CLUSION	12
2			des de détection de fake news	13
	2.1		duction	14
	2.2		roche linguistique de détection de fakes news	14
		2.2.1	La représentation de texte	14
		2.2.2	L'analyse syntaxique en profondeur (Deep Syntax)	14
		2.2.3	L'analyse sémantique	15
		2.2.4	L'analyse du discours	15
	2.3	L'app	roche automatique de fact-checking	15
		2.3.1	La vérification par les foules, crowdsourced fact-checking	15

		2.3.2 La mise à disposition d'experts
		2.3.3 L'utilisation de l'Intelligence artificielle (IA)
	2.4	L'approche basée sur le style de l'information
		2.4.1 La théorie des 4 facteurs
		2.4.2 Le réflexe de Semmelweis
		2.4.3 L'illusion de la vision asymétrique
		2.4.4 L'effet de l'écho-chambre
	2.5	L'approche basée sur la propagation de l'information
		2.5.1 Les techniques basées sur la propagation en cascade
		2.5.2 Les techniques basées sur le réseau de la diffusion
	2.6	Modèle conceptuel de l'EMI à l'épreuve des fake news
	2.7	scrapping
		2.7.1 Définition
		2.7.2 Les stratégies
		2.7.3 Différence entre les 2 stratégies
	2.8	Conclusion
3	mac	chine learning sous python 20
	3.1	Introduction
	3.2	Définition
	3.3	Les types de Machine Learning
		3.3.1 Apprentissage supervisé
		3.3.2 Apprentissage non-supervisé
		3.3.3 Apprentissage semi-supervisé
		3.3.4 Apprentissage par renforcement
	3.4	Les applications du Machine Learning
	3.5	Le langage python pour la Machine Learning
	3.6	Importer les librairies dans un IDE Python
	3.7	Quelle est la différence entre le Machine Learning et le Deep Learning? 25
	3.8	Détection des fausses nouvelle avec machine learning (mendicité )
	3.9	Conclusion
4	Imp	plémentation(MLP,Deep learning,ADD) 27
	4.1	Introduction
	4.2	Outils utilisée
		4.2.1 Logiciels utilisés
		4.2.2 Langages utilisés
		4.2.3 Bibliothèques utilisées
	4.3	Résultats
	4.4	Formule qui calcule le poids
	4.5	Formule qui calcule la moyenne

					`	
$T\Delta$	RI	F	DES	$M\Delta$	TIER	FS

4.6	Décisio	on	34
4.7	Les rés	seaux de neurones pour la détection et la modicité	35
	4.7.1	Perceptron multicouche	35
	4.7.2	La fonction d'activation	36
	4.7.3	Rétropropagation	37
	4.7.4	Implémentation d'un réseau de neurones en Python	38
	4.7.5	première prédiction	38
	4.7.6	Calcul de l'erreur de prédiction	39
Conclu	sion et	perspectives	39

### Table des figures

2.1	Modèle conceptuel de l'EMI à l'épreuve des fake news	18
3.1	Schéma explicatif de l'apprentissage supervisé	22
3.2	Schéma explicatif de l'apprentissage par renforcement	23
3.3	Environnement de développement en Python pour le ML	25
4.1	IDE pycharm	28
4.2	DB Browser	29
4.3	Exemple d'utilisation de la bibliothèques pandas	30
4.4	Exemple d'utilisation de la bibliothèques Youtube comment scraper python	30
4.5	Exemple d'utilisation de la bibliothèques Matplotlib	31
4.6	Exemple d'utilisation de la bibliothèques Numpy	31
4.7	Exemple d'utilisation de la bibliothèques Csv	31
4.8	Exemple d'utilisation de la bibliothèques Sqlite3	32
4.9	fichier csv qui contient les commentaires	32
4.10	fichier csv des commentaires	33
4.11	la base de données	33
4.12	Graphe d'apprentissages et test	34
4.13	La table de décision	35
4.14	Le perceptron	36
4.15	La fonction segmoide	37

### Introduction générale

"Il y a 200 ans, 99,999 % des idioties n'étaient pas enregistrées. Maintenant nous avons Internet." Steve Paulson (2018)[1]. "— Vrai, faux, peu importe, ce qui compte c'est que les gens sachent." Patrick McGuinness[2], Les cent derniers jours Comme le rapporte le blog du rapport Watters, le terme "fake news" (ou infox, ou fausses nouvelles diffusées par le Bulletin du gouvernement américain n°29 du 4 octobre 2018) s'est propagé lors des élections de 2016 aux États-Unis. Les causes sont multiples : crise du journalisme, crise civile, politique mais aussi crise de l'éducation et de la technique, du savoir, de l'expertise et de la science (voir [3] pour une analyse de la responsabilité), même des Émotions fortes ont eu une influence premier symptôme de contamination, le contenu générant des émotions fortes, particulièrement la colère, se répand plus rapidement sur les réseaux sociaux. Il n'est donc pas étonnant d'apprendre que les créateurs de fausses nouvelles essaient de nous faire peur ou de nous choquer. Ces causes multiples compliquent son analyse. Selon le Dictionnaire Le Collins[?] une infox est "une information fausse, souvent sensationnelle, diffusée sous le couvert de reportages". Par conséquent, c'est de la désinformation présentée de manière journalistique pour reconnaître ses réalisations. Ce terme s'est propagé en parallèle au terme "post Truth" (post vérité), qui ne signifie pas qu'on se situe après la vérité, mais que cette dernière est devenue moins importante, moins pertinente[4]. Une étude de l'économiste Roberto Cavazos de l'université de Baltimore permet de se rendre compte de l'impact économique immédiat de ces fakes news. Ainsi, selon l'étude, au moins 400 millions de dollars ont été dépensés pour la diffusion Fake news dans les campagnes politiques lors des dernières élections indiennes (140 M en 2019), Brésil (34 M en 2018), Royaume-Uni (1 millions), France (586 000 €), Australie (828 000), Kenya (20 millions), l'Afrique du Sud (2,7 millions) ou le Mexique (642 000 USD)[5]. Ce n'est là qu'un exemple de l'intérêt pour la détection des fausses nouvelles.

### Notre mémoire est constitué de 4 chapitres :

- 1 États d'art sur la détection des fakes news : ayant des informations générales concernant les fakes news.
- 2 Les méthodes de détection de fake news : nous verrons le web scraping ainsi que les principales méthodes utilisées afin de détecter les fakes news.
- 3 Machine learning sous python.
- 4 Implémentation : mise en œuvre du travail.

### Chapitre 1

### État d'art

### Contents

1.1	Intro	oduction
1.2	Déf	inition des fakes news
1.3	Les	types des fakes news
	1.3.1	Information fabriquée
	1.3.2	Propagande numérique
	1.3.3	Théories
	1.3.4	Canulars
	1.3.5	Information biaisée ou unilatérale
	1.3.6	Rumeur
	1.3.7	Titres accrocheurs
	1.3.8	Nouvelles satiriques
	1.3.9	Publicités trompeuses (misleading ads)
	1.3.10	Mendicité en ligne (online begging)
1.4	Les	composants des fausses nouvelles
	1.4.1	Créateur/Diffuseur de fausses nouvelles
	1.4.2	Contenu d'actualité
	1.4.3	Contexte sociale
1.5	Les i	impacts des fausses nouvelles
1.6	CON	NCLUSION

1.1. INTRODUCTION 9

### 1.1 Introduction

A l'ère des réseaux sociaux, la consommation d'informations s'est multipliée à un niveau sans précédent. Le phénomène des fausses nouvelles a beaucoup attiré l'attention ces dernières années vu sa grande influence sur les individus et la société moderne. Dans ce qui suit, nous essayons de fournir une vision claire du concept de fausses nouvelles et ses dérivés. Nous avons utilisé un terme plus général "fakes news" pour identifier clairement les divers aspects d'une fausse nouvelle. De plus amples informations ont également été présentées sur les principaux distributeurs de contrefaçons d'informations et de leurs objectifs et motivations.

### 1.2 Définition des fakes news

Le terme "fake news" est composé de deux mots anglais, "fake" et "news" . Ces messages délibérément trompeurs cherchent à attirer l'attention avec ce qui semble être "authentique" afin de choquer ou d'influencer les opinions des autres . Les fausses nouvelles sont rédigées par des individus et des groupes qui agissent pour leur propre bénéfice ou pour celui d'autrui . La création de cette désinformation est avant tout personnelle, politique ou financièrement motivée. Cependant, la diffusion d'informations falsifiées pour façonner les opinions sociales sur une question particulière n'est en aucun cas une nouvelle stratégie . Depuis l'existence de l'imprimerie, des gros titres passionnants, des articles mensongers et de la publicité à des fins politiques ont été utilisés. Mais à l'ère de l'échange d'informations numériques, ces fausses nouvelles sont devenues un phénomène en ligne difficile à contrôler . En partageant des publications sur les réseaux sociaux et en utilisant des robots de réseaux sociaux pour imiter les utilisateurs humains et diffuser de fausses nouvelles encore plus rapidement, ils atteignent rapidement une grande visibilité .

