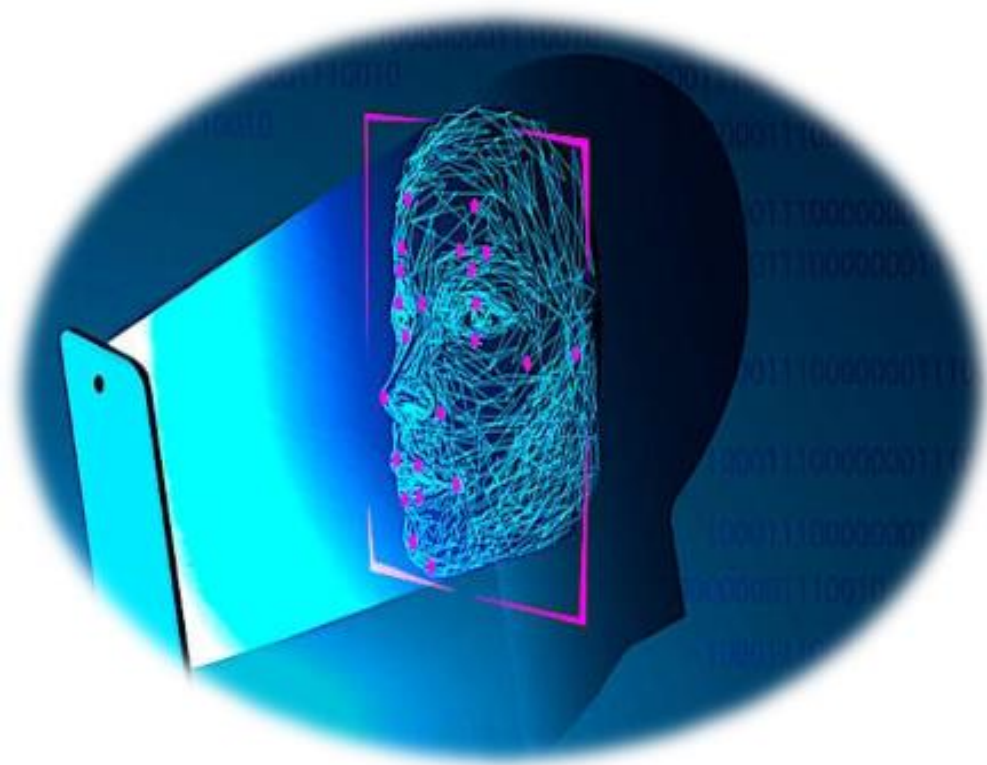


# RAPPORT DE PROJET PAS

Reconnaissance Faciale

---

LATIF Waïl - DECHANE Sanaâ



# Remerciements

*Avant toute chose, il nous paraît opportun de remercier tous ceux qui ont contribué à la réussite de notre étude par leur implication et leur sens de responsabilité.*

*Nous tenons à remercier tout particulièrement et à témoigner notre reconnaissance à Mme. Abina, notre tutrice de projet, qui nous a accompagnés le long de cette période de projet, par son suivi régulier et ses conseils pertinents. Mais aussi sur l'organisation et l'avancement de notre étude et sa disponibilité pour répondre aux problèmes que nous avons rencontrés.*

*Nous remercions aussi l'ESILV de nous avoir proposé un projet aussi intéressant.*

# Table de matières

Remerciements.....	2
Introduction.....	4
Présentation de la problématique.....	4
Définition.....	5
Historique.....	6
La reconnaissance faciale.....	7
Usages et Sécurités .....	7
Limites et Dangers.....	8
Etat de l'art .....	9
Enjeux éthiques .....	11
La législation / Que dit la Loi ? .....	12
Faut-il bannir la reconnaissance faciale ? .....	14
Comment ça fonctionne ? .....	15
Étape 1 : Détection de visage.....	16
Étape 2 : Alignement de visage.....	19
Étape 3 : Extraction des données biométriques .....	21
Étape 4 : Identification.....	22
API.....	23
Application web.....	23
Planning.....	26
Problèmes rencontrés.....	27
Conclusion.....	28
Glossaire.....	29
Sources.....	29

# Introduction

Dans le cadre de notre Projet d'Approfondissement Scientifique, différents sujets, tous plus différents les uns des autres nous ont été proposés. Nous avons choisi le sujet sur la reconnaissance faciale car c'est tout d'abord une technologie très présente de nos jours mais aussi car nous voulions comprendre son fonctionnement et sa mise en place.

Nous avons passé de nombreuses semaines à faire des recherches sur le sujet, afin de découvrir ce qui existe, comprendre et comparer les différentes technologies existantes. Ce jusqu'à obtenir les informations suffisantes pour savoir dans quelle direction nous voulions aller.

Ainsi, nous avons beaucoup appris sur le sujet, notamment les problèmes d'éthique que ça engendre, les avantages et les dangers de cette technologie... Par la suite, nous avons développé notre propre application de reconnaissance faciale. Celle-ci est composée d'une api (Python) et d'une interface web (Angular).

## Présentation de la problématique

Aujourd'hui les géants du web tels qu'Amazon/Google/Microsoft offrent des api pour faire de la reconnaissance faciale. Le but du projet est de développer une application web (en angular) qui utilise et compare les API des différents géants du web. Cependant, après avoir fait plusieurs recherches nous nous sommes rendu compte que les api développées sont soit privées (inaccessibles) soit payantes. Après discussion avec notre tutrice, nous avons alors décidé de développer seulement une application qui permettra de faire la reconnaissance faciale.

# Définition

La reconnaissance faciale est une technique qui permet à partir des traits de visage :

- D'authentifier une personne, appelée aussi one-to-many (1:N) : c'est-à-dire, vérifier qu'une personne est bien celle qu'elle prétend être (dans le cadre d'un contrôle d'accès)
- D'identifier une personne, appelée aussi one-to-one (1:1): c'est-à-dire, de retrouver une personne au sein d'un groupe d'individus, dans un lieu, une image ou une base de données.

En pratique, la reconnaissance peut être réalisée à partir d'images fixes (photos) ou animées (enregistrements vidéo) et se déroule en deux phases :

- A partir de l'image, un modèle ou « gabarit » qui représente, d'un point de vue informatique, les caractéristiques de ce visage est réalisé. Les données extraites pour constituer ce gabarit sont des données biométriques au sens du RGPD (Règlement général sur la protection des données : article 4-14).
- La phase de reconnaissance est ensuite réalisée par la comparaison de ces modèles préalablement réalisés avec les modèles calculés en direct sur des visages présents sur l'image candidate.

**Attention**, la reconnaissance faciale ne doit pas être confondue avec la détection de visage qui caractérise la présence ou non d'un visage dans une image indépendamment de la personne à qui il appartient. La détection de visage est donc inclus dans le processus de reconnaissance faciale.

