Chapitre II:

Les langages de protection de la vie privée état de l'art

I. Introduction

La confidentialité des données est une préoccupation croissante des entreprises et autres organismes dans une variété de secteurs, tels que la santé, la finance, le e-commerce, et le gouvernement. Chaque jour, ces organisations sont chargées de la responsabilité de la gestion des renseignements personnels. Contrairement à la sécurité des données, qui se concentre principalement sur la prévention des personnes non autorisées d'obtenir des renseignements de façon inappropriée, la protection de la vie privée doit offrir aux personnes la possibilité de contrôler la façon dont leurs données sont gérées et utilisées par une organisation particulière. Pour cela de nombreux organismes proposent des solutions tel que :

- **Les langages d'expression de politique de la vie privée** : ce sont des langages qui permettent aux sites web d'informer les utilisateurs de leurs politiques vis-à-vis du respect de la vie privée.
- **Les langages de préférences en termes de vie privée :** ce sont des langages qui permettent aux utilisateurs de définir leurs préférences.
- Des outils qui comparent les politiques des sites avec les préférences des utilisateurs, et avertit l'utilisateur en cas de non-respect de ces préférences.

Dans ce chapitre nous allons voir ces langages et ces outils.

II. Les Langages d'expression de politique de la vie privée

Dans cette section nous présentons les langages d'expression de politique, ces langages devraient fournir un degré élevé de fonctionnalité, afin de couvrir tous les types définis de politique. D'ailleurs, nous considérons l'expressivité d'un langage, qui garantit la définition de toutes les parties obligatoires d'une politique.
Cette section présentera les langages XACML, EPAL et plus en détaille le P3P le standard de w3c.

II.1. P3P (The Platform for Privacy Preferences)

II.1.1. Présentation

P3P est une recommandation du w3c, qui donne la possibilité aux sites web d'informer les utilisateurs de leurs politiques vis-à-vis du respect de la vie privée. Il définit un format standardisé pour décrire ces politiques. **[27]**

P3P permet aux sites Web d'exprimer leurs politiques de confidentialité dans un format normalisé que les agents utilisateurs[14] peuvent obtenir automatiquement et interpréter aisément et cela en langage XML (eXtensible Markup Language). Les agents utilisateurs P3P permettront d'informer les utilisateurs des pratiques des sites (dans des formats lisibles à la fois par une machine et par un humain) et d'automatiser au besoin les prises de décisions en fonction de ces pratiques. Les utilisateurs n'auront donc pas besoin de lire les politiques de confidentialité de chaque site visité. . **[45]**

II.1.2. La spécification P3P 1.0

La spécification P3P1.0 définit la syntaxe et la sémantique des politiques de confidentialité P3P et les mécanismes permettant d'associer les politiques aux ressources Web. Les politiques P3P consistent en déclarations utilisant le vocabulaire P3P afin d'exprimer des pratiques touchant à la vie privée. Les politiques P3P appellent également des éléments du schéma de données de base de P3P, un jeu standard d'éléments de données que tout agent utilisateur P3P devrait reconnaître. La

[14] Application cliente utilisée avec un protocole réseau particulier ; l'expression est plus généralement employée comme référence pour celles qui accèdent au World Wide Web. Les User Agents du Web vont de la gamme des navigateurs jusqu'aux robots d'indexation, en passant par les lecteurs d'écran ou les navigateurs braille pour les personnes ayant une incapacité.

spécification P3P comprend un mécanisme permettant de définir de nouveaux éléments de données et ensembles de données et un mécanisme simple autorisant l'extension du vocabulaire de P3P. **[26]**

La figure suivante donne une vision concrète du modèle p3p.