### 1.3 Les types des fakes news

La fake news se présente sous différentes formes. Chose importante à noter que la désinformation peut résulter du chevauchement de plusieurs catégories à la fois, parmi les huit catégories suivantes [6] :

### 1.3.1 Information fabriquée

Une information complètement imaginaire qui n'a aucune relation avec des faits réels.

### 1.3.2 Propagande numérique

Il s'agit d'une sous-forme spécifique d'informations fabriquées. Ce cas les fausses nouvelles ont été largement utilisées pendant la Seconde Guerre mondiale et la Guerre froide. La propagande est largement utilisée dans des contextes politiques pour influencer un public cible, dans le but de propager des idées, des projets politiques, des idéologies ou discréditer un parti

politique particulier ou un État national. La propagande est même possible changer le cours de l'histoire, comme l'invasion de l'Irak en 2003.

### 1.3.3 Théories

Du complot : référer à des récits théoriques qui expliquent des situations ou faits en invoquant des conspirations sans aucune preuve.

### 1.3.4 Canulars

: nouvelles contenant des informations fausses ou inexactes destinées à être Utilisées à mauvais escient la confiance de quelqu'un. Ils sont également connus comme des demi-vérités ou des factoïdes.

### 1.3.5 Information biaisée ou unilatérale

Ce type est appelé les nouvelles hyper-partisanes, des faits qui sont biaisées à l'intérêt d'une personne, d'un parti, d'une situation ou d'un événement.

#### 1.3.6 Rumeur

Un récit dont la source est inconnue et la véracité est ambiguë.

#### 1.3.7 Titres accrocheurs

Signifie l'utilisation intentionnelle de titres trompeurs sur le Web dans le but d'attirer plus de lecteurs. C'est un vieux type de fake news connu sous le nom de presse jaune.

### 1.3.8 Nouvelles satiriques

Un texte moqueur ou un contenu visuel critiquant des situations, personne, organisation ou gouvernement. Ce genre de nouvelles attire plus attention sur le net.

### 1.3.9 Publicités trompeuses (misleading ads)

Une publicité trompeuse est toute publicité qui, d'une manière quelconque, y compris sa présentation, est susceptible d'induire en erreur les personnes auxquelles elle s'adresse et d'influencer leur choix ou de porter préjudice à un concurrent. Une telle publicité est interdite par la loi.

### 1.3.10 Mendicité en ligne (online begging)

C'est un moyen de mendier a travers internet en racontant des histoires tragiques, axés sur le côté émotionnel principalement à l'aide de faux comptes. Ce sont souvent des histoires fausses, car ils maîtrisent la création de processus imaginaires. Ce phénomène a été exacerbé par l'émergence de demandes d'assistance financière électronique, destinées à répondre aux besoins vitaux, au traitement d'un patient souffrant d'une maladie grave ou à la collecte de fonds pour les victimes d'accidents de la route.

### 1.4 Les composants des fausses nouvelles

Le professeur Oihab Allal-Chérif Explique : "Les théories complotistes institutionnelles et malveillantes sont reprises par ceux qui y croient, qui les interprètent, les font évoluer, les combinent, et les relaient sous des formes différentes. Il s'agit d'une "uberisation" des fakes news ou chacun en devient à la fois consommateur, producteur et diffuseur. Dans un monde où tout le monde se prend pour un expert et est victime de biais cognitifs, chacun pense qu'il est de son devoir d'alerter les autres sur ce qu'il a découvert ou compris et que des forces occultes nous cacheraient" [7]. Le terme Fake News se base sur quatre composants principaux :

### 1.4.1 Créateur/Diffuseur de fausses nouvelles

Derrière la circulation de fausses informations se cache bien souvent une créateur/diffuseur qui peut être soit un humain, soit non :

- Humain : Ne sont que les porteurs de fausses nouvelles sur les médias sociaux.
- Non humain : Les robots sociaux ou « bots » sont des algorithmes programmés pour compléter une série de tâches sur les réseaux sociaux. Ils sont très efficaces pour publier et relayer des informations parfois douteuses. Les comptes qui propagent activement de la désinformation sont d'ailleurs plus souvent des robots que de réels utilisateurs influents.

### 1.4.2 Contenu d'actualité

chaque nouvelle est compose de deux types (physique et non physique :

- Le contenu physique : des fausses nouvelles contient le titre de la nouvelle, le corps de la nouvelle, des images, des vidéos, des hashtags, des signaux de mention, des emojis,...etc
- Le contenu non physique : le contenu non physique concerne les opinions, les émotions, attitudes et sentiments que les créateurs de nouvelles veulent exprimer.

#### 1.4.3 Contexte sociale

Le contexte social fait référence à l'ensemble du système d'activités et à l'environnement social dans lequel l'information est diffusée. Aujourd'hui, les technologies interactives sur les réseaux sociaux dominent de plus en plus les modes de partage d'actualités. Les utilisateurs en ligne peuvent non seulement se renseigner sur les tendances, mais aussi partager leurs histoires et leur soutien. S'ils partagent ces expériences et interactions dans certains groupes sociaux et membres partageant les mêmes idées de ces groupes, l'effet de ces derniers peut être amplifié. Cela facilite la diffusion de fausses nouvelles. Il se propage sur les réseaux sociaux beaucoup plus rapidement et plus longtemps que les vrais. Et la structure de leur propagation n'est pas la même. Sur la base de ces caractéristiques, des chercheurs en sciences computationnelles mettent en place des projets d'intelligence artificielle visant à détecter automatiquement de telles "fake news"

### 1.5 Les impacts des fausses nouvelles

Les fausses nouvelles sont un réel danger car elles visent des manipulations de toutes sortes (politiques, sanitaires, économiques, sociales, etc.). En faisant passer le mot "faux" pour "vrai", les fausses nouvelles créent une confusion dans l'esprit du public et peuvent provoquer certaines personnes, des mouvements de foule, etc... En matière politique, une fausse nouvelle sur une personnalité politique, diffusée en masse sur Internet, peut facilement ternir l'image de cette personnalité politique. Sur le plan social, dans le contexte d'un climat social tendu, les soirées sur les réseaux sociaux de fake news peuvent provoquer des polémiques pouvant déboucher sur des cas de violence.

### 1.6 CONCLUSION

Dans ce chapitre, différents concepts de fake news ont été introduits. Nous avons vu leurs significations, leurs caractéristiques ainsi que les différents modèles utilisés pour les détecter. La désinformation prend de nombreuses formes, allant d'une simple blague à des campagnes de propagande bien organisées et à des rumeurs. Les acteurs qui contribuent à la diffusion de ce type d'informations ont de nombreuses intentions et motivations différentes, ainsi que des objectifs variés. Comprendre les différents aspects de ce phénomène peut aider à concevoir des solutions plus efficaces et plus convaincantes.

### Chapitre 2

2.8

### Les méthodes de détection de fake news

Contents	<b>;</b>		
2.1	Int	roduction	14
2.2	L'a	pproche linguistique de détection de fakes news	14
	2.2.1	La représentation de texte	14
	2.2.2	L'analyse syntaxique en profondeur (Deep Syntax) $\ \ldots \ \ldots \ \ldots$	14
	2.2.3	L'analyse sémantique	15
	2.2.4	L'analyse du discours	15
2.3	L'a	pproche automatique de fact-checking	<b>15</b>
	2.3.1	La vérification par les foules, crowdsourced fact-checking	15
	2.3.2	La mise à disposition d'experts	15
	2.3.3	L'utilisation de l'Intelligence artificielle (IA)	16
2.4	L'a	pproche basée sur le style de l'information	16
	2.4.1	La théorie des 4 facteurs	16
	2.4.2	Le réflexe de Semmelweis	16
	2.4.3	L'illusion de la vision asymétrique $\ \ldots \ \ldots \ \ldots \ \ldots$	16
	2.4.4	L'effet de l'écho-chambre	16
2.5	L'a	pproche basée sur la propagation de l'information	17
	2.5.1	Les techniques basées sur la propagation en cascade	17
	2.5.2	Les techniques basées sur le réseau de la diffusion	17
2.6	Mo	dèle conceptuel de l'EMI à l'épreuve des fake news	17
2.7	scra	apping	18
	2.7.1	Définition	18
	2.7.2	Les stratégies	18
	2.7.3	Différence entre les 2 stratégies	19

### 2.1 Introduction

Au vu de la large diffusion des fausses informations et des fausses nouvelles en particulier, en plus de leur effet odieux, de nombreuses études ont été menées à l'échelle internationale sur la façon dont les gens perçoivent et utilisent les médias, les informations et les fausses informations afin de les réduire. En effet, pour mieux comprendre la vitalité et l'efficacité des fake news, une des clés est le contexte de consommation de l'information et, plus largement, un sentiment de confiance ou de méfiance envers les institutions.