# Historique

- **1964** : Des chercheurs américains, Woodrow Bledsoe, Helen Chan et Charles Bisson, étudient la programmation en vue de reconnaître des visages. Ils imaginent une méthode semi-automatique : des opérateurs doivent entrer dans l'ordinateur une vingtaine de mesures, comme la taille de la bouche ou des yeux.
- **1991** : Premier exemple réussi de technologie de reconnaissance faciale, Eigenfaces, qui utilise la méthode statistique d'analyse en composantes principales, est présenté par Alex Pentland et Matthew Turk, du Massachusetts Institute of Technology.
- **2011** : Tout s'accélère grâce au deep learning, une méthode d'apprentissage automatique s'appuyant sur des réseaux de neurones artificiels. C'est l'ordinateur qui sélectionne les points à comparer : plus il est alimenté en images, mieux il apprend.
- **2014** : Facebook sait identifier votre visage grâce à son algorithme maison, Deepface. Le réseau social affirme que sa méthode, avec ses 97 % d'efficacité, tutoie les performances de l'œil humain.
- **2018** : La police chinoise affirme avoir arrêté un suspect grâce à l'utilisation, en direct, de la reconnaissance faciale. L'homme, soupçonné de "crime économique", avait été repéré dans un concert de la pop star Jacky Cheung à Nanchang, dans la province du Jiangxi. Son visage, répertorié dans une base de données nationale, a été repéré dans une foule de 50 000 personnes.
- **Février 2019** : La ville de Nice, très en pointe en termes de vidéosurveillance (plus de 2 000 caméras), expérimente sur plusieurs volontaires la reconnaissance faciale dans l'espace public pendant trois jours, à l'occasion du carnaval. Elle dresse en août un bilan très positif mais contesté par la Commission nationale de l'informatique et des libertés (CNIL).

- **Juin 2019** : Le ministère de l'Intérieur et l'Agence nationale des titres sécurisés (ANTS) commencent les tests de l'application Alicem, malgré des réserves émises par la CNIL dès octobre 2018. Plus de 500 services publics doivent être à terme accessibles via cette nouvelle appli d'identité numérique, développée par Gemalto, une société acquise quelques mois plus tôt par l'industriel de défense Thales.
- **Décembre 2019** : En Chine, les personnes souhaitant acheter un nouveau téléphone doivent désormais accepter que l'opérateur numérise leur visage.

# La reconnaissance Faciale

## Usages et Sécurité

Les systèmes de reconnaissance faciale sont de plus en plus présents au quotidien. Ils sont par exemple utilisés sur les réseaux sociaux sur internet pour identifier quelqu'un sur une photo, sur les smartphones pour les déverrouiller, ou par des services de sécurité pour reconnaître des individus recherchés.

Ces utilisations peuvent être séparées en deux principales catégories : la sécurité et l'assistance à l'utilisateur (paiement).

### **Paiement :**

Tout comme les systèmes de reconnaissance d'empreintes digitales, le système de reconnaissance faciale permettrait d'effectuer ses achats sans avoir besoin de carte. Selon le Beijing Daily, ce genre de procédé est d'ores et déjà utilisé pour le paiement du métro de Pékin.

### **Sécurité :**

La sécurité est le principal domaine d'application des systèmes de reconnaissance faciale. Le système s'assure dans ce cas que l'utilisateur est bien un utilisateur valide avant de l'autoriser à accéder à un élément donné : Cela peut être utilisé dans un lieu public :

- Pour autoriser l'accès à un avion afin de s'assurer qu'un futur passager n'est pas recherché, comme cela est le cas à Sotchi.

- Pour autoriser l'accès à un pays, comme cela est fait dans plusieurs aéroports en France et plusieurs autres pays où cela est utilisé pour vérifier l'identité des citoyens avec un passeport biométrique éligible et expédier le passage de frontières pour eux.
- Pour suivre et potentiellement identifier une personne à partir des images d'un système de vidéosurveillance.

Mais également un logement ou une pièce (Domotique) : différents équipements comme SekuFACE ou iFace utilisent en effet la reconnaissance faciale pour s'assurer de l'identité de l'utilisateur.

Cet élément peut également se déplacer : différents équipements existent en effet pour des véhicules comme Mobii. Ou encore un environnement virtuel, cet environnement pouvant être:

- Les données d'un ordinateur, comme les exemples de systèmes Toshiba Face Recognition ou Blink.
- Les données d'une console, comme les exemples de la PlayStation 4 ou de la Xbox One.
- Les données d'un smartphone, il est alors possible de trouver des systèmes qui utilisent les capteurs du téléphone ou non (systèmes mis en place dès Android 4.0 ou Windows Phone).

Les systèmes de reconnaissance faciale, au-delà de la protection des données, permettent donc également d'interdire l'accès et l'utilisation d'éléments matériels ou immatériels.

## Limites et Dangers

### - **Sécurité et confidentialité :**

- Si par malheur un hacker accède aux données collectées par cette technologie, elles pourraient être exploitées à des fins malveillantes.
- Les autorités et les entreprises privées pourraient aussi s'en servir pour pister les individus.
- Légitime pour les citoyens de s'inquiéter de voir la reconnaissance faciale utilisée à des fins de vidéo-surveillance d'autant qu'elle est parfois utilisée à l'insu des citoyens, par exemple dans le quartier de King Cross à Londres. Dans un futur proche, vous ne pourrez peut-être plus vous déplacer dans les rues sans être identifié en permanence par des caméras.

### - **Fiabilité :**

- La reconnaissance faciale peut vous confondre avec un criminel. Même si les performances des systèmes ont été multipliées par 20 entre 2014



et 2018, et que le taux d'erreur est passé de 4% à 0,2%, le risque zéro n'existe pas.

- Les images filmées par les caméras du monde réel peuvent être floues ou mal éclairées, les visages peuvent être couverts, et les individus peuvent avoir vieilli par rapport à la photo servant de référence dans les bases de données. De fait, une personne peut être confondue avec une autre.
- **Problème de Biais qui gangrènent les algorithmes :**
  - Les réseaux de neurones étant principalement entraînés sur des photos d'hommes blancs, ils se révèlent par la suite moins performants pour identifier les femmes ou les personnes de couleur. Une étude menée par des chercheurs du Colorado démontre aussi que les principaux systèmes sont incapables de catégoriser correctement les personnes trans ou non-binaires.
  - Exemple : En 2018, lors d'un test mené par ses soins, l'ACLU a découvert que le logiciel Amazon Rekognition a confondu 28 membres du Congrès américain avec des criminels. Les concernés étaient principalement des personnes afro-américaines ou d'origine latine. Ce manque de précision à l'égard des minorités amplifie le risque que des innocents soient accusés à tort.
- **GAFAM :** La reconnaissance faciale est développée par les géants de la technologie tels que Google, Facebook, Apple, Microsoft et Amazon. Les gouvernements et les autorités n'ont d'autre choix que de se tourner vers les GAFAM pour profiter de cette innovation. Cette technologie ne fait que renforcer le pouvoir déjà exagérément élevé de ces entreprises privées colossales.
- **Prix élevé :** Son usage généralisé coûte extrêmement cher. Les caméras génèrent d'immenses volumes de vidéos, et les ressources nécessaires pour traiter et analyser ces vidéos sont astronomiques.

## Etat de l'art

La reconnaissance faciale se généralise dans le monde entier dans des buts d'identification, de sécurité et de surveillance. Pour une question de praticité nous nous focaliserons seulement sur la Chine et la France.

### En France :

Pour l'édition 2019, qui s'achève, la municipalité de Nice expérimente un dispositif inédit de reconnaissance faciale. Parmi les centaines de milliers de visiteurs, 1 000 volontaires ont

donné leur accord pour être repérés, l'objectif du test étant que les caméras parviennent à en retrouver certains au milieu de la foule. Depuis 2015, le maire se déclare favorable à ce type d'installations avec un objectif sécuritaire, dans une ville lourdement frappée par le terrorisme. Une autre initiative devrait être lancée dans les tramways niçois dans le but de repérer, grâce à la reconnaissance faciale, des *"comportements suspects"*.

