# Chapitre III:

## Conception et implémentation

## I. Introduction

Le présent chapitre décrit les détails de conception et d'implémentation du système développé.

En premier lieu, on va présenter l'architecture de notre application pour avoir une vision globale sur son but et son fonctionnement. En suite, on va décrire les tests d'utilisation, les outils de développement. Et enfin quelques expérimentations.

## II. Architecture et fonctionnement

### II.1. Présentation

Le but de notre application est la détection de toute utilisation non autorisée des données personnelles d'un utilisateur lors de son usage d'un site Web. Comme représente la figure III.1, l'application est conçue pour être intégrée dans un navigateur Web (les éléments 1 et 2 de la figure).


**Figure III.1 :** Navigateur

Après que l'utilisateur saisit l'adresse d'un site Web, et en pressant le bouton (1) l'application peut indiquer si le présent site respecte ou non ses préférences.

Un utilisateur peut définir ses préférences en terme de confidentialité[20]a traves une interface graphique accessible en cliquant sur le bouton (2) . Les détails seront présentés dans la partie description de la section III.

### II.2. Architecture

Comme il est présenté dans la figure III.2 Notre système est composé de quatre modules principaux *: le module de localisation et de téléchargement de la politique de confidentialité (MLTP), le module de définition des règles de préférences (MDRP), le module de comparaison (MC)* et enfin *le module de gestion de comportement (MGC).*

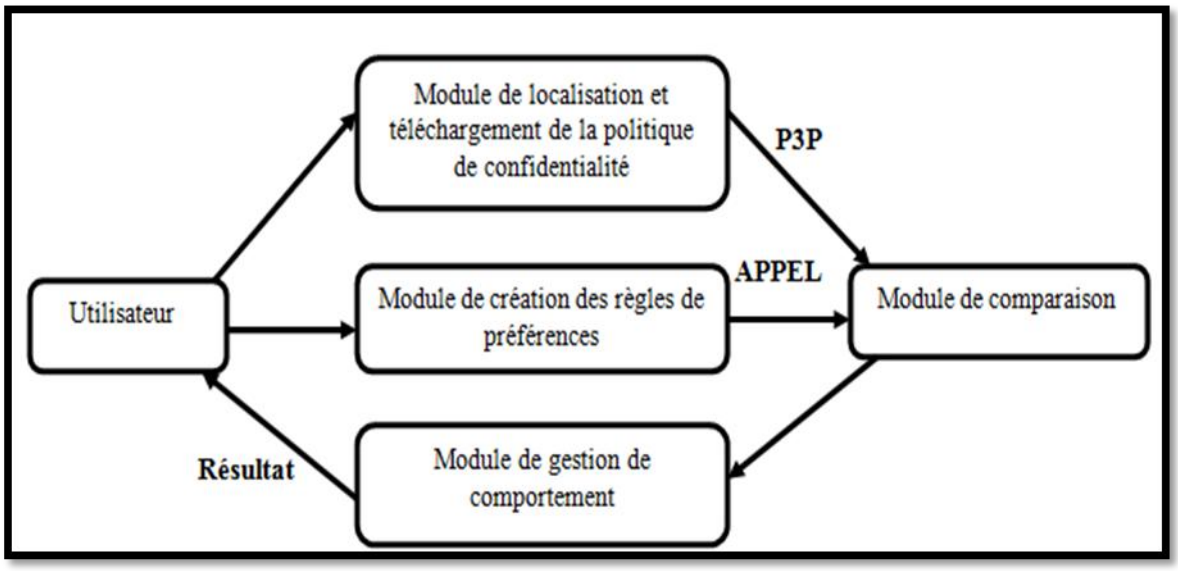


**Figure III.2 :** Architecture du système

1. ***le module de localisation et de téléchargement de la politique*** **(MLTP)** : son rôle est la localisation et le téléchargement du fichier P3P qui contient la politique de confidentialité du site visité par l'utilisateur. Ce fichier est envoyé par la suite au module de comparaison (MC).
2. ***Le module de définition des règles de préférences (MDRP):*** ce module fournit à l'utilisateur une interface graphique qui lui permet de définir ses préférences en termes de confidentialité (figure III.3). les choix de l'utilisateur sont transformés sous fourme de règles en utilisant le langage APPEL. Le fichier APPEL généré est envoyé par la suite au module de comparaison (MC).