Dans ce chapitre, on va identifier les principaux fondements théoriques sur lesquelles sont fondées ces études ainsi que les méthodes utilisées afin de détecter les fakes news. On va aborder aussi le scraping et ses stratégies

### 2.2 L'approche linguistique de détection de fakes news

Distinguer les bonnes et les mauvaises informations est simplement une distinction entre la vérité et le mensonge, un domaine où la linguistique continue d'apporter sa contribution. Par conséquent, il est très logique qu'un système de détection automatique de fausses nouvelles emprunte théorie et modèle à la même linguistique, et son application est moins évidente dans le contexte de grandes quantités de données. En effet, l'analyse prédictive du texte a permis de développer un système linguistique permettant de détecter les fausses informations. Il s'agit d'une étude des «« l'interrelation entre les marqueurs linguistiques et l'action considérée comme une activité intentionnelle, consciente et subjectivement significative »[8]. Plus précisément, Le modèle d'analyse prédictive utilisé dans le système de détection est basé sur celui proposé par Feng et al : la plupart des menteurs utilisent en oral ou en écrit le langage de manière stratégique pour leurrer leur public[9]. Malgré les tentatives de contrôler leur discours, une « fuite de langage » se produit. Cela peut être identifié par des caractéristiques linguistiques spécifiques, en particulier la fréquence des mots, l'utilisation des pronoms, les conjonctions et les mots avec des émotions négatives. Le but de l'approche linguistique est de rechercher de telles "lacunes" dans le contenu du message. Cette approche se concentre sur l'utilisation de la technologie d'apprentissage automatique (Machine learning). Plusieurs processus sont répertoriés pour les méthodes de détection automatique des fausses nouvelles, dont les plus typiques sont:

### 2.2.1 La représentation de texte

Ètant considérée comme la méthode la plus simple car elle ne s'intéressait qu'à un seul mot qui était agrégé et analysé pour révéler des preuves de tromperie.

### 2.2.2 L'analyse syntaxique en profondeur (Deep Syntax)

qui est, en Traitement Automatique des Langues. Elle ne suffit pas non seulement d'analyser superficiellement les mots, mais aussi d'étudier les phrases qui les contiennent et leur structure

syntaxique.

### 2.2.3 L'analyse sémantique

L'analyse sémantique propose de rechercher le sens et le signifié. Dans ce cas, le sens et le format sont requis. Par conséquent, elle étend la puissance de l'analyse syntaxique en recherchant des indicateurs de véracité obtenus en analysant le degré de compatibilité entre le message contenu dans le texte et le profil de son auteur.

### 2.2.4 L'analyse du discours

La Théorie de la Structure Rhétorique, elle propose une explication de la cohérence des textes, une fonctionnalité importante que le système de détection de fausses nouvelles ne peut pas manquer. Appliquer la rhétorique à l'information numérique peut indiquer une tromperie, mais son application, comme le constate Conroy et al. (2015) reste actuellement relativement limitée.

### 2.3 L'approche automatique de fact-checking

Le fact-checking est devenue un outil essentiel permettant aux citoyens de découvrir la vérité. L'utilisation d'appareils techniques est plus courante. Elle consiste à utiliser la technologie de l'intelligence artificielle (IA) pour comparer des informations potentiellement incorrectes avec de nouvelles informations provenant de sources qui étaient auparavant considérées comme fiables [10]. Cette approche repose sur l'existence d'une base de connaissances humaines validée, structurée et accessible au public. Les recherches informatiques sur ces outils de validation automatisés ont permis de développer des plug-ins de navigateur capables de calculer en temps réel des pourcentages de fiabilité des informations [11]. C'est le cas du projet Trooclick, lancé en France en 2013 et spécialisé dans l'information financière. La fact-checking, une pratique ancienne de vérification des informations, commence également à évoluer sous l'influence de l'intelligence artificielle et des nouvelles pratiques sociales en ligne. Le fact-checking poursuit son efficacité, comme en témoignent de nombreux processus :

### 2.3.1 La vérification par les foules, crowdsourced fact-checking

Une forme de collaboration entre les humains et la technologie qui reconnaît les aspects sociaux et cognitifs qui n'auraient pas existé sans elle en tirant parti de l'intelligence de la foule pour obtenir des informations. La compréhension est toujours incomplète.

### 2.3.2 La mise à disposition d'experts

C'est une méthode intéressante, mais qui n'est pas pratique compte tenu de l'utilisation généralisée de fausses informations sur Internet. De plus, le site Web en question ne comprend pas de vérificateur, de sorte que les utilisateurs n'ont pas la possibilité de fournir toutes les informations dans tous les domaines.

### 2.3.3 L'utilisation de l'Intelligence artificielle (IA)

L'utilisation de l'IA pour la vérification automatisée des informations a donné naissance à plusieurs applications qui n'atteignent pas toujours la même efficacité. La principale raison en est que ces applications doivent utiliser une base de données existante contenant des informations valides et à jour sur un sujet particulier (Conroy et al, 2015). De plus, comme le déclare, « en calculant automatiquement le degré de fiabilité d'une information, ces applications semblent repousser très loin la part de l'humain dans le jugement de fiabilité et introduire "du sens" dans la machine »[11]. Certains modèles fournissent des indices sur la véracité des informations, mais indiquent qu'il est impossible pour les utilisateurs finaux de savoir comment interpréter et interagir avec ces prédictions. D'où sa proposition d'une approche mixte centrée sur l'humain.

### 2.4 L'approche basée sur le style de l'information

Les méthodes de détection basées sur les connaissances visent à évaluer l'authenticité des informations, tandis que les méthodes basées sur le style tentent d'évaluer l'intention des informations. Ces méthodes examinent un ensemble de propriétés quantifiables qui permettent d'exprimer la tromperie dans les nouvelles et de la distinguer de la vérité. Nous allons voir maintenant les théories de style de déception :

#### 2.4.1 La théorie des 4 facteurs

Les mensonges s'expriment de différentes manières en termes d'excitation (degré de provocation), de contrôle comportemental, d'émotions et de raisonnement.

### 2.4.2 Le réflexe de Semmelweis

Les individus ont tendance à rejeter les nouvelles preuves parce qu'elles contredisent les normes et croyances établies.

### 2.4.3 L'illusion de la vision asymétrique

Les gens perçoivent leurs connaissances comme supérieures à celles des autres.

### 2.4.4 L'effet de l'écho-chambre

Les croyances et les convictions sont amplifiées ou renforcées par la communication et la répétition dans un système fermé.

### 2.5 L'approche basée sur la propagation de l'information

Les méthodes basées sur la diffusion de l'information étudient les données pertinentes. Qui sont reliées à la diffusion de fausses informations, c'est-à-dire comment se propagent-elles et comment elles sont diffusées par les utilisateurs. Par cette approche nous verrons 2 techniques :

### 2.5.1 Les techniques basées sur la propagation en cascade

La plupart des études utilisent le modèle en cascade comme expression formelle pour diffuser de fausses informations. Le modèle cascade a une structure arborescente dites pseudo-arbre qui représente la propagation de fausses informations sur les réseaux sociaux. Le nœud racine représente l'utilisateur (auteur) qui a initialement publié les mauvaises informations, et les autres nœuds représentent les utilisateurs qui se connectent au nœud racine qui partagent et republient la fausse information par la suite.

### 2.5.2 Les techniques basées sur le réseau de la diffusion

La méthode basée sur le réseau de diffusion construit un réseau flexible pour capter indirectement la diffusion de fausses informations. Ces réseaux contiennent différents types de nœuds qui sont connectés par différents types de relations. Ces relations sont analysées dans le but de détecter des informations incorrectes à l'aide de plusieurs méthodes telles que les modèles probabilistes, l'apprentissage multitâche et l'algorithme PageRank.

## 2.6 Modèle conceptuel de l'EMI à l'épreuve des fake news

Sur la base des recommandations des déclarations de Moscou, un modèle conceptuel a émergé pour aider à établir la politique d'EMI. Ils ont l'avantage d'apporter une vision macro des enjeux de l'information dans la société et l'inconvénient d'éviter plutôt certains enjeux de fake news. Son objectif est de proposer une approche humaine de la détection de la désinformation, une alternative à l'information technologique, et permettra à toute personne ayant un besoin d'information de l'utiliser efficacement en toute indépendance. Il s'agit d'une approche individuelle et collaborative dans le sens où elle appelle à la socialisation des résultats du processus d'information à travers un système de recommandation si l'information est digne de confiance ou signalant si ce n'est pas une fausse nouvelle[12]. Comparé aux modèles de détection automatique des fake news, ce modèle présente plusieurs qualités :

- Il n'est basé sur aucune technologie ou aucun algorithme dont on n'ignore le fonctionnement
- Il utilise les capacités humaines de traitement de l'information.