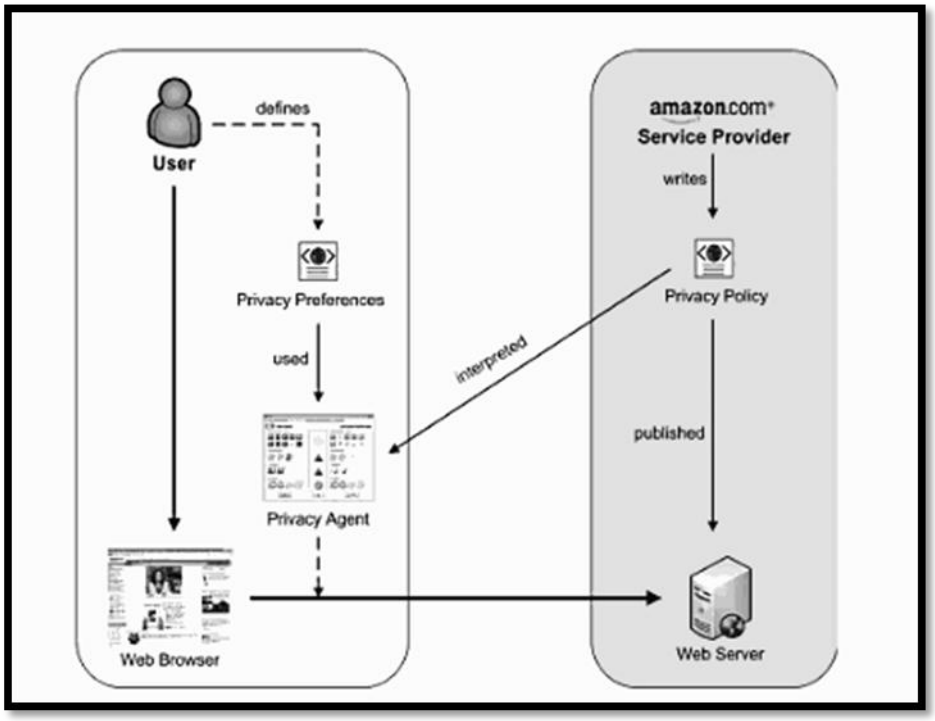

Figure II.1 : Le modèle P3P [28]

II.1.3. Les buts et les possibilités de P3P1.0

Le protocole P3P version 1.0 est conçu pour informer les utilisateurs du Web des pratiques des sites Web concernant la collecte de données. Il permet à un site Web de transcrire ses pratiques de collecte et d'utilisation des données dans un format XML, lisible par une machine, que l'on appelle *politique P3P*.

Le but de P3P version 1.0 est double :

Premièrement, permettre aux sites Web d'annoncer leurs pratiques de collecte de données de manière normalisée, lisible par une machine et facilement disponible.

Deuxièmement, permettre aux utilisateurs du Web de savoir quelles données seront collectés par les sites visités, comment ces données seront utilisées, et quels usages de ces données ces utilisateurs accepteront ou bien refuseront.

Cinq premiers topiques ont pour but d'exprimer l'intension de site Web.

- Qui est entrain de collecter cette donnée.
- Quelle information est entrain d'être collectée.
- Pour quel but.
- Quelles informations vont être partagés avec d'autre (site)
- Qui va recevoir ces informations **[26]**

II.1.4. Les politiques P3P

Les politiques P3P utilisent un codage XML avec des espaces de nommage du vocabulaire P3P afin de fournir les coordonnées de l'entité légale responsable des pratiques de confidentialité d'une politique, d'énumérer les types de données ou les éléments de données collectés et d'expliquer la destination des données en question comme il est montré dans la figure II.2. En outre, les politiques identifient les destinataires des données et divulguent d'autres informations, dont les renseignements pour la résolution des litiges et l'adresse de la politique de confidentialité d'un site écrite pour un humain. Les politiques P3P doivent couvrir tous les éléments de données et pratiques mobilisés.

Toutefois, les questions concernant le respect des demandes de renseignement légales ne sont pas traitées par cette spécification. Tout en respectant sa politique de non-redistribution des données à des tiers, un site peut être contraint de le faire par force de loi. Les déclarations P3P sont positives : les sites annoncent ce qu'ils font plutôt que ce qu'ils ne font pas. Le vocabulaire P3P est conçu pour décrire les pratiques d'un site plutôt que d'être juste un indicateur de la conformité à une loi particulière ou un code de conduite particulier. Par contre, on peut développer les agents utilisateurs de façon à tester si les pratiques d'un site sont conformes, ou non, à une loi ou un code.