[20] Le terme confidentialité possède le même sens que la vie privée.

Un fichier APPEL possède plusieurs règles, chacune d'elles:

- Décrit les usages prévus des données.
- Exprime une ou plusieurs restrictions concernant la collecte ou l'utilisation des données.
- Définit l'entité légale ou le domaine où les données peuvent être distribuées.

Il est bien de noté qu'à travers ce module l'utilisateur peut à tout moment modifier ses préférences de confidentialité.

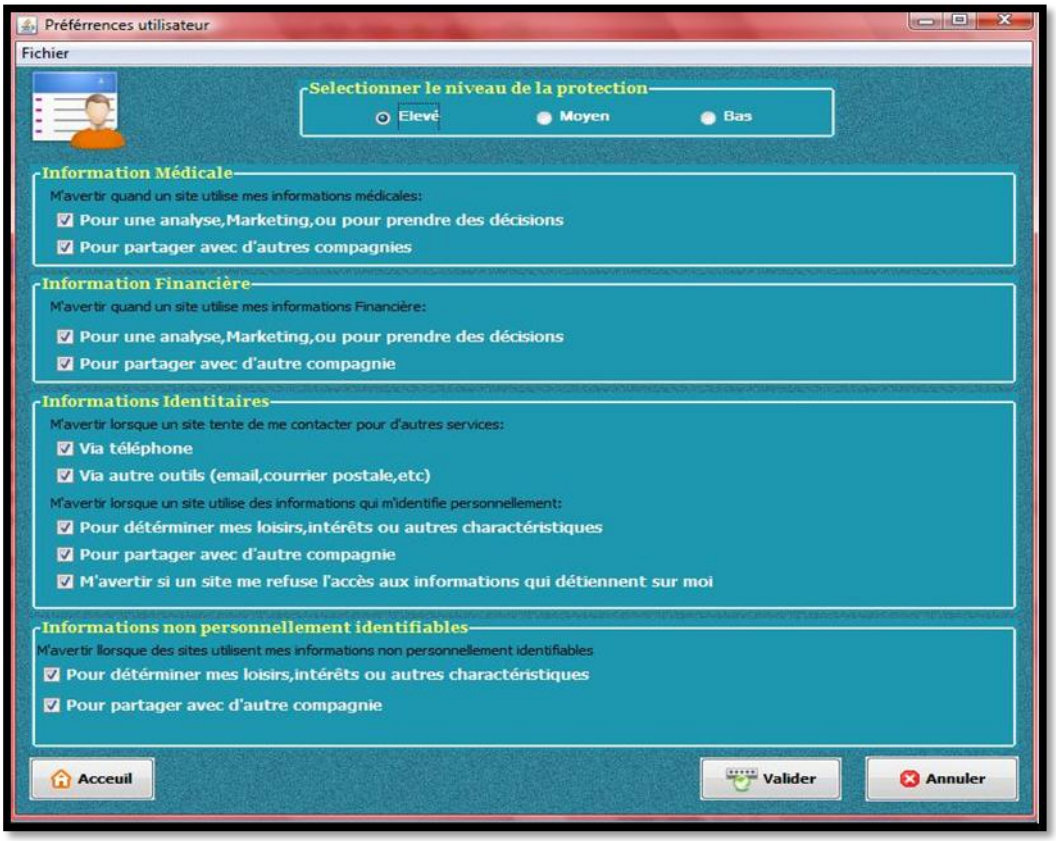


**Figure III.3 :** Interface de définition et de Modification des préférences de confidentialité.

3. ***le module de comparaison (MC)*** *:* ce module utilise le fichier P3P téléchargé par le *MLTP*, et le fichier APPEL généré par le *MDRP* pour faire une opération de mise en correspondance, cette opération a comme résultat l'affirmation de l'existence ou de l'absence de conformité entre la politique du site et les préférences de l'utilisateur. Le résultat de cette étape est transmit au module de gestion de comportement (*MGC*) pour déclencher l'action adéquate.