La mise en place de tels dispositifs soulève néanmoins des questions éthiques et juridiques. Le recours à ces installations n'est, certes, pas nouveau en France. Les aéroports de Nice ou encore celui de Paris-Charles-de-Gaulle ou encore les gares telles que la Gare du Nord sont déjà équipés de sas de contrôle à reconnaissance faciale (cette technologie permet de comparer le véritable visage d'un passager à la photo qui figure sur son passeport biométrique). Et 77% des aéroports envisagent d'investir dans ces technologies, selon une étude de la Société internationale de télécommunication aéronautique. Toujours pour des raisons sécuritaires, afin d'éviter les intrusions, la région Provence-Alpes-Côte d'Azur a également souhaité mettre en place la reconnaissance faciale à l'entrée de deux lycées, à Nice et à Marseille.



*Sas de contrôle à la Gare du Nord au départ de train à grande vitesse Eurostar*

### En Chine :

- La reconnaissance faciale permet de payer, d'ouvrir des portes à l'hôtel.
- De nombreuses caméras surveillent les passages piétons pour dénoncer ceux qui ne respectent pas le Code de la route.
- Depuis 2018, dans 16 provinces chinoises, la police est équipée de lunettes à reconnaissance faciale qui permettent d'identifier les personnes de plus de 16 ans en moins d'une seconde.
- Dans certaines universités, les élèves sont reconnus par des caméras à l'entrée des cours.
- La technologie est poussée jusqu'à reconnaître ceux qui abusent de l'utilisation de papier dans les toilettes publiques.
- Forte de 200 millions de caméras, la Chine en a installé 400 millions de plus fin 2020. De quoi renforcer le projet de "crédit social", un système de notation des individus basé sur la surveillance, que Pékin veut généraliser d'ici l'an prochain. **Plus aucun** Chinois ne pourra alors, théoriquement, se promener dans le pays sans que l'Etat ne puisse tout connaître de son parcours.

## Enjeux éthiques

Des craintes sont ainsi formulées sur les risques d'atteinte à la protection de la vie privée et des libertés publiques. La CNIL, notamment, a demandé la tenue d'un débat démocratique sur la reconnaissance faciale.

En effet, le sentiment de surveillance renforcée, l'exploitation accrue et potentiellement à grande échelle de données personnelles, pour certaines sensibles (données biométriques), la restriction de la liberté d'aller et de venir anonymement, sont autant de problématiques essentielles pour le bon fonctionnement de notre société démocratique.

Les traitements de données biométriques sont d'une sensibilité particulière, justifiant une protection renforcée des personnes. Notamment, les dispositifs de reconnaissance faciale sont particulièrement intrusifs et présentent des risques majeurs d'atteinte à la vie privée et aux libertés individuelles des personnes concernées. Ils sont par ailleurs de nature à créer un sentiment de surveillance renforcé. Ces risques se trouvent accrus lorsque les dispositifs de reconnaissance faciale sont appliqués à des mineurs.

Dans ce contexte de contrôle extrême des individus, 80 ONG ont appelé Google, Amazon et Microsoft à s'engager à ne pas *"mettre à disposition des États leur technologie de*

*reconnaissance faciale*", pointant une possible dérive de l'utilisation de ces outils. Brad Smith, le patron de Microsoft, s'est lui-même inquiété de l'usage de cette technologie. En décembre 2018, il a appelé à agir et à réglementer le secteur *"avant de nous réveiller et de constater que l'année 2024 ressemble à '1984'"*, en référence au roman de George Orwell, dans lequel un régime dictatorial épie les moindres faits et gestes des citoyens, leur rappelant constamment : *"Big Brother vous regarde"*. Le groupe créé par Bill Gates a incité les géants du web à mettre en place des principes d'utilisations transparents. Apple, de son côté, assure que les données de son système Face ID ne sont stockées que sur les appareils des utilisateurs, pas sur des serveurs situés à distance.

## La législation / Que dit la Loi ?

La reconnaissance faciale est tout d'abord un traitement automatisé de l'image d'une personne, laquelle constitue une donnée personnelle. À ce titre, la personne qui souhaite mettre en place un système de reconnaissance faciale devra respecter la réglementation relative au traitement des données personnelles :

- La loi du 6 janvier 1978 « Informatique et liberté » modifiée par la loi du 20 juin 2018, puis par l'Ordonnance du 12 décembre 2018 ;
- Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD) ;
- La Directive (UE) 2016/680 du Parlement européen et du conseil du 27 avril 2016 relative au traitement des données en matière pénale (« Police Justice »).

Tout projet devra faire l'objet d'une analyse d'impact\* relative à la protection des données (AIPD).

Le RGPD (règlement général sur la protection des données personnelles), régit en effet la réglementation sur l'utilisation des données dans le cadre des dispositifs de reconnaissance faciale. Gérard Haas, avocat spécialisé en nouvelles technologies, y voit *"une grande avancée"* : *"Grâce à ce règlement, les données biométriques [telles que les données liées à la reconnaissance faciale] sont entrées dans la catégorie 'données sensibles'."* Or l'article 9 du RGPD interdit la collecte et le traitement de ce type de données, sauf si les personnes

concernées y ont consenti. C'est le cas dans les aéroports équipés de ces dispositifs : la machine vérifie simplement que votre visage correspond aux données contenues dans votre passeport (et non pas dans un serveur à distance), document biométrique édité avec votre accord. Dans le cas du carnaval de Nice, 1 000 personnes se sont portées volontaires pour être repérées, le RGPD a donc été respecté.

L'article 10 de ce texte européen précise que *"le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique (...) est autorisé uniquement en cas de nécessité absolue"*. Cette fois, le consentement de la personne ne suffit plus, il faut prouver qu'il y a *"une nécessité absolue"* à traiter ces données pour *"protéger les intérêts vitaux"* d'un individu.

Or en la matière, contrairement à ce qui existe pour les caméras de vidéosurveillance, la loi française ne prévoit pour l'heure aucune mesure d'application concrète sur la reconnaissance faciale.

#### **D'autres exceptions :**

- La reconnaissance faciale intégrée dans les systèmes (smartphone, ordinateur...) :

Dans ce cas, la CNIL distingue selon que le dispositif biométrique est intégré dans le système (déverrouiller l'accès...), ou qu'il fonctionne depuis des serveurs distants :

- Dans le premier cas, le dispositif peut bénéficier de l'exemption dite « domestique », et ne pas être soumis à la réglementation sur le traitement des données personnelles (article 2 2) c du RGPD).
- Dans le second cas, le droit est applicable, et la CNIL recommande d'effectuer une analyse d'impact\*.

- La reconnaissance faciale sur les lieux de travail :

Les employeurs privés ou publics peuvent mettre en œuvre des dispositifs de contrôle d'accès biométriques à condition d'être conformes à un règlement type élaboré par la CNIL.

Par délibération du 10 janvier 2019, la CNIL a adopté un règlement type relatif à la mise en œuvre d'un dispositif ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail.

Outre la réglementation applicable susvisée, les employeurs souhaitant mettre en place de tels dispositifs devront par conséquent respecter ce règlement type.

- La reconnaissance faciale pour le compte de l'État :

La reconnaissance faciale pour le compte de l'État peut être justifiée par l'intérêt public (article 6 III de l'Ordonnance de 2018). Elle doit être autorisée par décret en Conseil d'État après avis de la CNIL, lorsqu'elle :

- Intéresse la sûreté de l'État, la défense ou la sécurité publique.
- A pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté. (Article 31 II de l'Ordonnance).
- Est nécessaire à l'authentification ou au contrôle de l'identité des personnes, et que l'État agit dans l'exercice de ses prérogatives de puissance publique. (Article 32 de l'Ordonnance).

## Faut-il bannir la reconnaissance faciale ?

En juillet 2019, **la ville de San Francisco a décidé de bannir totalement** l'usage de la reconnaissance faciale par le gouvernement et les autorités dans un souci de protection de la confidentialité de ses habitants. Il s'agit de la première ville américaine à prendre cette décision. Elle a ensuite été suivie par les villes d'Oakland, Berkeley et Sommerville.