Il faut remarquer que chaque politique P3P s'applique aux ressources Web spécifiques (pages Web, images, cookies, etc.) listées dans un fichier d'appel de politique. **[26]**

Pour plus d'informations sur le vocabulaire de P3P voir **Annexe B**.

```
<ENTITY>
<DATA-GROUP>
<DATA ref="#business.name">Location Provider Service</DATA>
<DATA ref="#business.contact-info.online.email">p3p@example.com</DATA>
<DATA ref="#business.contact-info.online.uri">http://www.example.com</DATA>
<DATA ref="#business.contact-info.postal.street">University Address</DATA>
</DATA-GROUP>
</ENTITY> <ACCESS><all/></ACCESS>
<DISPUTES-GROUP>
<DISPUTES resolution-type="service" service=http://www.example.com/p3p_dispute.html short-description="Dispute">
<LONG-DESCRIPTION> For any inconvenience, apply to our Customer Service (dispute@example.com) </LONG-DESCRIPTION>
<REMEDIES><correct/><money/><law/></REMEDIES>
</DISPUTES>
</DISPUTES-GROUP>
```

Figure II.2: Échantillon de politique de P3P **[26]**

II.1.5. Les agents utilisateurs P3P

Les agents utilisateurs P3P peuvent être intégrés aux navigateurs Web, aux modules d'extension des navigateurs ou aux serveurs mandataires. Ils peuvent aussi se présenter sous forme d'applets Java[15] ou de scripts JavaScript, ou être intégrés à des portefeuilles électroniques, des remplisseurs de formulaire automatiques ou à d'autres outils de

[15] Désigne les programmes développés en langage Java et que l'on trouve sur le Web. Ils fonctionnent quelque soit la plate-forme, grâce à une machine virtuelle Java (JVM), ou dans l'AppletViewer de Sun, un outil permettant de tester les applets Java. ....

gestion des données de l'utilisateur. Les agents utilisateurs P3P recherchent les appels de politiques P3P dans l'emplacement notoire, dans les en-têtes P3P des réponses HTTP et dans les balises link incorporées à un contenu HTML. Ces appels indiquent l'emplacement des politiques P3P concernées. Les agents utilisateurs peuvent récupérer la politique à l'endroit indiqué, l'analyser puis afficher des symboles, émettre des sons ou générer des invites pour l'utilisateur afin de refléter les pratiques de confidentialité P3P d'un site. Ils peuvent aussi comparer les politiques P3P aux préférences de confidentialité choisies par l'utilisateur et prendre les mesures appropriées. Un agent utilisateur n'autoriserait la délivrance des données si la politique est cohérente avec les préférences de l'utilisateur.

La spécification P3P1.0 impose peu de contraintes sur l'interface utilisateur des agents utilisateurs. Les développeurs peuvent ainsi choisir les messages et symboles à présenter à l'utilisateur pour les informer de la politique de confidentialité d'un site Web. Les développeurs ne sont pas tenus d'utiliser textuellement les définitions qui se trouvent dans cette spécification pour leurs interfaces utilisateurs. Toutefois, ils devraient s'assurer que les informations présentées à l'utilisateur, quelles qu'elles soient, représentent fidèlement les politiques P3P décrites. **[26]**

II.1.6. La mise en œuvre de P3P1.0 sur les serveurs

Les sites Web peuvent mettre en œuvre P3P1.0 sur leurs serveurs en transcrivant leurs politiques de confidentialité, lisibles par un humain, vers une syntaxe P3P puis en publiant les fichiers résultants en même temps qu'un fichier d'appel de politique qui désigne les parties du site concernées par la politique. Des outils automatisés peuvent assister les opérateurs de site dans cette traduction. **[26]**

II.1.7. La localisation du fichier de référence

Ce sont des mécanismes utilisés pour indiquer la location du fichier de référence des politiques.

- Dans une location bien connue
- Un document peut indiquer la location en utilisant la balise link du HTML
- Un document peut indiquer la location en utilisant la balise link du XHTML

- Dans l'entête de la réponse HTTP.

Les politiques sont appliquées au niveau de ressource. Une page peut se composer de plusieurs ressources, et chacun peut avoir une politique associée à lui. **[26]**

II.1.8. Les politiques compactes

Les politiques compactes sont des politiques P3P récapitulés qui fournies des conseils à des agents pour que ces agents puissent prendre des décisions vite. Les politiques compactes sont une optimisation de performance dont sa présente n'est pas obligatoire pour les agents comme les serveurs. Un agent d'utilisateur qui ne peut pas obtenir assez d'information à prendre une décision doit obtenir la politique normale.