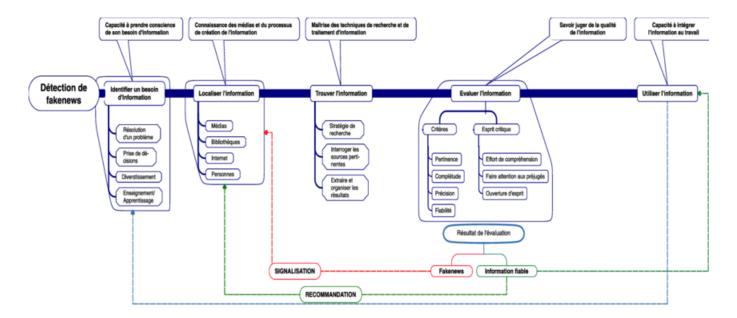


FIGURE 2.1 – Modèle conceptuel de l'EMI à l'épreuve des fake news.

- Il n'a pas besoin d'une base de données de référence pour comparer les informations prétendument fausses.
- Il n'est pas exclusif à un domaine spécifique
- Il s'applique à l'information tout court, quelle que soit sa nature ou sa forme.

### 2.7 scrapping

### 2.7.1 Définition

Youtube regorge de données diverses qui peuvent être utiles pour atteindre certains objectifs. Récupérer ce type de données est souvent fastidieux, et encore plus compliqué de les réutiliser par la suite. Pour cela nous utilisons le scraping qui définit généralement une technique permettant d'extraire des informations d'une ou plusieurs chaînes YouTube (titre de la chaîne, commentaires, .......) de manière totalement automatique. Ces scripts et programmes informatiques sont chargés d'extraire ces informations dont le but est d'extraire le contenu de manière structurée et simples.

### 2.7.2 Les stratégies

Dans un environnement d'apprentissage automatique, la collecte de données est l'étape la plus difficile à laquelle tout data scientist est confronté. Parce que des données importantes donneront un excellent modèle et que le mauvais rend le modèle nul. Il existe de nombreuses façons de collecter des données. Deux stratégies ont été sélectionnées pour être présentées dans ce chapitre :

• sans google api Dans l'extraction des données, si bien qu'au début l'utilisateur était obligé de copier et de coller des données dans excel ou un autre programme et de les stocker manuellement Mais aujourd'hui Il existe plusieurs façons d'éffectuer du scraping

2.8. CONCLUSION 19

et les développeurs ont pu développer leurs propres scrapers qui répondent à leurs besoins en utilisant principalement des langages de programmation tel que python ainsi que d'autres bibliothèques, parmi les outils et les logiciels les plus connus

- avec google api Une API permet de rendre disponibles les données ou les fonctionnalités d'une application existante afin que d'autres applications les utilisent. Utiliser une API permet donc d'utiliser un programme existant plutôt que de le re-développer. Google fournit un large éventail d'API parmi lesquelles le développeur peut choisir. Chaque service fourni par Google est associé à une API. Étant l'un d'entre eux, l'API de données YouTube est très simple à utiliser et fournit des fonctionnalités telles que :
- Rechercher des vidéos
- Gérez les vidéos comme récupérer des informations sur une vidéo, insérer une vidéo, supprimer une vidéo, etc.
- Gérez les abonnements comme répertorie tous les abonnements, insérez ou supprimez un abonnement, etc.

### 2.7.3 Différence entre les 2 stratégies

les deux méthodes présentent des différences majeures :

- Accès aux données : le scraping permet d'extraire les données de n'importe quel site alors que les API vous donnent un accès direct aux données souhaitées
- Transparence : les web scrapers peuvent scanner toutes les données figurant sur une page. A l'inverse, l'utilisation des API est une sorte de « contrat » : la nature des données partagées et les protocoles d'extraction sont définis entre les deux parties
- Sécurité des données : les API permettent d'ouvrir l'accès aux données en maintenant un niveau de contrôle et de sécurité élevé. Le propriétaire des données choisit quelles ressources il souhaite partager et avec quels acteurs tiers.
- Innovation : rendre ses API accessibles à des partenaires ou à des acteurs tiers peut permettre de générer de nouvelles opportunités de revenus. C'est aussi une source d'innovation car le développement et la collaboration externes favorisent l'apparition de nouveaux usages.

### 2.8 Conclusion

Les fausses nouvelles sont l'une des raisons de détruire l'un des éléments fondamentaux d'une société juste, la vérité et la promotion du mensonge. Il est donc nécessaire d'aider à éliminer ces parasites, et c'est pourquoi nous avons abordé dans ce chapitre les mécanismes les plus importants de détection de la désinformation qui peuvent être collectés à partir de quatre axes : la langue, la vérification des faits, le style d'écriture et la diffusion (propagation). On peut également utiliser des méthodes hybrides qui intègrent ces techniques pour améliorer la tâche de détection.

### Chapitre 3

### machine learning sous python

Contents	<b>;</b>	
3.1	Introduction	21
3.2	Définition	<b>21</b>
3.3	Les types de Machine Learning	21
	3.3.1 Apprentissage supervisé	22
	3.3.2 Apprentissage non-supervisé	22
	3.3.3 Apprentissage semi-supervisé	23
	3.3.4 Apprentissage par renforcement	23
3.4	Les applications du Machine Learning	23
3.5	Le langage python pour la Machine Learning	24
3.6	Importer les librairies dans un IDE Python	<b>24</b>
3.7	Quelle est la différence entre le Machine Learning et le Deep	
	Learning?	<b>25</b>
3.8	Détection des fausses nouvelle avec machine learning (mendicité )	<b>25</b>
3.9	Conclusion	<b>26</b>

### 3.1 Introduction

La propagation des fausses nouvelles n'a cessé d'augmenter malgré qu'il y ai eu pas mal de techniques qui avait pour but de les détecter (technique qu'on avait aborder dans le chapitre 2) mais cela n'a pas été suffisant pour extraire les fausses nouvelles avec l'évolution de la langue ainsi que les limites présenter par les approches qui permettent de le faire pour la prise en charge de plusieurs aspects tel que les relations entre les mots et certaines caractéristiques relatives aux réseaux sociaux tel que l'url, auteur, le temps,...etc. C'est là que les techniques d'apprentissage automatique rentrent en jeu et joue un rôle très important. Les entreprises et les organisations tentent de résoudre le problème de comprendre les données ainsi que la grande puissance de calcul et les vastes ressources de stockage des ordinateurs en créant des systèmes intelligents utilisant les concepts et les méthodes de la science des données (Data Science), de l'exploration de données et de l'apprentissage automatique. L'apprentissage automatique, en particulier avec Python, est l'un des domaines les plus passionnants. Ce n'est pas une erreur de décrire l'apprentissage automatique comme une application et une science des algorithmes qui comprennent les données et avec lequel il nous aidera à atteindre notre objectif qui est la détection ainsi que l'extraction des fausses nouvelles malgré leur évolution comme nous l'avons cité plutôt.

### 3.2 Définition

L'apprentissage automatique est un sous-domaine de l'informatique concerné par le développement d'algorithmes basés sur un ensemble d'exemples de certains phénomènes. Ces exemples peuvent provenir de la nature, être fabriqués à la main par l'homme ou générés par un autre algorithme. L'apprentissage automatique peut également être défini comme le processus de résolution d'un problème pratique en collectant un ensemble de données et en construisant un modèle d'algorithme statistique basé sur cet ensemble de données. Un peu plus générale : L'apprentissage automatique est le domaine d'étude qui donne aux ordinateurs la possibilité d'apprendre sans être explicitement programmés.

### 3.3 Les types de Machine Learning

Il existe différents algorithmes, techniques et méthodes d'apprentissage automatique qui peuvent être utilisés pour créer des modèles à utiliser dans de nombreux domaines, tels que le développement de véhicules autonomes et de systèmes de recommandation en ligne (tels que Netflix et Amazon). Dans ce qui suit, ils sont classés selon qu'ils nécessitent ou non une supervision humaine (apprentissage supervisé, non supervisé, semi-supervisé et par renforcement).

### 3.3.1 Apprentissage supervisé

Ce type de formation est utilisé comme entrée pour les données de formation fournies à l'algorithme, y compris les solutions, appelées étiquettes. L'algorithme apprend en comparant la sortie réelle de l'entrée avec la sortie attendue, pour trouver les erreurs et ajuster le modèle en conséquence jusqu'à ce que le meilleur taux de reconnaissance soit atteint. Le fonctionnement de l'apprentissage supervisé peut être facilement compris à partir de l'exemple et du graphique ci-dessous : Les algorithmes d'apprentissage supervisé peuvent être classés en deux catégories

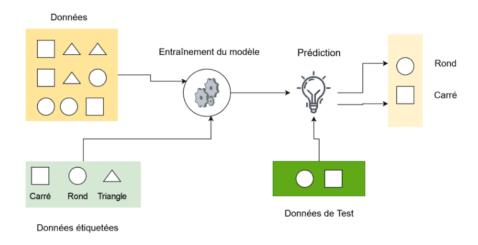


FIGURE 3.1 – Schéma explicatif de l'apprentissage supervisé.