Dans un article daté du 17 octobre 2019, le New York Times appelle à aller plus loin en interdisant la reconnaissance publique aussi bien dans le secteur public que pour les entreprises privées. Aux yeux des journalistes du prestigieux journal, il est **important de bannir cette technologie avant d'en devenir dépendant** au point d'accepter ses dangers comme des nécessités.

Tant que l'usage de la reconnaissance faciale ne sera pas correctement encadré et réglementé, il sera en effet impossible d'éviter les dérives et les abus. C'est la raison pour laquelle **la seule solution semble être de bannir cette technologie purement et simplement.**

Cependant, plusieurs industriels et législateurs doutent de la nécessité de bannir cette technologie. À leurs yeux, ses bienfaits sont plus nombreux et importants que ses méfaits. Ils estiment également que la méfiance vis-à-vis de la reconnaissance faciale est une réaction

habituelle face aux nouvelles technologies, que l'on avait aussi pu observer lors de l'apparition des capteurs d'empreintes digitales. Le **débat reste donc ouvert sur la nécessité de bannir ou non la reconnaissance faciale**, et risque de donner lieu à de vives tensions entre ses partisans et ses détracteurs au fil des années à venir à mesure que son adoption se généraliser.

## Comment ça fonctionne ?

La reconnaissance faciale est une technologie combinant les techniques biométriques, l'intelligence artificielle, la cartographie 3D et le Deep Learning pour **comparer et analyser le visage d'une personne afin de l'identifier**. Elle doit son récent essor aux avancées effectuées dans les domaines du Big Data, des réseaux de neurones et des GPU.

Actuellement considérée comme l'une des trois technologies biométriques les plus performantes pour identifier un individu, la reconnaissance faciale est aussi la technologie biométrique qui connaît la plus forte croissance. Son marché pourrait atteindre une valeur de 7,7 milliards de dollars d'ici 2022.

Dans un premier temps, le visage d'un individu est localisé sur une photo ou une vidéo. Les **caractéristiques de son visage sont ensuite converties en données**, et ces données peuvent ensuite être comparées avec celles de visage entrées dans une base de données centralisée.

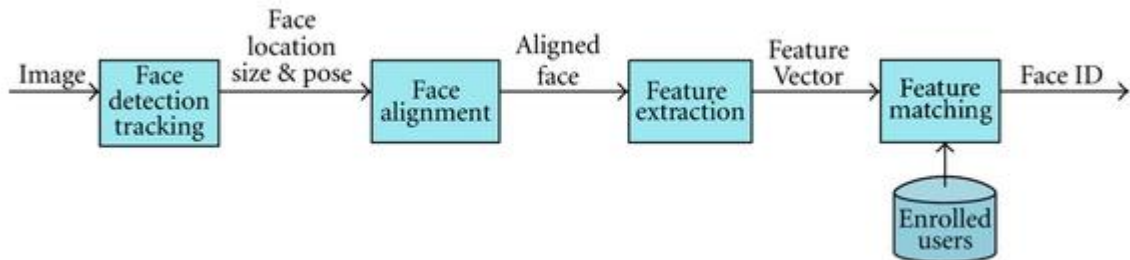
En règle générale, les logiciels de reconnaissance faciale actuels **analysent environ 80 caractéristiques du visage que l'on n'appelle aussi points nodaux**. Parmi ces caractéristiques, on compte la distance entre les yeux, la longueur du nez, la forme des joues, la profondeur des orbites, ou encore la largeur de la mâchoire.

Ces traits diffèrent sur chaque individu, et c'est pourquoi la reconnaissance faciale permet de reconnaître une personne avec précision. Les points ainsi collectés sont **mesurés en créant un code numérique appelé faceprint**, permettant de représenter le visage au sein d'une base de données. Les nouvelles technologies les plus récentes se basent sur la texture de la peau, propre à chaque individu, pour des résultats encore plus précis.

Pour être en mesure de détecter instantanément un visage, les systèmes de reconnaissance faciale sont basés sur l'intelligence artificielle. Grâce au Deep Learning, **les algorithmes sont entraînés à reconnaître les visages humains** à partir de nombreuses photos et vidéos. De

nombreuses entreprises entraînent leurs réseaux de neurones sur les milliards de photos de visages stockées sur internet par Instagram, Facebook ou encore Google.

Il y a ainsi 4 étapes dans le processus de reconnaissance faciale :



## Étape 1 : Détection de visage

La détection de visage est la première étape du système de reconnaissance faciale. En effet, sans visage aucune reconnaissance ne peut être effectuée. Cette étape déterminera les performances et la précision du système, c'est donc l'étape la plus importante du système de reconnaissance. Pour la réaliser efficacement, de nombreux chercheurs ont proposé différentes approches.

En général, il existe quatre groupes de méthodes de détection des visages :

- Les méthodes basées sur la connaissance :

La méthode basée sur la connaissance est basée sur un ensemble de règles, et sur la connaissance humaine pour détecter les visages. Par exemple, un visage doit avoir un nez, des yeux et une bouche à une certaine distance. Le grand problème de ces méthodes est la difficulté à établir un ensemble de règles appropriées. Il peut y avoir de nombreux faux positifs si les règles sont trop générales ou trop détaillées. Cette approche à elle seule est insuffisante et ne permet pas de trouver de nombreux visages dans de multiples images.

- Les méthodes basées sur les caractéristiques :

La méthode basée sur les caractéristiques consiste à localiser les visages en extrayant les caractéristiques structurelles du visage. Elle est d'abord entraînée comme classifieur, puis utilisée pour différencier les parties faciales et non faciales d'une image. L'idée est de dépasser les limites de notre connaissance instinctive des visages. Cette approche se divise en plusieurs étapes, cette



méthode à un taux de réussite moyen de 94% et ceux même en utilisant des photos avec de nombreux visages.

- Les méthodes basées sur des modèles (templates) :

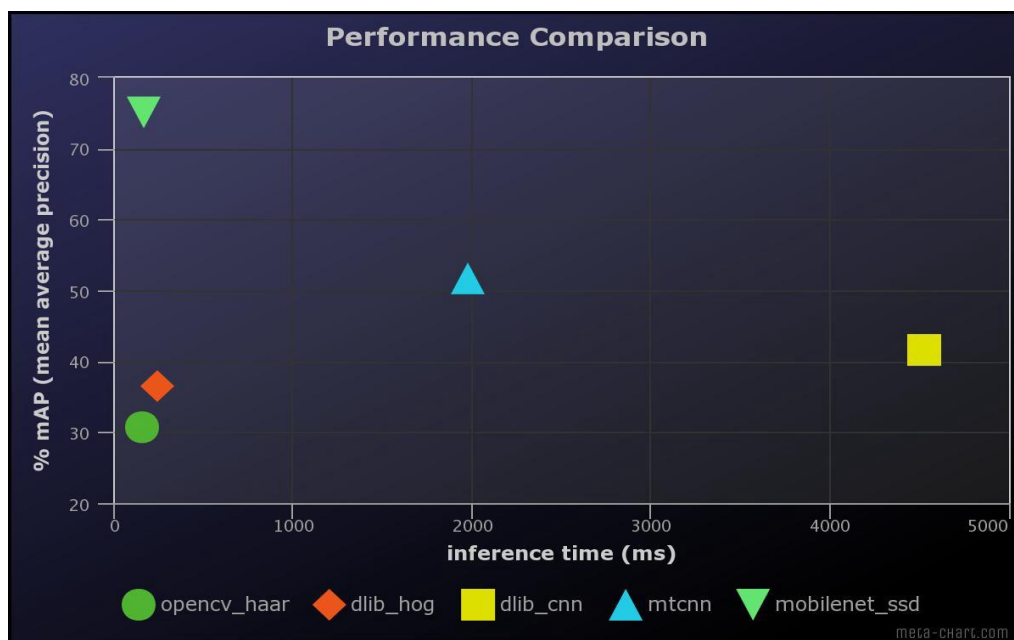
Ces méthodes utilisent des modèles de visage prédéfinis ou paramétrés pour localiser ou détecter les visages par la corrélation entre les modèles et les images reçus. Un visage humain peut être divisé en yeux, contour du visage, nez et bouche. De plus, un modèle de visage peut être construit par les contours en utilisant simplement la méthode de détection des contours. Cette approche est simple à mettre en œuvre, mais elle est inadéquate pour la détection des visages. Cependant, des modèles déformables ont été proposés pour résoudre ces problèmes.