Dans P3P 1.0, les politiques compactes contiennent des informations politiques concernant seulement les cookies. Le serveur Web doit construire les politiques compactes pour représenter des politiques sur les cookies dans la politique entière. **[26]**

Voici un exemple de politique compacte :

```
compact-policy-field = `CP="` compact-policy `"`
compact-policy = compact-token *(" " compact-token)
compact-token = compact-access |
                compact-disputes |
                compact-remedies |
                compact-non-identifiable |
                compact-purpose |
                compact-recipient |
                compact-retention |
                compact-categories |
                compact-test
```

Figure II.3: Syntaxe de la politique compacte **[26]**

II.1.9. Les Politiques complètes

Une version longue et complète de la politique de confidentialité peut être donnée au format XML, selon une forme (DTD) spécifiée par le W3C. Ce document XML, placé à un endroit « bien connu » de l'arborescence du site peut être consulté automatiquement par le navigateur afin de connaître la politique de confidentialité du site Web préalablement à la navigation.

En complément, cette politique de confidentialité sous forme informatique peut renvoyer vers une page lisible par l'internaute (une page Web). **[26]**

II.1.10. État actuel des choses

Actuellement, cette technologie n'est utilisée que par certains navigateurs et seulement :

- Pour gérer les cookies de manière «intelligente», par exemple en bloquant ceux donnant la possibilité un enregistrement abusif des actions de l'internaute.
- Pour afficher un résumé de cette politique de confidentialité à la demande de l'internaute.

D'autre part, peu de sites Web envoient une politique P3P. Ceci limite toujours la portée de cette technologie.

Etant donné que la plupart des internautes n'est guère susceptible de modifier des paramètres préconfigures sur leur logiciel de navigation, la configuration "par défaut" des choix de l'utilisateur en matière de respect de sa vie privée influera considérablement sur le niveau global de protection de la vie privée en ligne. **[26]**

II.2. XACML

II.2.1. Présentation

Est l'un des langages les plus complets qui est une extension de XML et a été conçu principalement pour permettre la restriction d'accès.

XACML (eXtensible Access Control Markup Language) est d'abord un langage basé sur XML dédié au contrôle d'accès. Il s'agit à la fois d'un langage de politique de contrôle d'accès basé sur les attributs et d'un langage protocolaire de type requêtes/réponses. De plus, la spécification fournit une architecture qui définit différentes entités impliquées dans le processus de prise de décision d'une autorisation d'accès.

Le langage de politique XACML est utilisé pour décrire les exigences générales de contrôle d'accès en termes de contraintes sur des attributs comme il est montré dans la figure II.5. Un attribut peut être n'importe qu'elle caractéristiques d'un sujet, d'une action, d'une ressource ou de l'environnement dans lequel la requête d'accès est produite. Le fait de considérer les attributs rend le langage très flexible.

De plus, XACML présente des points d'extension standards pour définir de nouveaux types de données, des fonctions additionnelles, des combinaisons de logiques, etc. **[46]**