### principales:

- La Classification
- La Régression

### Les algorithmes d'apprentissage supervisé les plus importants

- K plus proches voisins;
- Régression linéaire;
- Régression logistique;
- Machines à vecteurs de support (SVM);
- Arbres de décision et forêts aléatoires

### 3.3.2 Apprentissage non-supervisé

Ce type d'apprentissage utilise des données non étiquetées en entrée, de sorte que l'algorithme d'apprentissage trouve lui-même des points communs parmi ses données. L'algorithme d'apprentissage dans ce cas est appliqué uniquement pour trouver des similitudes et discriminer au sein de ces données, et pour regrouper un ensemble d'éléments hétérogènes dans un ensemble qui partage des propriétés communes.

### 3.3.3 Apprentissage semi-supervisé

L'apprentissage semi-supervisé est une technique qui se situe entre l'apprentissage supervisé, qui utilise uniquement des données étiquetées, et l'apprentissage non supervisé, qui utilise uniquement des données non étiquetées, est alors une solution alternative. Il utilise beaucoup de données non étiquetées et moins de données étiquetées, car les données non étiquetées sont moins chères et plus faciles à obtenir. Il se caractérise par la présence de quelques informations disponibles sur l'ensemble des données. Ces informations sont représentées soit sous la forme de quelques données labellisées, soit sous la forme de ressemblance ou dissemblance au sein de couples de données.

### 3.3.4 Apprentissage par renforcement

Ce type d'apprentissage regroupe trois principaux composants :

- 1. l'agent
- 2. l'environnement
- 3. les actions

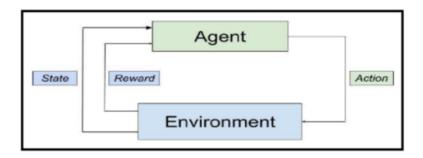


FIGURE 3.2 – Schéma explicatif de l'apprentissage par renforcement.

L'agent collecte des informations à travers un plan d'action en interagissant avec l'environnement. En réponse à une action, l'agent reçoit la récompense immédiate liée à l'action qu'il vient d'entreprendre, et l'objectif était que l'agent choisisse des actions qui augmentent les récompenses attendues sur une période donnée. L'agent atteindra cet objectif plus rapidement en suivant des règles bien établies. Le but de l'apprentissage par renforcement est d'apprendre la meilleure grammaire

### 3.4 Les applications du Machine Learning

De nos jours nous utilisant souvent l'apprentissage automatique sans le savoir en exploitant des outils tel que Siri, Google Map, Google assistant...etc. Dans cette partie nous aborderons les applications les plus courantes du Machine Learning :

- La reconnaissance des images: La reconnaissance d'image, sous-catégorie de la computer vision et de l'Intelligence Artificielle, représente un ensemble de méthodes de détection et d'analyse d'images pour permettre l'automatisation d'une tâche spécifique. Il s'agit d'une technologie qui est capable d'identifier des lieux, des personnes, des objets et plusieurs autres types d'éléments au sein d'une image et d'en tirer des conclusions en les analysant. Nous avons Facebook comme exemple parfait
- La reconnaissance vocale : consiste en l'analyse de la voix humaine, afin de la transformer en texte. Tout passe par la voix, qui est identifiée puis captée en fréquences sonores (voice-to-text). Vient ensuite l'analyse de ces fichiers sonores, par les technologies du deep learning liées à l'intelligence artificielle. Les assistants vocaux Google, Siri, Cortana et Alexa utilisent la technologie de reconnaissance vocale pour exécuter les instructions vocales.
- Les voitures à conduite autonome : une voiture autonome est un type de véhicule motorisé particulier, capable de circuler sans intervention de l'homme dans un environnement de conduite normal grâce à un système de pilotage automatique complexe. Tesla, la société de construction automobile la plus populaire, travaille sur des voitures à conduite autonome.
- La détection de fraude : Chaque fois que nous effectuons une transaction en ligne, il peut y avoir plusieurs façons de réaliser une transaction frauduleuse, comme de faux comptes, de faux identifiants, et de voler de l'argent au milieu d'une transaction. Pour détecter cela, le réseau neuronal Feed Forward nous aide en vérifiant s'il s'agit d'une transaction authentique ou d'une transaction frauduleuse.
- Le diagnostic Médical : En construisant des modèles 3D qui peuvent prédire les positions exactes des lésions dans le cerveau grâce à cela ça devient facile de détecter les tumeurs cérébrales et d'autres maladies liées au cerveau.

### 3.5 Le langage python pour la Machine Learning

En Data Science, deux langages, code R et Python, se sont peu à peu imposés. Le code Python open source, crée en 1989, est simple mais relativement puissant, et dispose d'un grand nombre de bibliothèques qui peuvent être utilisées pour appeler des fonctions préprogrammées, faisant la plupart de l'informatique d'aujourd'hui. La communauté des développeurs Python est très active. Nous trouverons également de nombreux codes open source (ou des parties de celui-ci), des didacticiels en français, des vidéos pédagogiques (YouTube) et de nombreuses aides en ligne sur ce langage.

### 3.6 Importer les librairies dans un IDE Python

Le succès de Python s'explique par la disponibilité de dizaines de bibliothèques de fonctions. Les plus utilisés en Data Science sont Pandas, Numpy (tableaux multidimensionnels),

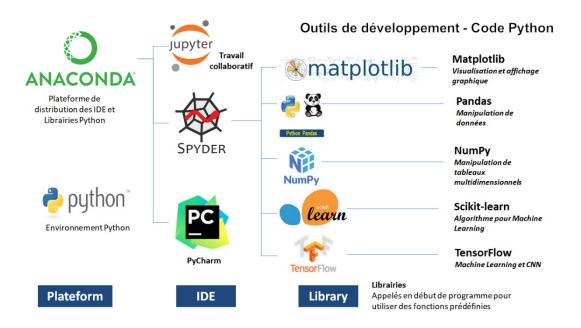


FIGURE 3.3 – Environnement de développement en Python pour le ML.

Scipy (calcul scientifique), Matplotlib (tracé graphique), Seaborn (représentation graphique multifenêtrage), ScikitLearn (pour un apprentissage réel), et Keras pour l'attaque de la bibliothèque TensorFlow (réseaux de neurones et CNN pour les réseaux de neurones convolutifs pour le traitement d'images). Pour utiliser ces bibliothèques, nous devons les importer dans un environnement de développement intégré (IDE). Les IDE Python les plus couramment utilisés sont Jupyter (fonctionnant en mode collaboratif), Spyder ou PyCharm. Le langage Python est actuellement le langage de développement le plus utilisé (35%), notamment en machine learning.

# 3.7 Quelle est la différence entre le Machine Learning et le Deep Learning?

Le deep learning est un sous-domaine du machine learning, qui a recours à un réseau neuronal inspiré du système cérébral humain, et qui nécessite énormément de données et de puissances de calcul pour s'entraîner. Adapté aussi bien à l'apprentissage supervisé que l'entrainement non supervisé, il est surtout utilisé en reconnaissance visuelle ou sonore.

### 3.8 Détection des fausses nouvelle avec machine learning (mendicité )

Quand on parle de fakes news on fait réferences a plusieurs pratique et parmi celle-ci la mendicité électronique. La mendicité electronique se fait souvent a travers des commentaires de youtube, facebook, twitter...etc meme dans les lives.celle-ci consiste à utiliser l'affection des

gens et joué avec les emotions afin de les escroquer en demandant de l'argent par paypal ou ccp et differents outils permettant de transferer l'argent et on peut les reconnaitre facilement car ils ont le meme style d'abordage et en réecrivant le meme commentaire mais differente personnes nous verrons cette pratique plus en detail dans l'implementation de notre chapitre 4 qui sera notre objet d'étude.

### 3.9 Conclusion

Dans ce chapitre nous avons exposé les notions fondamentales de l'apprentissage automatique tout en passant en revue les différents types d'apprentissage, certaines définitions, ses types et quelques applications ainsi le rôle que joue le machine learning dans la détection des fakes news qui sont vraiment un problème pesant dans notre société.