- Les méthodes basées sur l'apparence :

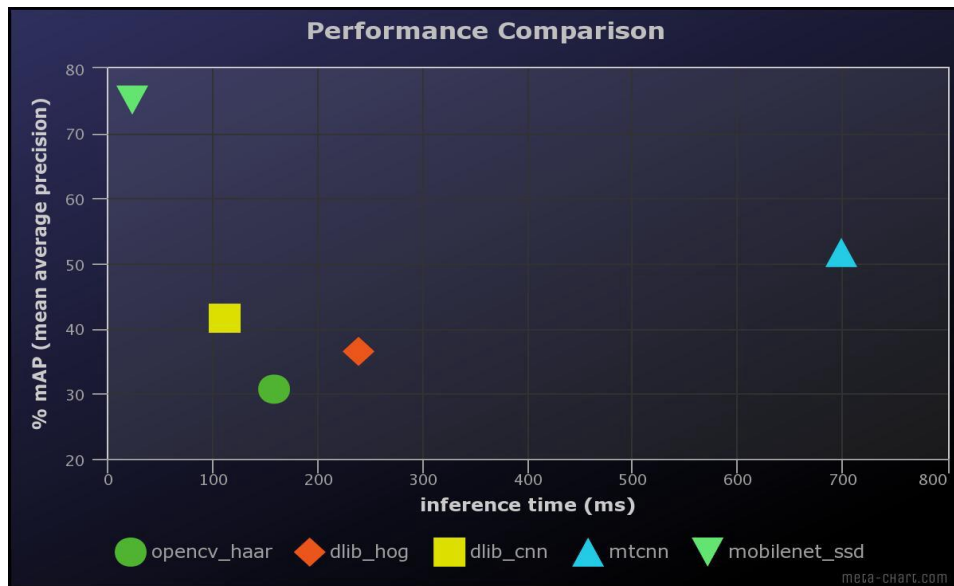
Elles reposent sur des techniques d'analyse statistique et d'apprentissage automatique (Deep Learning) pour trouver les caractéristiques pertinentes des images de visages. Ces méthodes sont entraînées sur un ensemble d'images de visages pour trouver des modèles (templates) de visages pertinents.

**L'approche basée sur l'apparence a de meilleures performances que les autres.**

Elle comprend plusieurs méthodes, dont celle basée sur les réseaux de neurones. Étant celle utilisée par les meilleurs systèmes de reconnaissance faciale c'est celle à laquelle nous allons nous intéresser. Pour cela, nous avons comparé plusieurs modèles :



*Comparaison des performances des modèles (CPU)*



*Comparaison des performances des modèles (GPU)*

Ci-dessus, nous pouvons voir que le modèle Mobilenet\_ssd est le plus performant (temps de calcul), mais aussi le plus précis (mAP) que ce soit sur CPU (processeur) ou GPU (carte graphique). Pour nous, seul le premier graphique est intéressant, n'étant pas équipés de GPU Nvidia, il nous est impossible d'exécuter ces modèles sur GPU.

**Dans notre cas**, n'ayant pas pu trouver de modèle Mobilenet\_ssd pré-entraîné à utiliser pour notre application. Nous nous sommes retranchés sur le modèle ResNet-SSD (mis en place par Google) qui a été entraîné sur une base de données de **140 000 personnes de tous types** (ethnie).

Le modèle va découper à plusieurs reprises l'image en plusieurs parties afin de pouvoir détecter des visages dans chacune des parties de l'image. À chacune des itérations l'image va être découpée comme ceci :

1. en sous partie de taille 112x112 pixels
2. en sous partie de taille 56x56 pixels
3. en sous partie de taille 28x28 pixels
4. en sous partie de taille 14x14 pixels
5. en sous partie de taille 7x7 pixels

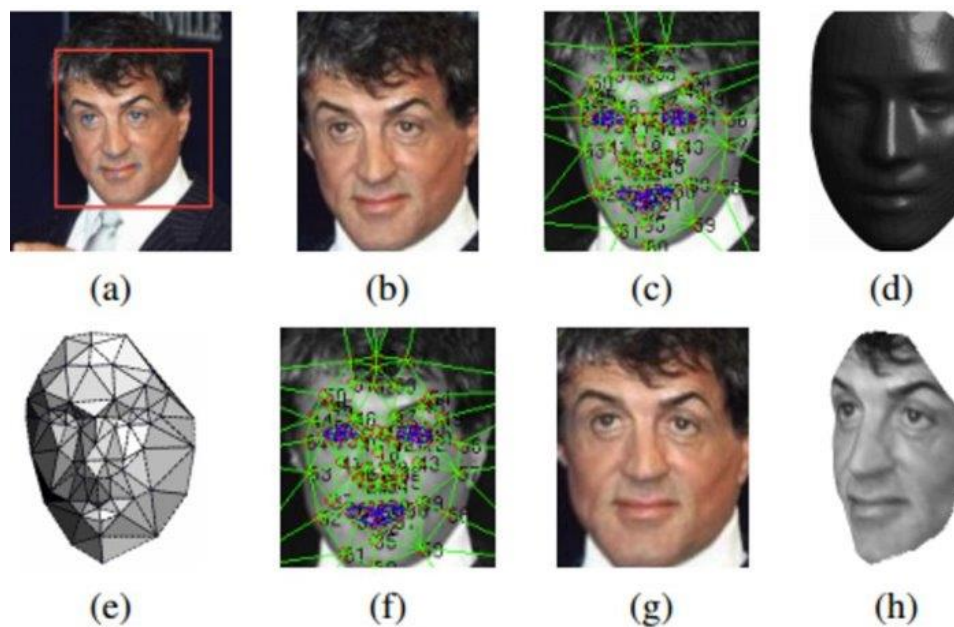
Une fois ceci fait, pour chacune des parties de l'image qui ont été analysées à l'aide de ces découpages, le modèle va retourner la probabilité qu'elle contienne un visage. Nous avons donc mis en place un seuil de confiance qui doit être dépassé afin de considérer que la portion de l'image en question contienne un visage humain. **Ce seuil a été établi à 55%.**

## Étape 2 : Alignement de visage

L'alignement des visages est une étape en amont du processus moderne de reconnaissance des visages. Google a déclaré que l'alignement des visages augmente la précision de son modèle de reconnaissance des visages FaceNet de 98,87% à 99,63%. Cela représente une amélioration de la précision de près de 1 %.

Ils existent plusieurs méthodes d'alignement :

- Les méthodes 3D comme le fait facebook avec Deepface. Elles consistent en une transformation appliquée à chaque trait du visage, afin de faire tourner le visage dans la direction où le regard est porté.