4. ***module de gestion de comportement (MGC)*** : le rôle de ce module est le déclanchement d'une action selon les résultats fournis par le MC, une action peut être un simple message textuel, visuel ou sonore pour informer l'utilisateur des résultats fournis par le MC. Les différents types d'action généré par notre application son décrite en détaille dans la partie description de la section III.

La comparaison se fait en appliquant l'algorithme suivant sur chaque élément d'une règle APPEL :

Deux expression P (d'un fichier P3P) et A (d'un fichier APPEL) se correspondent si et seulement si :

1. Les noms des deux éléments sont identique (par exemple <STATEMENT>, <POLICY>) ;
2. Touts les attributs de l'expression « A » se correspondent avec les attributs de l'expression « P ». si « P » contient des attributs non existants dans « A », alors ces attributs sont ignorés.
3. Si l'expression « A » contient un connecteur « ***OR*** », alors au moins un des expressions contenues dans « A » doit se correspondre avec l'un des expressions contenues dans « P » en appliquant les deux règles 1 et 2. si d'autres éléments existent dans P qui sont pas référencés dans « A » alors ces éléments sont ignorés.
4. Si l'expression « A » contient un connecteur « ***and*** », alors toutes les expressions contenues dans « A » doivent se correspondre avec les expressions similaires contenues dans « P » en appliquant les deux règles 1 et 2. si d'autres éléments existent dans « P » et ne sont pas référencés dans « A » alors ces éléments sont ignorés.
5. Si l'expression « A » contient un connecteur « ***or-exact***» alors au moins l'un des expressions contenues dans A doit se correspondre avec l'un des expressions contenues dans « P » en appliquant les deux règles 1 et 2. si d'autres éléments existent dans « P » et ne sont pas référencés dans « A » alors il n y a pas une correspondance entre « A » et « P ».
6. Si l'expression « A » contient un connecteur « ***and-exact***» toutes les expressions contenues dans « A » doivent se correspondre avec les expressions similaires contenues dans « P » en appliquant les deux règles 1 et 2. si d'autres

éléments existent dans « P » et ne sont pas référencés dans « A » alors il n y a pas une correspondance entre « A » et « P ».

7. Si A ne contient pas de connecteur alors on applique la règle 6.

### II.3 Fonctionnement

Le diagramme de séquence suivant représente l'ordre chronologique des interactions entre les différents modules de notre système,dans le cas ou un site posséde une politique de confidentialité.