### Chapitre 4

# Implémentation(MLP,Deep learning,ADD)

### Contents

4.1	Int	roduction	
4.2	Out	ils utilisée	
	4.2.1	Logiciels utilisés	
	4.2.2	Langages utilisés	
	4.2.3	Bibliothèques utilisées	
4.3	Rési	ultats	
4.4	Forn	mule qui calcule le poids	
4.5	Forn	mule qui calcule la moyenne	
4.6	Déc	ision	
4.7	Les	réseaux de neurones pour la détection et la modicité $\dots$ 35	
	4.7.1	Perceptron multicouche	
	4.7.2	La fonction d'activation	
	4.7.3	Rétropropagation	
	4.7.4	Implémentation d'un réseau de neurones en Python	
	4.7.5	première prédiction	
	4.7.6	Calcul de l'erreur de prédiction	

### 4.1 Introduction

L'implémentation d'un programme informatique, désigne sa réalisation et sa mise en œuvre, pour passer à l'interaction avec les utilisateurs. Dans ce chapitre nous verrons l'implémentation de notre travail qui sera basé sur un exemple très intéressant qui est la mendicité électronique que nous avons vu plutôt dans le chapitre 3, aussi nous allons présenter les outils utilisées (les logiciels, les langages, les bibliothèques et les données utilisés dans notre programme, ensuite nous aborderons et discuterons les résultats.

### 4.2 Outils utilisée

### 4.2.1 Logiciels utilisés

Dans notre travail nous avons utilisé l'environnement IDE Pycharm pour la phase de traitement ainsi que DB Browser pour SQLite pour la phase de consultation :

### **IDE Pycharm**

PyCharm est un environnement de développement intégré utilisé pour programmer en Python. Il permet l'analyse de code et contient un débogueur graphique. Il permet également la gestion des tests unitaires, l'intégration de logiciel de gestion de versions, et supporte le développement web avec Django.

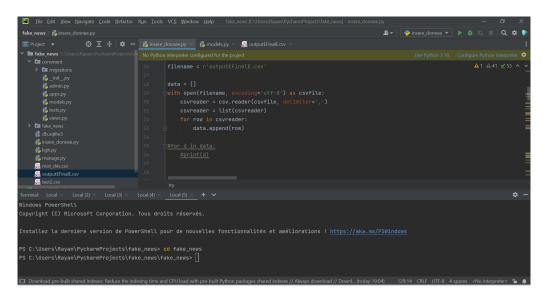


FIGURE 4.1 – IDE pycharm.

#### **DB** Browser

DB Browser pour SQLite est un outil visuel et open source de haute qualité pour créer, concevoir et éditer des fichiers de base de données compatibles avec SQLite. Il est destiné aux

utilisateurs et aux développeurs souhaitant créer des bases de données, rechercher et modifier des données.

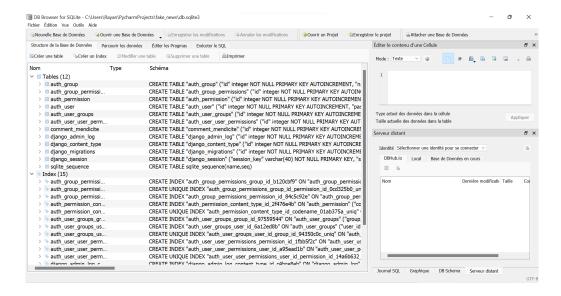


Figure 4.2 - DB Browser.

### 4.2.2 Langages utilisés

Dans notre travail nous avons eu recours au langage python pour la partie du traitement ainsi que le Framework Django pour le pré-traitement de la base :

#### Python

Python est un langage de programmation interprété, multiparadigme et multiplateformes. Il favorise la programmation impérative structurée, fonctionnelle et orientée objet

### Django

Django est un cadre de développement web open source en Python. Il a pour but de rendre le développement web 2.0 simple et rapide. Pour cette raison, le projet a pour slogan « Le Framework pour les perfectionnistes avec des deadlines ».

### 4.2.3 Bibliothèques utilisées

Nous avons eu recours a plusieurs bibliothèques qui nous ont permises à faire notre travail comme souhaité nous avons tout d'abord : Pandas, youtube comment scraper python, Matplotlib, Numpy, Csv, SQlite3 et pour finir :

#### **Pandas**

Pandas est une bibliothèque écrite pour le langage de programmation Python permettant la manipulation et l'analyse des données. Elle propose en particulier des structures de données

et des opérations de manipulation de tableaux numériques et de séries temporelles. Pandas est un logiciel libre sous licence BSD.

```
import pandas as pd

df = pd.DataFrame(data)

df = df.replace('\n', ' ', regex=True)

df = df[['Comment', 'Likes']].drop_duplicates(keep="first")

df.to_csv('Data.csv', index=False)
```

FIGURE 4.3 – Exemple d'utilisation de la bibliothèques pandas .

### Youtube comment scraper python

Youtube-Comment-Scraper-Python est une bibliothèque python permettant de récupérer des commentaires vidéo sur youtube à l'aide de l'automatisation du navigateur. Il ne fonctionne actuellement que sur Windows.

```
from youtube_comment_scraper_python import *
youtube.open("https://www.youtube.com/watch?v=-FFsLIMNlBQ")
youtube.keypress("pagedown")
all_data = []
currentpagesource = youtube.get_page_source()
lastpagesource = ''

while (True):
    if (lastpagesource == currentpagesource):
        break

lastpagesource = currentpagesource
for i in range(0,10):
    response = youtube.video_comments()
    data = response['body']
    all_data.extend(data)

youtube.scroll()
currentpagesource = youtube.get_page_source()
```

FIGURE 4.4 – Exemple d'utilisation de la bibliothèques Youtube comment scraper python.

### Matplotlib

Matplotlib est une bibliothèque du langage de programmation Python destinée à tracer et visualiser des données sous formes de graphiques. Elle peut être combinée avec les bibliothèques python de calcul scientifique NumPy et SciPy.

### Numpy

NumPy est une bibliothèque pour langage de programmation Python, destinée à manipuler des matrices ou tableaux multidimensionnels ainsi que des fonctions mathématiques opérant sur ces tableaux.

```
import matplotlib.pyplot as plt
training_y = moyenne_liste[:round(len(moyenne_liste) * 0.8)]
training_x = taille_comment[:round(len(taille_comment) * 0.8)]
test_y = moyenne_liste[len(training_y):]
test_x = taille_comment[len(training_x):]
```

FIGURE 4.5 – Exemple d'utilisation de la bibliothèques Matplotlib .

```
import numpy
modd = numpy.polyfit(training_x_training_y_1)
mymodel = numpy.poly1d(modd)
myline = numpy.linspace(0_80_80)
```

FIGURE 4.6 – Exemple d'utilisation de la bibliothèques Numpy.

### Csv

Le format CSV (Comma Separated Values, valeurs séparées par des virgules) est le format le plus commun dans l'importation et l'exportation de feuilles de calculs et de bases de données.

```
import csv
filename = r'outputEFinalE.csv'
data = []
jwith open(filename, encoding='utf-8') as csvfile:
    csvreader = csv.reader(csvfile, delimiter=',')
    csvreader = list(csvreader)
    for row in csvreader:
    data.append(row)
```

Figure 4.7 – Exemple d'utilisation de la bibliothèques Csv.

### Sqlite3

SQLite fait partie de la famille des SGBD dits « Relationnelles », car les données sont alors placées dans des tables et traitées comme des ensembles. En Python, le module sqlite3 permet de travailler avec ce moteur, mais ne supporte pas le multi-thread.

```
import sqlite3
ptry:

conn = sqlite3.connect('db.sqlite3')
cur = conn.cursor()
print("Connexion réussie à SQLite")
```

FIGURE 4.8 – Exemple d'utilisation de la bibliothèques Sqlite3.

Maintenant que nous avons vu les principaux outils que nous avons utilisées nous pouvons désormais aborder la partie de notre résultat mais avant cela nous allons parler brièvement sur ce que nous allons faire pour mieux nous situer But du projet : Le but de notre projet était de localiser les faux commentaires qui avait pour but d'escroquer les gens en mendiant c'est pour cela que nous avons fait une certaine étude sur un exemple concret qui nous dira oui ou non si ce commentaire fait partie des fakes news (mendicité). Nous nous sommes basés sur des mots clés spécifique qui sont très clairement des mots utilisés pour mendier et grâce à notre système informatique nous allons découvrir le vrai du faux. Nous allons voir en détail ce travail.

### 4.3 Résultats

Tout d'abord voici ci-dessous la premiere partie du travail qui consister a extraire les commentaires d'une chaine Youtube et les mettre dans un fichier CSV que nous allons voir sous forme de tableau Nous avons besoin que des commentaires pour mener notre étude donc nous

	1	2	3	4	5	6
1			Likes		UserLink	user
2	0		1		https: //www. youtube.	Zahra Yassmin
3	1		3		https: //www. youtube.	Ssgsh Hhdyj
4	2		3	il y a 1 an	https: //www. youtube.	اولادي حياتي
5	3		3		https: //www. youtube.	Mister N
6	4	On edt très fiers d	0		https: //www. youtube.	Lila

FIGURE 4.9 – fichier csv qui contient les commentaires.

n'aurons pas besoin des autres colonnes (Likes, Time, UserLink, user). Apres avoir extrait les commentaires nous avons pu les insérer dans notre base de données grâce à des requêtes Sql nous allons voir désormais notre base de données qui sera constituée de (id, comment, moyenne, et la liste des mot clés qui seront primordiaux) comme attribut.