*Alignement 3D*

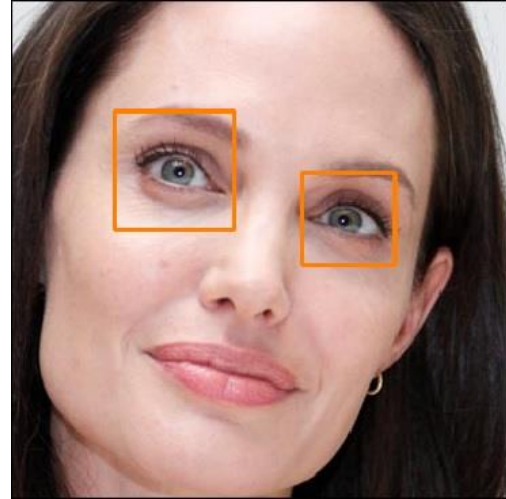
- Les méthodes 2D, qui permettent d'appliquer une rotation simple à l'image.

**Dans notre cas** nous allons nous concentrer sur l'alignement 2D car cette méthode est plus simple à implémenter que celle en 3D.

Après avoir détecté le visage, et rogné l'image, il faut maintenant détecter les yeux. Pour cela, nous avons utilisé une bibliothèque basée sur le détecteur des repères faciaux dlib (68 repères).

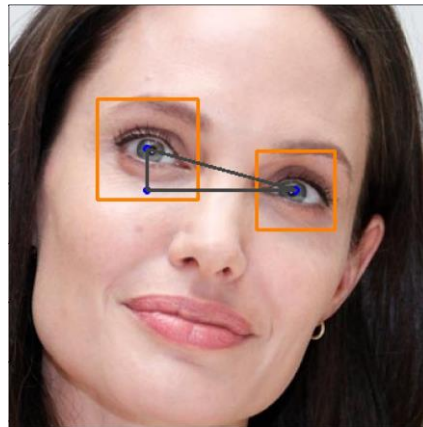


*Image de base*

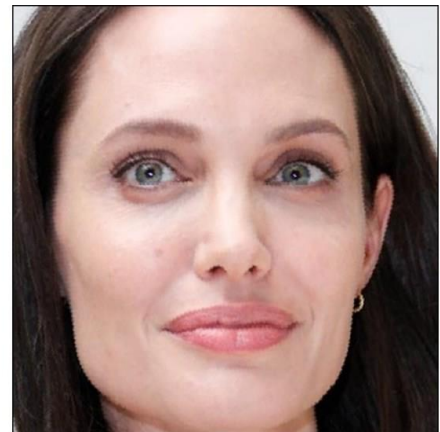


*détection des yeux*

Nous avons besoin de l'angle exact entre la ligne horizontale et la ligne permettant de lier le centre des yeux. C'est sur la base de cet angle que l'image sera pivotée. Dans cette image, l'œil gauche est plus haut que l'œil droit. C'est pourquoi, l'image subira une rotation suivant le sens inverse des aiguilles d'une montre.



*Calcul de l'angle*



*Résultat final : l'image a été pivotée afin d'aligner les yeux.*

### Étape 3 : Extraction des données biométriques

L'une des étapes les plus importantes dans le problème de la reconnaissance faciale est l'extraction des traits du visage. Une bonne extraction de caractéristiques augmentera les performances du système de reconnaissance faciale. Différentes techniques ont été proposées et sont principalement classées en quatre groupes :

Groupe de méthodes basées sur les caractéristiques géométriques : les caractéristiques sont extraites en utilisant les positions et les tailles relatives des composants importants du visage tels que les yeux, le nez...

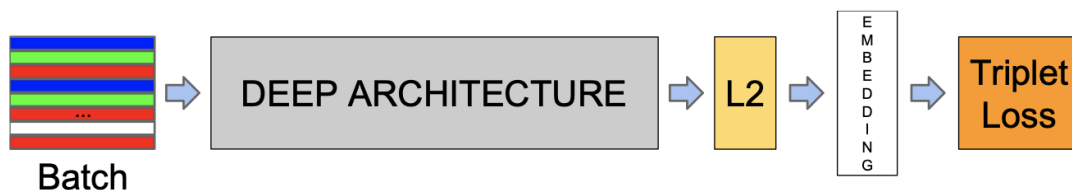
Groupe de méthode basé sur un modèle (template) : basé sur une fonction de modèle et une fonction énergétique appropriée, ce groupe de méthode extrait les caractéristiques des composants importants du visage tels que les yeux et la bouche...

Groupe de méthodes basées sur la segmentation des couleurs : cette méthode de groupe est basée sur la couleur de la peau pour isoler le visage.

Groupe de méthodes basées sur l'apparence : l'objectif de ce groupe tout comme celui vu précédemment pour la détection du visage est d'utiliser des modèles de Deep Learning (Réseau de neurones) et des méthodes statistiques pour trouver les vecteurs de base pour représenter le visage.

**Le groupe de méthodes basées sur l'apparence** s'est avéré le plus performant dans le problème d'extraction des caractéristiques du visage, car il conserve les informations importantes de l'image du visage, rejette les informations redondantes, et reflète la structure globale du visage, c'est également celui utilisé par Facenet (Google).

**Dans notre cas**, nous avons choisi d'utiliser le modèle Facenet (Google). Ce modèle utilise un CNN( réseau de neurones convolutifs) afin d'extraire ces données :



- Batch : l'image reçue après détection du visage, centrage et alignement.
- DEEP architecture : réseau de neurones permettant l'extraction de données dans le cas de Facenet un CNN est utilisé.
- L2 : couche (layer) de normalisation des données

- Embedding : vecteur permettant de représenter le visage
- Triplet Loss : fonction permettant de calculer le taux d'erreur

Pour le cas de Facenet les modèles de Google ont été entraînés de 1000 à 2000 heures et sont composées de 500M-1.6G paramètres à optimiser. Comme on peut le deviner, il existe plusieurs modèles Facenet adaptés à plusieurs types d'appareils (téléphones, ordinateurs, objets connectés...). Certains de ces modèles ont été drastiquement allégés afin de pouvoir être utilisés sur des appareils à ressources limitées, notamment des smartphones.

## Étape 4 : Identification

La décision de l'identification est basée sur la distance entre le vecteur de la personne à identifier et ceux sur lesquels le système s'est entraîné. On peut classer les faces comme paires si leur distance est inférieure à un seuil.

La distance peut être déterminée par différentes mesures telles que la similitude cosinus, la distance euclidienne etc.

**Dans notre cas**, nous avons calculé la similarité cosinus afin de comparer deux vecteurs. Elle permet de calculer la similarité entre deux vecteurs à  $n$  dimensions en déterminant le cosinus de l'angle entre eux. Nous avons mis en place un seuil de 0.4 (seuil conseillé dans la documentation de Facenet). Ainsi, si cette mesure d'erreur est inférieure à 0.4 on peut juger que c'est la même personne (par rapport aux personnes enregistrés dans notre base de données).

## API

Afin de mettre en place notre api, nous avons décidé d'utiliser **Python**. Nous avons choisi ce langage car il nous permet d'avoir accès à de nombreuses ressources dans le domaine du Deep Learning et notamment dans le domaine de la reconnaissance faciale. Cela nous a facilité la mise en place du modèle de reconnaissance faciale.