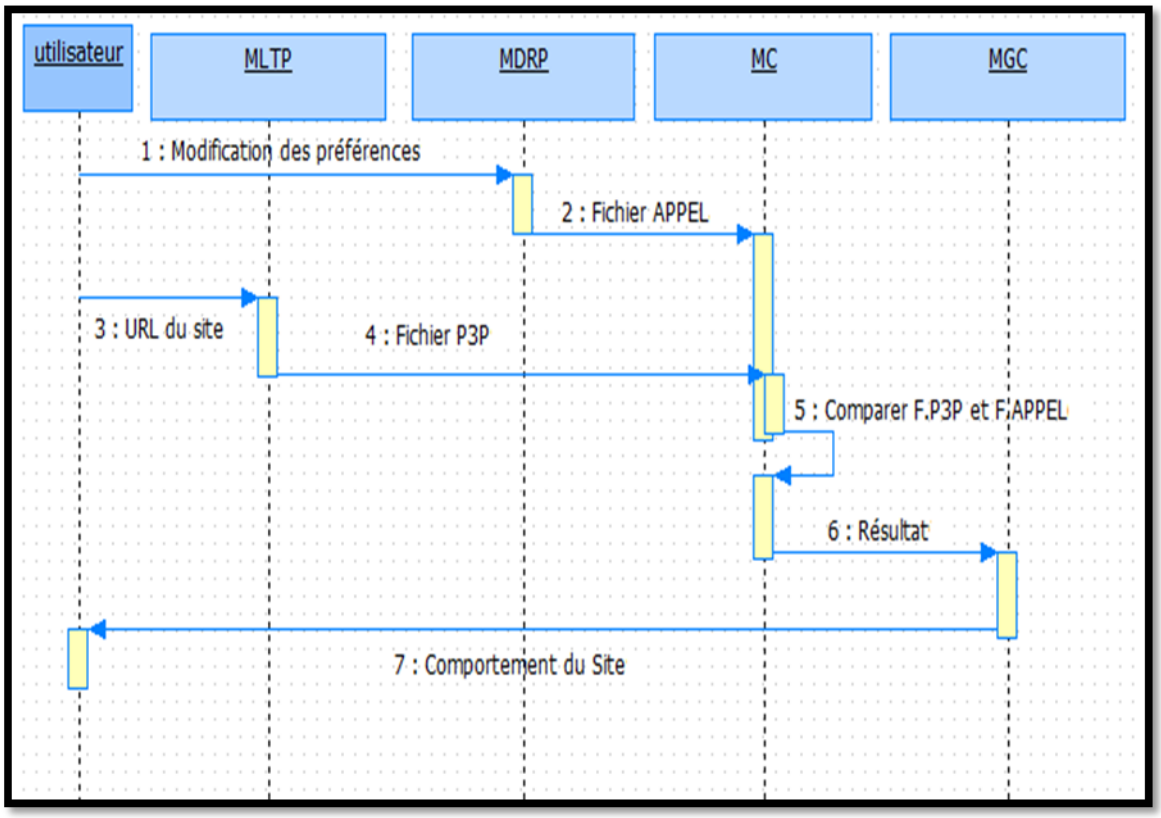


**Figure III.4 :** Diagramme de séquence du système.

Dans la première étape l'utilisateur doit définir ses préférences de confidentialité au niveau du « MDRP », ce dernier génère un fichier APPEL et le transmit au « MC ».

La deuxième étape est déclenchée lorsque l'utilisateur veut naviguer sur un site Web. Le module « MLTP » récupère l'adresse du site saisie par l'utilisateur, et essaie de localiser le fichier P3P qui contient la politique de confidentialité. Si le site définie une tel politique le « MLTP » la télécharge et la transmit au « MC ». Le « MC » fait une comparaison entre le fichier P3P et le fichier APPEL précédemment généré. Les

résultats de cette comparaison sont fournis au « MGC **»,** qui a son tour prévient l'utilisateur si le site respecte ou non ses préférences de confidentialité.

## III. Description

Cette section présente une description des différentes facettes et fonctionnalités de notre application.

Après qu'un utilisateur saisit une adresse d'un site Web, en cliquant sur le bouton 1 de la figure III.1 (section II.1), notre application et à traves le module « MGC » retourne le résultat de mise en correspondance entre la politique du site et les préférences de l'utilisateur. On peut faire face à l'un des cas suivants:

- **Cas n°1**

Le site n'a pas de politique P3P ou notre système ne trouve pas la politique à l'emplacement prévu, l'application retourne un message textuel « impossible de récupérer la politique du site » et une icône jaune (voir la figure III.5).


**Figure III.5 :** politique du site introuvable

**Cas n°2**

La politique de sécurité du site web concorde avec les préférences d'utilisateur. L'application retourne le message montré dans la figure III.6 avec une icône verte.


**Figure III.6:** Matching réussie

**Cas n°3**

La politique du site ne respect pas les préférences de l'utilisateur. L'application retourne le message montré dans la figure III.7 et une Icône rouge.


**Figure III.7:** Matching non réussie

Pour la configuration des différent paramètres de confidentialité, on clique sur le bouton (2) (figure III.1), notre application affiche une interface d'accueil (voir la figure III.8). Cette interface fournit à l'utilisateur l'accès à plusieurs fonctionnalités parmi lesquelles la définition et la modification de ses préférences (en cliquant sur le bouton (6) de la figure III.8).


**Figure III.8 :** Accueil de l'application

Dans le cas d'échec de la comparaison, l'utilisateur peut avoir plus de détail sur la cause du conflit en pressant le bouton (3), la figure III.9 montre un exemple.