- L'attribut comment représente les commentaires extrait et mis sur le fichier CSV



FIGURE 4.10 – fichier csv des commentaires.

- L'attribut moyenne représente le taux de fake en pourcentage que notre système a déduit se basant sur le poids des mots clés pour chaque commentaire
- Les attributs des mots clés nous trouverons le poids de chacun sur chaque commentaire.

### 4.4 Formule qui calcule le poids

A = nombre d'occurrences d'un mot clé /taille du commentaire

### 4.5 Formule qui calcule la moyenne

Z= poids de mot clé de chaque ligne

B = (som (z)/Nombres de mot clés) \*100

_			e de Données 🕌 Enregistrer les modifica		er les modifications	Ouvrir un Projet	Enregistrer le p
		e la Base de Données Parcourir les do omment mendicite			r dans n'importe que	lo colon	
auit	id	comment	movenne	AŠ1	مرضی	العملية	^ ارملة
	Filtre		Filtre	Filtre	Filtre	Filtre	Filtre
10	10	. صحة فطوركوم خوتي	0	0.0	0.0	0.0	0.0
11	11	ممكن رقم ديالهم الله يجزيكم	0.217391304347826	0.2	0.0	0.0	0.0
12	12	ارجوا المساعدة بمواد بدون	0.434782608695652	0.0	0.1	0.0	0.0
13	13	الله يعاون الله يجز ك خير انشاء الله	0	0.0	0.0	0.0	0.0
14	14	جزكم الله خير	0	0.0	0.0	0.0	0.0
15	15	الله يبارك يا ولاد بلادي هادو هما	0	0.0	0.0	0.0	0.0
16	16	الله يحفضكم كيفاه نوصل ليهم	0.265111346765642	0.0	0.0	0.024390243902439	0.0
17	17	ربي يحفظكم	0	0.0	0.0	0.0	0.0
18	18	سلام يا لناس الخير انقيدوني يا	0.167224080267559	0.0	0.0	0.0	0.0
19	19	الله يجازيكم بالخير رقم الهاتف	0.434782608695652	0.2	0.0	0.0	0.0
20	20	السلام عليكم ورحمة الله وبركاته	0.28604118993135	0.0	0.0	0.0	0.0
21	21	من فضلكم رقم الهاتف او صفحته	0.250836120401338	0	0.0	0.0	0.0
22	22	الله يجزيكم بالخير ساعدني انا	0.250836120401338	0.0	0.0	0.0	0.0
23	23	ناس الخير أنا ام لأربعة أبناء	0.203804347826087	0.0	0.0	0.0	0.0
24	24	جزاگم الله خیرا یا رجال و نساء	0.0205086136177194	0.0	0.0	0.0	0.0
25	25	السلام عليكم ورحمة الله وبركاته	0.0836120401337793	0.0	0.0	0.0	0.0
26	26	والله اول مرة نكتب تعليق على	0.108695652173913	0.0	0.0	0.0	0.0
77	27	dis non-classic las	0 077467760115047	0.0	0.0	0.0	00 >

FIGURE 4.11 – la base de données .

Apres avoir implémenter notre base de données ainsi que nous ayons toutes les données souhaitées nous allons ploter sous forme de graphe notre travail afin de trouver notre trace de

régression qui grâce à elle trouverons un seuil sur lequel nous allons prendre une décision.

- L'axe des X représente la taille de chaque commentaire.
- L'axe des Y représente la moyenne.

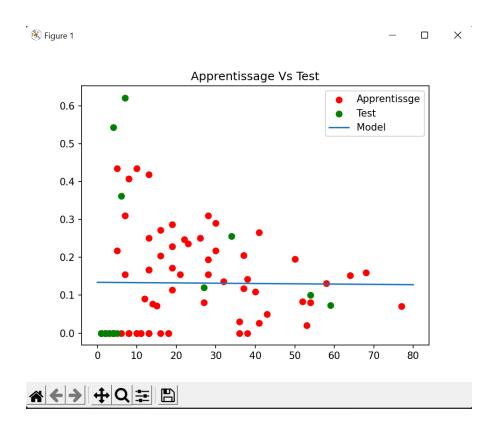


Figure 4.12 – Graphe d'apprentissages et test.

### 4.6 Décision

- Tout point qui est inférieure à la ligne de régression ne représente pas un fake comment.
- Tout point qui est supérieur ou égal à la ligne de régression représente un fake comment.
   Ceci est le résultat que notre système a déduit.

Pour finir viens l'expertise celle-ci consiste à dire en lisant le commentaire directement si oui ou non le commentaire est fake un travail assez simple et direct à faire pour finalement comparer ce que le système a déduit et ce nous avons déduit avec l'expertise Dans la table ci-dessous nous trouvons l'expertise, la moyenne et actuelle (actuelle qui représente la décision du système, expertise qui représente notre décision)

- 1 = True pour dire que c'est fake
- 0 = False pour dire que c'est vrai



FIGURE 4.13 – La table de décision.

### 4.7 Les réseaux de neurones pour la détection et la modicité

### 4.7.1 Perceptron multicouche

Le MLP (Perceptrons Multicouches) est un type de réseaux de neurones multicouches à résonnement par généralisation, souvent lié à un apprentissage supervisé, est très utilisés pour des applications variées. Le mode de fonctionnement des MLP se résumé en : Une topologie définie souvent sur plusieurs couches à savoir :

- Une couche d'entrée : Reçoit les entrées du système (Xi[.]) multiplier par les différents poids synaptiques (Wi[.]).
- Des couches cachées: Traite via plusieurs neurones à partir de plusieurs couches cachées (une fonction d'activation est appliquée) et renvoie le résultat à l'aide d'une couche de sortie.
- Une couche de sortie : Présente les différentes valeurs calculées pour enfin déterminer par un processus souvent binaire la classe trouvées parmi les classes attendues.

Ce processus d'estimation des résultats est techniquement connu sous le nom de « propagation vers l'avant ». Ensuite, nous comparons le résultat obtenu avec celle souhaitée (réelle). La tâche consiste à rendre la sortie vers le réseau neuronal aussi proche de la sortie réelle (souhaitée). Chacun de ces neurones contribue à l'erreur à la sortie finale. Afin de réduire l'erreur d'apprentissage, il faut minimiser la valeur/le poids des neurones qui contribuent davantage à l'erreur et cela se produit en revenant aux neurones du réseau de neurones et en trouvant où se situe l'erreur. Ce processus est connu sous le nom de « propagation vers l'arrière ». Les deux processus sont répété tant que l'erreur d'apprentissage est conséquente et que l'nombre maximal d'itération n'est pas atteins. Afin de réduire ce nombre d'itérations pour minimiser

l'erreur, les réseaux de neurones utilisent un algorithme commun appelé «retropropagation du gradient», qui permet d'optimiser la tâche rapidement et efficacement.

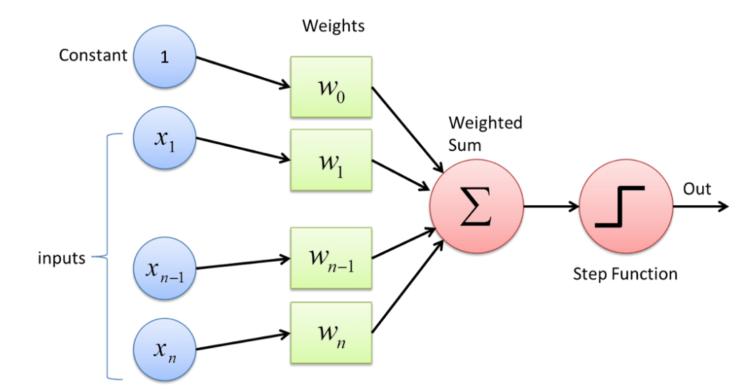


FIGURE 4.14 – Le perceptron .

### 4.7.2 La fonction d'activation

La fonction d'activation prend la somme des entrées pondérées (w1\*x1 + w2\*x2 + w3\*x3 + ... + 1\*b) comme argument et renvoie la sortie du neurone.

$$a = f(\sum_{i=0}^{N} w_i x_i)$$

De plus, la fonction d'activation est principalement utilisée pour effectuer une transformation non linéaire qui nous permet d'ajuster des hypothèses non linéaires ou d'estimer les fonctions complexes. Il existe plusieurs fonctions d'activation, comme "Sigmoid", "Tanh", "ReLu" et bien d"autres. Sous python : input = np.linspace(-10, 10, 100)

```
def sigmoid(x) :
return 1/(1+np.exp(-x))
from matplotlib import pyplot as plt
plt.plot(input, sigmoid(input), c="r")
```

Vous pouvez voir que si l'entrée est un nombre négatif, la sortie est proche de zéro, sinon si l'entrée est positive, la sortie est proche de 1. Cependant, la sortie est toujours comprise

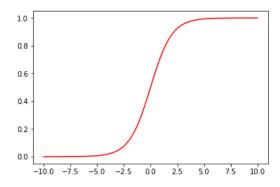


FIGURE 4.15 – La fonction segmoide.

entre 0 et 1. C'est ce que nous voulons. Cela résume la partie feedforward de notre réseau de neurones. C'est assez simple. Nous devons d'abord trouver le produit scalaire de la matrice de caractéristiques d'entrée avec la matrice de pondération. Ensuite, passez le résultat de la sortie via une fonction d'activation, qui dans ce cas est la fonction sigmoïde. Le résultat de la fonction d'activation est essentiellement la sortie prévue pour les entités d'entrée.