Une fois le système de reconnaissance faciale implémenté, il nous a fallu le rendre accessible pour notre application web. Pour ce faire, nous avons le choix entre 2 frameworks, Django et **Flask**. Étant donné notre situation, il nous fallait mettre en place une api rapidement. Nous avons ainsi choisi Flask pour sa facilité d'implémentation, et mis en place 3 points d'entrées à notre api :



- / : permet de vérifier l'accessibilité de l'api
- /identify : permet d'identifier les personnes sur une photo
- /add : permet d'ajouter une personne à la base de données

Afin que les messages envoyés par l'api soient facilement utilisables par l'application web nous avons décidé d'utiliser l'architecture **RESTful**.

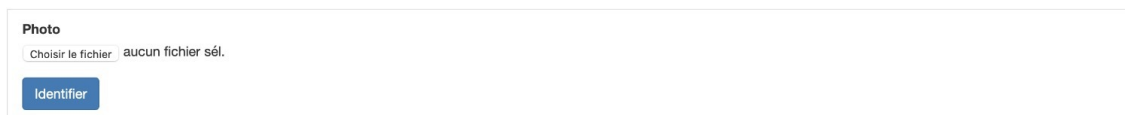
## Application web

Nous avons mis en place une application web en Angular. Cette interface est simple à utiliser, elle permet :

- d'ajouter une personne en envoyant sa photo afin que le programme l'enregistre.
- identifier les personnes sur une image : elle encadre en rouge chaque personne et indique au-dessus de ce cadre le prénom de la personne si elle l'a reconnu sinon il y a écrit "inconnue".

Voici ci-dessous notre application web :

### Identification

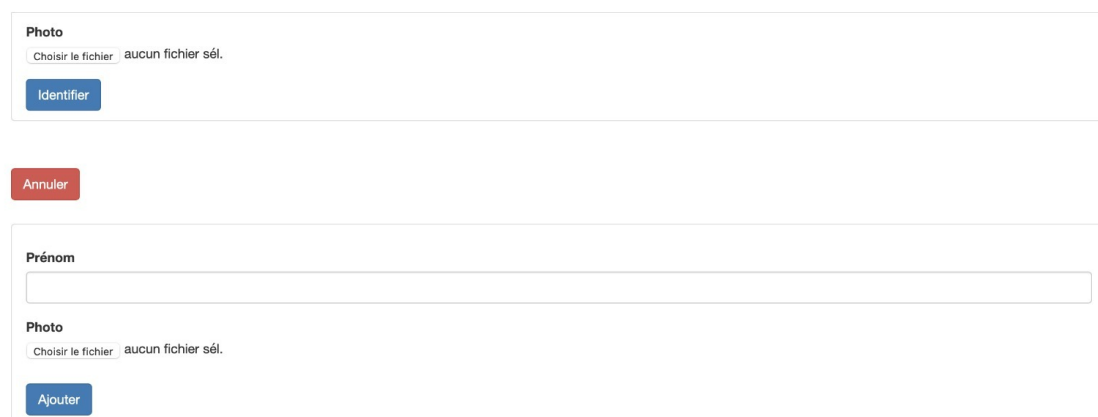


Ajouter une personne

*Première partie de l'application : identification des personnes sur une image*

Si l'on clique par la suite sur le bouton « Ajouter une personne », la deuxième partie s'affiche :

### Identification



*Deuxième partie de l'application : Ajout d'une personne dans notre base de données*

Voici quelques exemples de reconnaissance faciale sur notre application web :

- Commençons par ajouter une personne à notre base de données. Pour cela il suffit d'entrer le prénom de la personne ainsi que d'envoyer sa photo et de cliquer sur le bouton « Ajouter » :


Annuler

Prénom

analyse\_keating

Photo

Choisir le fichier Viola-Davis...744852.jpg



Ajouter

Une fois la personne enregistrée, testons si l'identification de cette personne fonctionne :


## Identification

Photo

Choisir le fichier aucun fichier sél.

Identifier

Résultat de l'identification



Ajouter une personne

## Identification

Photo

Choisir le fichier aucun fichier sél.

Identifier

Résultat de l'identification



Ajouter une personne

Nous voyons bien ci-dessus sur la photo de gauche que l'identification a fonctionné malgré le fait que son visage sur la photo envoyée pour s'enregistrer ne soit pas neutre. Par contre, nous avons voulu tester si pour cette même personne sans maquillage et sans sa perruque cela fonctionnerait. On peut observer sur la photo de droite que sans perruque et sans maquillage, il ne l'a pas reconnu.



- Un autre exemple intéressant :

## Identification

Photo

Choisir le fichier

aucun fichier sél.

Identifier

Résultat de l'identification



Ci-dessus, on peut voir que pour une même personne, le modèle n'a pas réussi à identifier la personne sur les deux photos. En effet, on voit que sur la photo de droite le modèle a réussi à l'identifier, en revanche sur celle de gauche non. Cela pourrait être dû au fait que sur celle de gauche il n'a pas de cheveux et aussi que son visage soit très sombre.

- Un autre exemple intéressant :

Prénom


Jackie\_chan

Photo

Choisir le fichier

Jackie\_chan\_1.jpg

Ajouter



Identification


Photo

Choisir le fichier

aucun fichier sél.