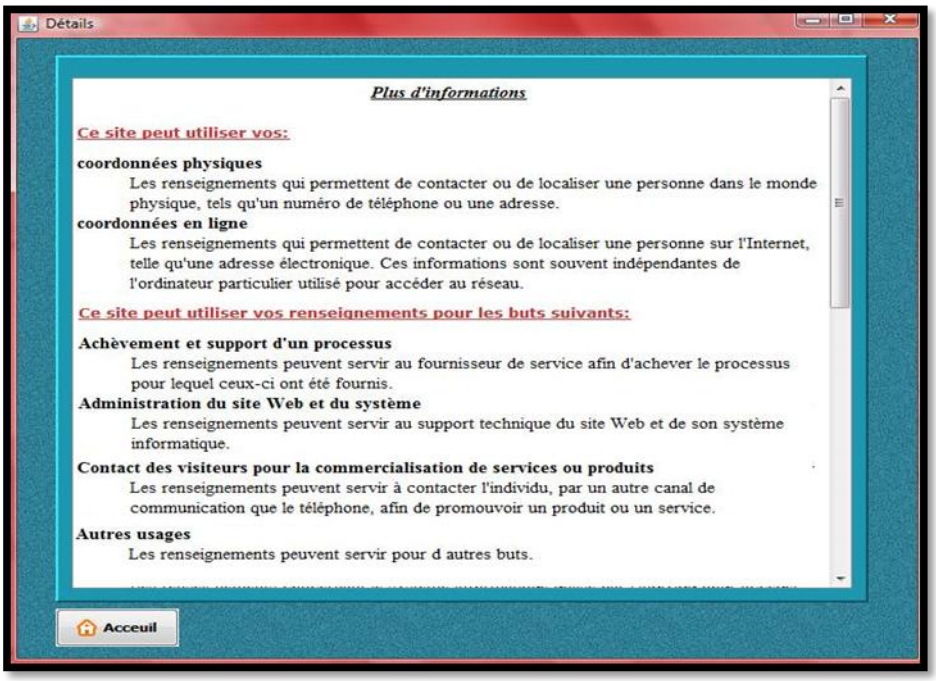


**Figure III.9 :** Plus d'informations sur la cause du conflit

En cliquant sur le bouton (4), on obtient plus d'informations sur la politique du site exprimé en langage naturel (voir figure III.10).

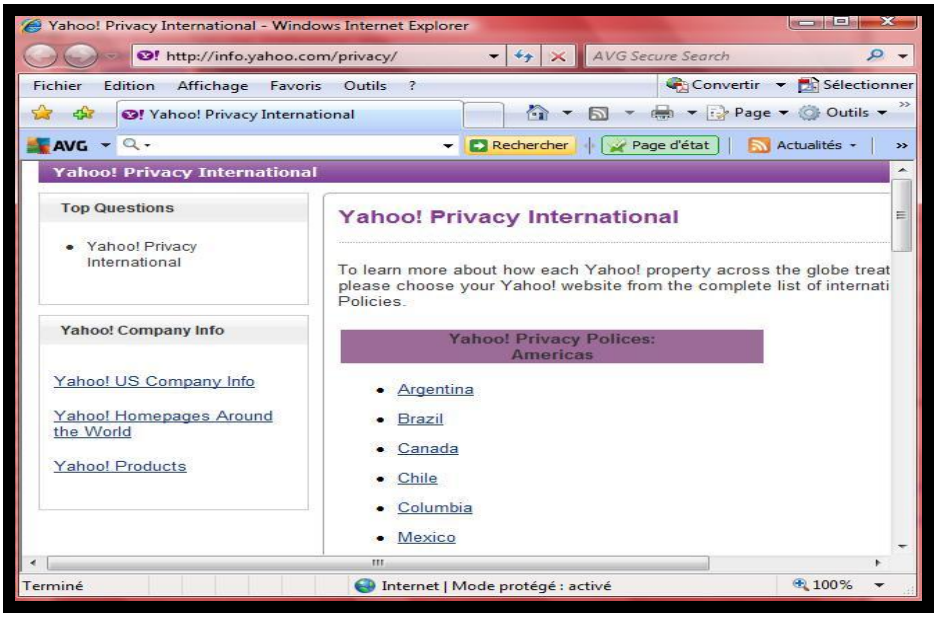


**Figure III.10 :** La politique complète du site

Comme on peut aussi voir la politique du site écrite en P3P en cliquant sur le bouton (5) la figure III.11, présente un exemple.