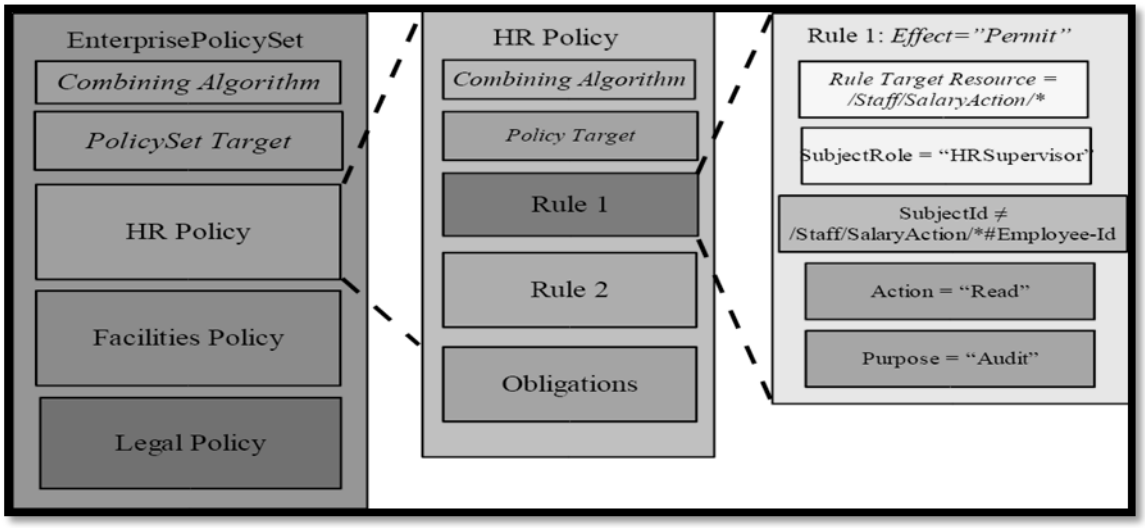

Figure II.4 : Exemple de politique en XACML **[47]**

II.2.2. Architecture de XACML

Après Une demande d'autorisation au *point de politique d'application* (PEP). Le PEP crée une demande XACML et il l'envoie au point de politique de décision (PDP), qui évalue la demande et renvoie une réponse. La réponse peut être autorisé ou refusé l'accès, avec les obligations appropriées.

Le PDP arrive à une décision après avoir évalué les politiques et les règles en leur sein. Un certain nombre de politiques peuvent être disponibles: Le PDP n'évalue pas tous, seulement ceux qui sont pertinents sont choisis pour l'évaluation, fondée sur l'objectif de la politique. L'objectif de la politique contient des informations sur le sujet, l'action, et d'autres propriétés de l'environnement.

Pour arriver à des politiques, le PDP utilise la politique Access Point (PAP), qui écrit des politiques et établit les politiques et les rend disponibles pour le PDP. Le PDP peut également invoquer le Point de politique d'information (PIP) de service pour récupérer les valeurs d'attribut liées à l'objet, la ressource, ou l'environnement. La décision d'autorisation est parvenu le PDP est envoyé à la PEP. Le PEP remplit les obligations et, en fonction de la décision d'autorisation adressée par PDP, soit autorise ou refuse l'accès. **[48]**

La figure suivante démontre ce qu'on vient de dire :

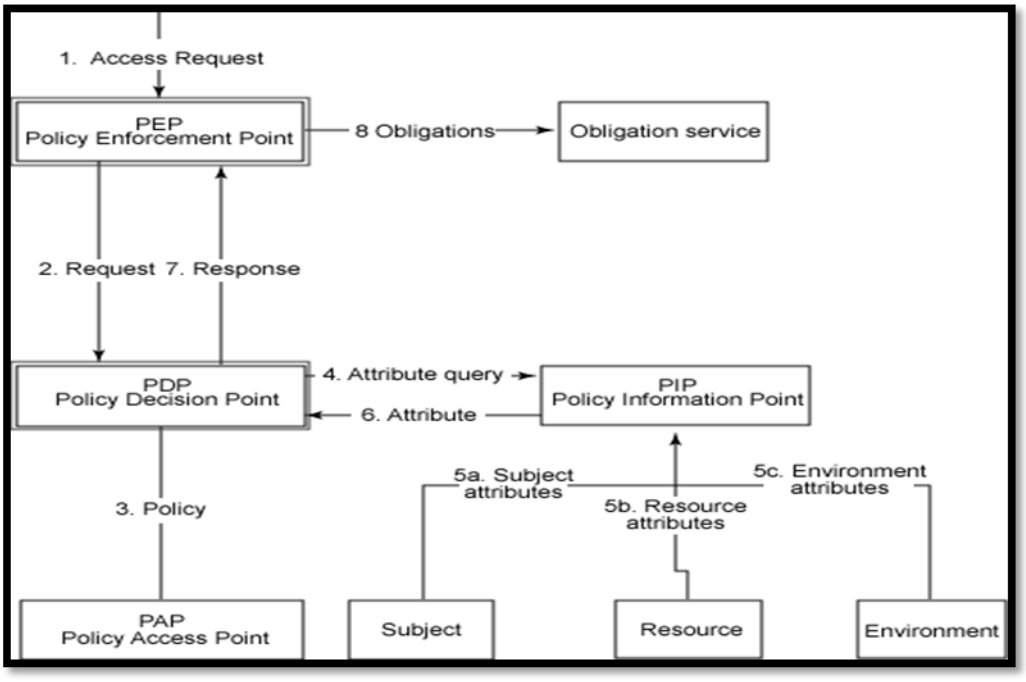

Figure II.5: Les composantes de XACML **[48]**

II.3. EPAL (Enterprise Privacy Authorization Language)

En 2002, IBM[16] publié un modèle pour la formalisation des politiques de la vie privée aux entreprises. Le modèle identifie six éléments nécessaires d'une politique de la vie privée. Basé sur ce travail, une plateforme a été proposée pour le cadre des pratiques de la vie privée d'entreprise E-p3p, qui permet à des entreprises d'imposer automatiquement des pratiques en matière de la vie privée. En conclusion, E-p3p a servi au développement d'un " langage d'autorisation de la vie privée d'entreprise" EPAL en tant qu'élément de la solution de gestion de la vie privée de l'entreprise d'IBM.