Identifier

Résultat de l'identification



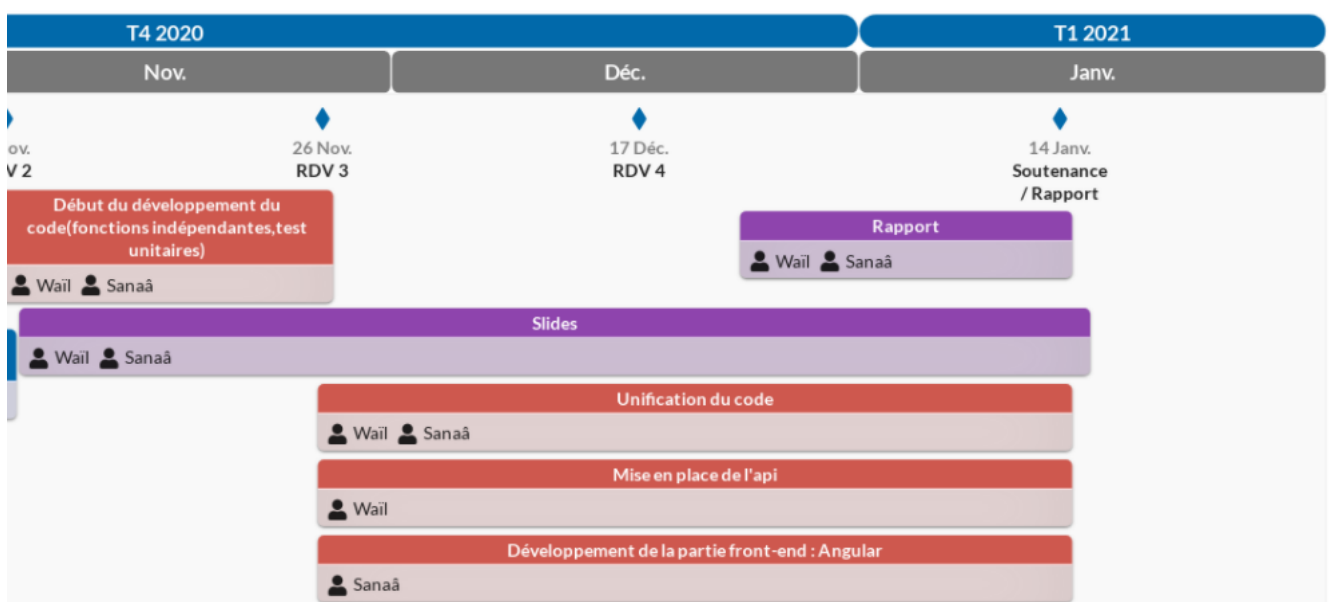
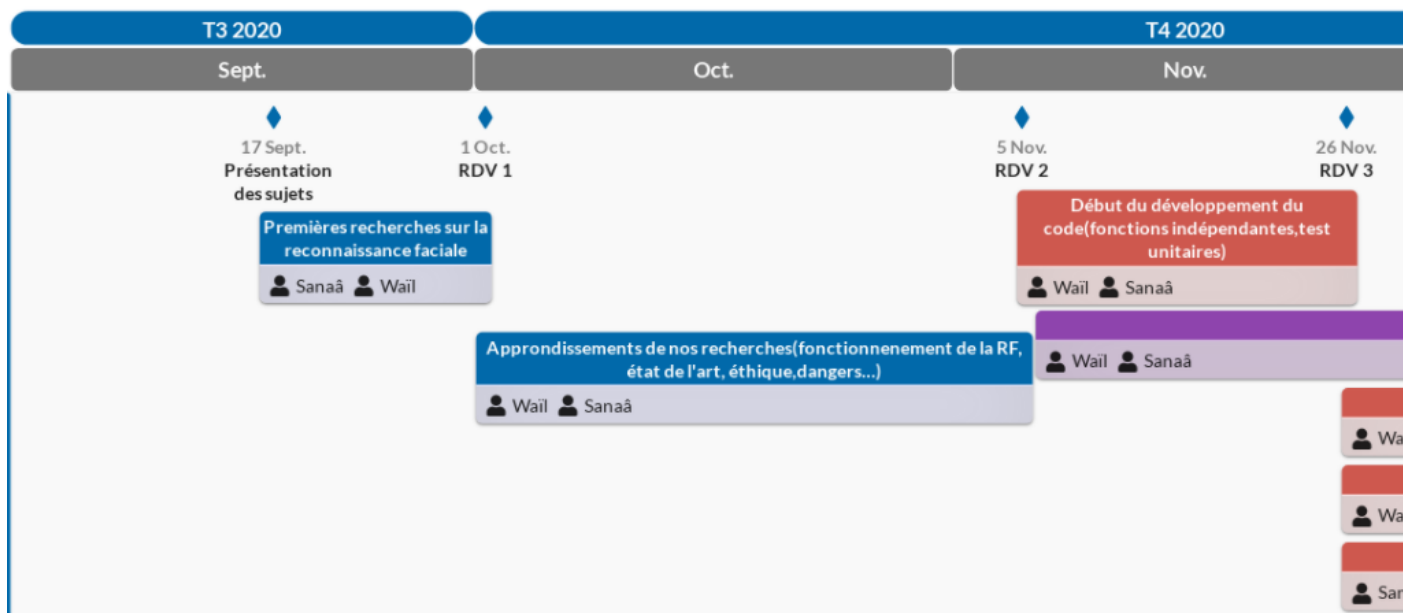
Ajouter une personne

Ci-dessus, on peut observer sur la photo de droite, que malgré le fait que son visage soit légèrement différent (lunettes en plus, et vieillesse) par rapport à la photo enregistrée en base de données (photo de gauche), le modèle a bien réussi à reconnaître la personne sur la photo de droite. Ce qui est donc très satisfaisant.

# Planning

Ci-dessous notre planning (image divisée en 2 afin de faciliter la lecture). Nous l'avons élaboré dès les premières semaines de projet pour avoir une vue d'ensemble et nous repérer au fil du temps. Nous avons essayé de nous répartir les tâches de la façon la plus efficace et équitable possible.

## Projet PAS



# Problèmes rencontrés

Avant de conclure notre travail nous tenons à présenter les problèmes que nous avons rencontré au cours de notre projet.

Nous avons tout d'abord pris beaucoup de temps à analyser les technologies qui existaient afin de savoir lesquelles étaient accessibles gratuitement. Malheureusement la plupart d'entre elles ne l'étaient pas ou étaient privées. Ensuite, nous avons eu beaucoup de mal à trouver un modèle pré-entraîné (afin d'extraire les données biométriques plus facilement) dans le but d'implémenter notre propre système de reconnaissance faciale.

Concernant la partie du code nous n'avons pas rencontré de difficultés particulières, mis à part le fait qu'on ne connaissait pas le framework Angular. Nous avons donc dû nous former, ce qui nous a pris du temps, avant de pouvoir coder l'application web. Mais cela nous a permis d'augmenter en compétences.

# Conclusion

Après un semestre sur ce projet, nous sommes plutôt fiers du résultat. Nous ne nous attendions certainement pas à en apprendre autant. Ce projet fut un véritable projet de recherche et d'approfondissement. Les premières semaines passées à faire de la veille technologique nous ont paru longues, mais ont été tout sauf inutiles. Elles nous ont servi à forger une base solide pour notre solution.

Il s'agit donc de la partie la plus importante, bien que la partie développement n'est pas à négliger. Nous avons d'ailleurs parfois eu du mal à nous répartir les tâches car le développement a duré plus longtemps que prévu. En effet, en codant nous avons rencontré des problèmes que nous n'avions pas anticipés, mais à chaque fois nous avons su trouver une solution adéquate.

Ce projet nous a permis à tous les deux d'améliorer nos compétences individuelles mais aussi collectives. À l'aide de **Git Hub** (outils de gestion de versions), nous nous tenions informés des modifications apportées. Lorsque l'un de nous était en difficulté sur une tâche, l'autre était prêt à intervenir et à aider pour plus d'efficacité. Finalement, à partir d'un énoncé aux apparences banales se cachait un véritable projet d'équipe qui a été enrichissant et formateur pour nous deux.

# Glossaire

## Analyse d'impact :

Selon la réglementation, le responsable de traitement doit effectuer une analyse d'impact lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques. Les données biométriques étant sensibles, une analyse d'impact est requise lorsqu'elle a pour finalité d'identifier une personne physique de manière unique parmi lesquelles figurent des personnes dites « vulnérables » : élèves, personnes âgées, patients, employés, demandeurs d'asile, etc...

Lorsque le traitement est effectué pour le compte de l'Etat, et à des fins pénales, l'analyse d'impact doit être adressée à la CNIL, avec demande d'avis.

## Sources

[https://fr.wikipedia.org/wiki/Syst%C3%A8me\\_de\\_reconnaissance\\_faciale](https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_reconnaissance_faciale)

<https://www.cnil.fr/fr/definition/reconnaissance-faciale>

<https://www.franceculture.fr/societe/quand-la-reconnaissance-faciale-en-france-avance-masquee>

<https://www.franceinter.fr/monde/la-chine-distribue-des-bons-et-des-mauvais-points-a-ses-citoyens>

[https://www.lemonde.fr/idees/article/2020/02/20/promesses-et-risques-de-la-reconnaissance-faciale\\_6030160\\_3232.html](https://www.lemonde.fr/idees/article/2020/02/20/promesses-et-risques-de-la-reconnaissance-faciale_6030160_3232.html)

<https://www.europe1.fr/societe/entre-progres-et-dangers-quels-usages-pour-la-reconnaissance-faciale-3944627>

[https://www.rtf.be/classic21/article/detail\\_quels-sont-les-enjeux-ethiques-de-la-reconnaissance-faciale?id=10255702](https://www.rtf.be/classic21/article/detail_quels-sont-les-enjeux-ethiques-de-la-reconnaissance-faciale?id=10255702)

<https://siecledigital.fr/2018/06/28/les-ia-de-reconnaissance-faciale-sont-elles-dangereuses/>

<https://inhesj.fr/articles/reconnaissance-faciale-les-enjeux-ethiques-et-juridiques-dune-technologie-qui-fascine-et-inquiete>