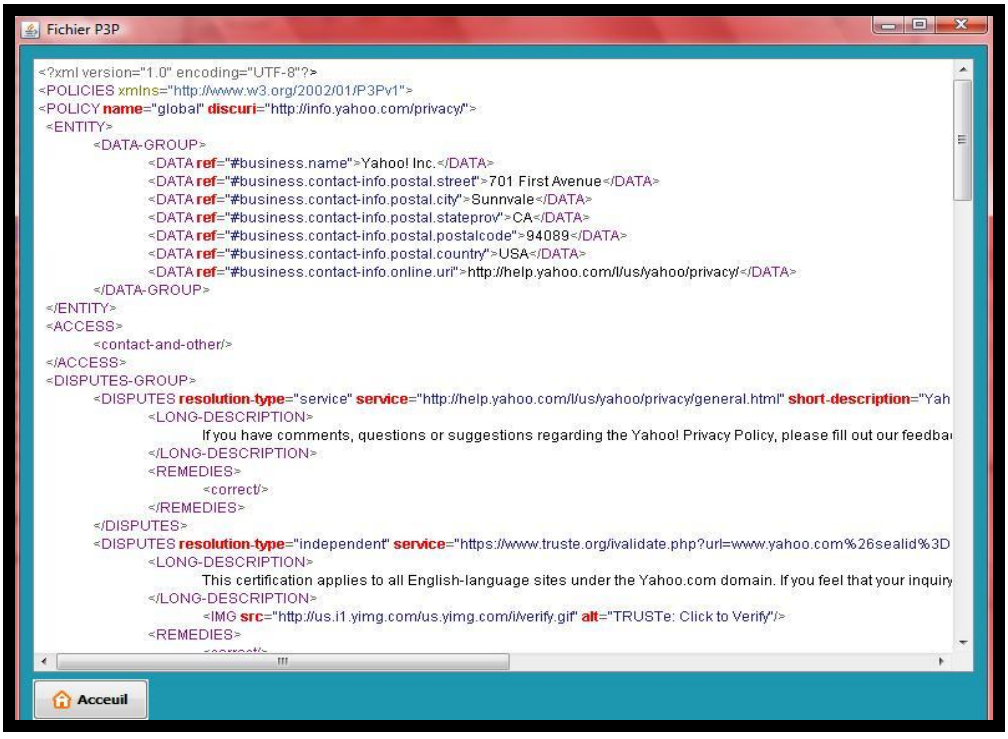


**Figure III.11 :** Exemple de fichier P3P.

## IV. Les outils de développement

Le développement de notre système a été fait avec le langage JAVA sous l'environnement Netbeans. Plusieurs API sont utilisées dont en cite : DOM, XPath et SAX. Le présent paragraphe donne un bref aperçu de ces outils.

- L'IDE Netbeans

On a choisie l'IDE Netbeans pour réaliser notre prototype et cela pour sa simplicité et sa richesse en termes de bibliothèques.

- API DOM

DOM est l'acronyme de Document Object Model permet de modéliser, de parcourir et de manipuler un document XML. Le principal rôle de DOM est de fournir une représentation mémoire d'un document XML sous la forme d'un arbre d'objets et d'en permettre la manipulation (parcours, recherche et mise à jour).

- XPath

XPath permet de parcourir un fichier XML d'une façon à la fois simple et puissante. De la sorte, en peu de temps, un développeur peut rapidement et aisément extraire les informations qui l'intéressent.

- API SAX

**S**imple **A**PI for **X**ML ou SAX est une API générale pour la lecture d'un flux XML. Ce type de parseur utilise des événements pour piloter le traitement d'un fichier XML.