### 4.7.3 Rétropropagation

Au début, avant de l'entraîner, le réseau de neurones fait des prédictions aléatoires qui sont loin d'être correctes. Le principe de fonctionnement d'un réseau de neurones est simple. Nous commençons par laisser le réseau faire des prédictions aléatoires sur la sortie. Nous comparons ensuite la sortie prédite du réseau de neurones avec la sortie réelle. Ensuite, nous affinons nos pondérations et le biais de manière à ce que notre sortie prédite se rapproche de la sortie réelle, qui est essentiellement connue sous le nom de "la phase d'apprentissage du réseau de neurones".

a Étape 1 : (Calcul de la fonction coût) : La première étape de la section de rétropropagation consiste à trouver le "coût" des prédictions. Le coût de la prédiction peut simplement être calculé en trouvant la différence entre la sortie prévue et la sortie réelle. Plus la différence est élevée, plus le coût sera élevé. Il existe plusieurs autres façons de trouver le coût, mais nous utiliserons la fonction de coût d'erreur quadratique moyenne. Une fonction de coût est simplement la fonction qui trouve le coût des prédictions données. La fonction de coût d'erreur quadratique moyenne peut être représentée mathématiquement comme suit :

$$MSE = \frac{1}{n} \sum_{je=1}^{n} (prer\'ejecter\'e - observer\'e)^2$$

Ou n est le nombre d'observations.

b Étape 2 : (Minimiser le coût) Notre objectif ultime est d'affiner les sorties de notre réseau de neurones de manière à minimiser les coûts. Si vous regardez notre réseau de neurones, vous remarquerez que nous ne pouvons contrôler que les pondérations et le biais. Tout le reste est hors de notre contrôle. Nous ne pouvons pas contrôler les entrées,

nous ne pouvons pas contrôler les produits scalaires et nous ne pouvons pas manipuler la fonction sigmoïde. Afin de minimiser le coût, nous devons trouver les valeurs de poids et de biais pour lesquelles la fonction de coût renvoie la plus petite valeur possible. Plus le coût est faible, plus nos prévisions sont correctes. Il s'agit d'un problème d'optimisation où nous devons trouver les minima de la fonction. Pour trouver les minima d'une fonction, nous pouvons utiliser l'algorithme de gradient décent. np.random.seed(42) weights = np.random.rand(3,1) bias = np.random.rand(1) lr = 0.05

### 4.7.4 Implémentation d'un réseau de neurones en Python

Tout d'abord, vous définissez les trois vecteurs, un pour l'entrée et les deux autres pour les poids. Ensuite, vous calculez à quel point input-vectoret weights-1sont similaires. Pour ce faire, vous appliquerez le produit scalaire. Puisque tous les vecteurs sont des vecteurs bidimensionnels, voici les étapes à suivre :

- 1. Multipliez le premier indice de input-vectorpar le premier indice de weights-1.
- 2. Multipliez le deuxième indice de input-vectorpar le deuxième indice de weights-2.
- 3. Additionnez les résultats des deux multiplications. Voici un exemple de code pour calculer le produit scalaire de input-vectoret weights-1 :

```
In [1]: input-vector = [1.72, 1.23]

In [2]: weights-1 = [1.26, 0]

In [3]: weights-2 = [2.17, 0.32]

In [5]: first-indexes-mult = input-vector[0] * weights-1[0]

In [6]: second-indexes-mult = input-vector[1] * weights-1[1]

In [7]: dot-product-1 = first-indexes-mult + second-indexes-mult
```

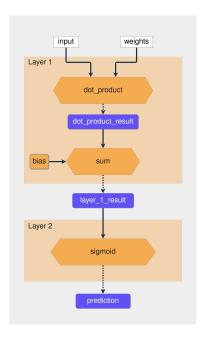
Maintenant que vous savez comment calculer le produit scalaire, il est temps d'utiliser np.dot()depuis NumPy. Voici comment calculer dot-product-1 en utilisant np.dot() :

```
In [9]: import numpy as np
In [10]: dot-product-1 = np.dot(input-vector, weights-1)
In [10]: dot-product-2 = np.dot(input-vector, weights-2)
```

### 4.7.5 première prédiction

Les hexagones jaunes représentent les fonctions et les rectangles bleus représentent les résultats intermédiaires. Il est maintenant temps de transformer toutes ces connaissances en code. Vous devrez également envelopper les vecteurs avec des tableaux NumPy. C'est le code qui applique les fonctions présentées dans l'image ci-dessus :

```
In [13]: input-vector = np.array([1.66, 1.56])
In [14]: weights-1 = np.array([1.45, -0.66])
In [15]: bias = np.array([0.0])
In [16]: def sigmoid(x): ...: return 1 / (1 + \text{np.exp(-x)})
In [17]: def make-prediction(input-vector, weights, bias): layer-1 = np.dot(input-vector, weights) + bias
```



layer-2 = sigmoid(layer-1) return layer-2 In [18] : prediction = make-prediction(input-vector, weights-1, bias)

### 4.7.6 Calcul de l'erreur de prédiction

Pour comprendre l'ampleur de l'erreur, vous devez choisir un moyen de la mesurer. La fonction utilisée pour mesurer l'erreur est appelée fonction de coût ou fonction de perte . Dans ce didacticiel, vous utiliserez l'erreur quadratique moyenne (MSE) comme fonction de coût. Vous calculez le MSE en deux étapes :

- 1. Calculez la différence entre la prédiction et la cible.
- 2. Multipliez le résultat par lui-même.

Le réseau peut faire une erreur en sortant une valeur supérieure ou inférieure à la valeur correcte. Étant donné que le MSE est la différence au carré entre la prédiction et le résultat correct, avec cette métrique, vous obtiendrez toujours une valeur positive.

### Conclusion et perspectives

Nous avons détaillé dans ce chapitre les différents outils utilisés pour la mise en œuvre de notre proposition ainsi que les résultats obtenus et leur discussion, nous avons montré ce qu'un système peut déduire en analysant chaque donnée la véracité ainsi que la fausseté de chaque commentaire comparé à l'expertise qui a donné une compatibilité claire.

Ce qui nous a permis d'en conclure des résultats satisfaisants à nos attentes.

### Bibliographie

- [1] Paulson, S (2018) Thomas Kuhn threw an Ashtray at me Nautilus, 63.
- [2] Patrick McGuinness, Les cent derniers jours, 36
- [3] Mercier, A. (2018). Fake news et post-vérité. 20 textes pour comprendre et combattre la menace. Paris : The conversation.
- [4] Davis, E. (2017). Post-truth. Peak bullshit and what we can do about it. London: Abacus.
- [5] Roberto cazavos
- [6] Détection de fausses informations sur le web et les réseaux sociaux : Cas de l'infodemie sur coronavirus , Cheyma, TAGUIA and Zahra, SID ,2020
- [7] Oihab Allal-Chérif, Neoma Business School, Covid-19: une uberisation des fake news
- [8] Guidère, M., La Linguistique Prédictive : De La Cognition à l'action, Editions L'Harmattan, 2015
- [9] Feng, V. W., and Hirst, G., Detecting Deceptive Opinions with Profile Compatibility, Proceedings of the Sixth International Joint Conference on Natural Language Processing 2013
- [10] Solanki, V., Rane, A., Fernandes, R. and Patel, G., Automated Fake News Detection, from viveksolanki.com, 2019.
- [11] Serres A., Réflexions Sur Le I de l'EMI, June 1, 2014
- [12] Djibril and Kouakou, Kouassi Sylvestre, Détection des fake news : Pour une alternative humaine aux approches technologiques, 2021

#### Webographie

- https://www.data-transitionnumerique.com/web-scraping-python/21 juin 2022
- https://www.data-transitionnumerique.com/machine-learning-python/23 juin 2022
- https://www.ionos.fr/digitalguide/web-marketing/les-media-sociaux/que-sont-les-fake-news/27 juil 2020
- https://espe-rtd-reflexpro.u-ga.fr/docs/scied-cours-num/fr/latest/fake-news.html
   mars 2021