## V. Expérimentations

Le tableau suivant représente le résultat de comparaison de notre application avec l'outil Priavcy Bird.

| | **L'@ du site** | **Résultat de PrivacyBird** | **Résultat de notre application** |
|---|---|---|---|
| **1** | **http://www.google.com/** | No Privacy Policy was found | Impossible de récupérer la politique du site |
| **2** | **http://www.yahoo.com/** | Yahoo! Inc. may use some collected information | Ce site ne respect pas votre vie privée |
| **3** | **http://www.privacybird.org/** | CMU Usable Privacy and Security Lab's privacy policy matches your preferences | Ce site respect votre vie privée, aucune donnée n'a été collecté |
| **4** | **http://www.nature.com/** | Nature America's privacy policy does not match your preferences | Ce site ne respect pas votre vie privée |
| **5** | **http://www.drugs.com/** | Drugsite Trust's privacy policy does not match your preferences | Ce site ne respect pas votre vie privée |
| **6** | **http://www.bird.com/** | Privacy policy has an error in its P3P policy | Ce site ne respect pas votre vie privée |
| **7** | **http://www.democracyclub.org.uk/** | Democracy Club's privacy policy matches your preferences. | Ce site respect votre vie privée, aucune donnée n'a été collecté |
| **8** | **http://checky.mozdev.org/** | checky.mozdev.org's privacy policy does not match your preferences | Ce site respect votre vie privée, les données ont été rendus anonymes |
| **9** | **http://www.charityusa.com/** | CharityUSA, LLC.'s privacy policy does not match your preferences | Ce site respect votre vie privée, aucune donnée n'a été collecté |
| **10** | **http://www.usatoday.com/** | USATODAY.com's privacy policy does not match your preferences | Ce site ne respect pas votre vie privée |
| **11** | **http://www.ftc.gov/** | Federal Trade Commission's privacy policy matches your preferences | Ce site respect votre vie privée, aucune donnée n'a été collecté |
| **12** | **http://www.addthis.com/** | LLC's privacy policy matches your preferences. | Ce site respect votre vie privée, aucune donnée n'a été collecté |

| | | | |
|---|---|---|---|
| **13** | **https://www.toolbarn.com/** | Privacy policy has an error in its P3P policy | Ce site respect votre vie privée, aucune donnée n'a été collecté |
| **14** | **http://www.developper.com/** | No Privacy Policy was found | Impossible de récupérer la politique du site |
| **15** | **http://www.microsoft.com/1** | Microsoft Corporation's privacy policy does not match your preferences | Ce site ne respect pas votre vie privée |
| **16** | **http://www.att.com/** | AT&T's privacy policy does not match your preferences | Ce site ne respect pas votre vie privée |
| **17** | **http://www.latimes.com/** | latimes.com's privacy policy does not match your preferences | Ce site ne respect pas votre vie privée |
| **18** | **http://www.ebags.com/** | eBags Inc.'s privacy policy does not match your preferences | Ce site ne respect pas votre vie privée |
| **19** | **http://ninemsn.com.au/** | ninemsn Pty Ltd's privacy policy does not match your preferences | Ce site ne respect pas votre vie privée |
| **20** | **http://www.sky.fm/** | Privacy policy has an error in its P3P policy | Ce site respect votre vie privée, aucune donnée n'a été collecté |

**Tableau III.1 :** Etude comparative

D'après ce tableau les résultats retournés sont presque identiques il y a une différence seulement pour les deux cas (8 et ), cela nous confirme la crédibilité des résultats fourni par notre application puisque elle est comparée avec l'outil le plus complet connu dans ce domaine.

Le point fort de notre application par rapport à Privacy Bird c'est que les résultats sont fournis à l'utilisateur dans un délai plus court que Privacy Bird.

## VI. Conclusion

Dans ce chapitre nous avons présenté la partie pratique de notre travail de ce fait nous avons présenté un prototype dont le but est la protection de la vie privée des utilisateurs web, ce prototype permet la vérification des politiques de confidentialité relatives aux informations recueillies lors d'une navigation.

L'un des avantages de notre application est qu'elle présente une interface utilisateur conviviale qui n'impose aucune connaissance préalable de la syntaxe de politique de confidentialité de la part des utilisateurs.

La comparaison de notre application avec Privacy Bird a montré son efficacité et sa fiabilité.