EPAL offre un langage formel comme XACML, ressemble à une solution de contrôle d'accès. Le cadre est établi sur le même modèle d'application de politique appliqué dans XACML. De même, EPAL fournit également une définition spécifique des attributs.
EPAL représente une liste de règles de priorité différente. Les règles définissent également les conditions pour considérer le contexte externe de l'information.

Nous montrons dans la figure II.7 un exemple simplifié d'une règle d'EPAL, l'exemple correspond à une politique de la vie privée qui permet de rassembler les informations des contacts pour les buts de recherches et pour se conformer aux restrictions légales strictes.

```
<rule>
  <ruling>ALLOW</ruling>
  <userCategory>organization name</userCategory>
  <action>DISCLOSE</action>
  <dataCategory>ContactInformation </dataCategory>
  <purpose>ResearchPurpose </purpose>
  <condition>Disclosure subject to strict legal restrictions </condition>
  <obligation/>
</rule>
```

Figure II.6: Exemple d'une règle EPAL **[49]**

[16] Société multinationale américaine présente dans les domaines du matériel informatique, du logiciel et des services informatiques.

Le langage EPAL permet à une organisation d'exprimer un ensemble de règles (une politique de confidentialité) relatives à l'habilitation pour l'aspect confidentialité. Autorisations et interdictions doivent contrôler l'utilisation des ressources informationnelles dans une organisation. Le modèle demande de dresser des listes hiérarchiques de catégories de données, de catégories d'utilisateurs, et des finalités de cueillette, ainsi que des ensembles d'actions, d'obligations et de conditions, toutes axées sur la confidentialité. Les actions disent comment les données sont utilisées, les obligations disent quelles actions doivent être effectuées, les conditions évaluent des éléments du contexte.

Une politique EPAL catégorise les données détenues par l'entreprise et établit des règles pour chaque catégorie. Dans la politique, l'ordre des règles est important car un principe de précédent listé (descending precedence) s'applique (rendant inopérantes les règles suivantes dans une liste). Comme une règle XACML, une règle EPAL comporte un sujet, une action et une ressource avec une indication de permission ou d'interdiction, et elle comporte en plus une mention de finalité. Une règle peut aussi contenir des conditions et des obligations.

Comme XACML, EPAL est conçu comme solution de contrôle d'accès et, par conséquent permet l'application automatique des politiques. **[49]**

III. Langages de préférences en termes de vie privée

Après une analyse des langages de politique, cette section discute les langages d'expression des préférences en termes de vie privée.
En plus d'APPEL, langage d'expression de préférence compatible avec P3P, cette section analyse XPREF et présente un langage de préférence sémantique le Rei.

III.1. APPEL (A P3P Preference Exchange Language)

APPEL (A P3P Preference Exchange Language) est un langage proche de P3P défini par le w3c. Il vise à fournir un moyen aux internautes de décrire leurs préférences personnelles en matière d'utilisation de leurs données. Ces préférences sont décrites en langage XML. Evidemment, on ne peut pas demander à un utilisateur basique d'écrire un fichier XML contenant des connecteurs logiques, des expressions régulières et des balises et attributs bien définis. Donc, il est possible d'importer des préférences par

défaut répondant aux attentes de la plupart des utilisateurs. Mais rien n'empêche un utilisateur de définir son propre fichier APPEL.

Le fichier de préférences APPEL contient un ensemble de règles (balise RULE) regroupées dans une même balise RULESET. Une règle est caractérisée par un comportement (attribut behavior) à adopter en cas de succès. Le w3c propose 3 comportements:

– **request** : la politique du site est acceptable

– **limited :** l'accès à la ressource devrait être limité

– **block :** l'accès à la ressource ne devrait pas être autorisé

Voici un extrait d'un fichier APPEL (figure qui indique que l'utilisateur accepte les cookies qui sont déposés dans le but d'adapter le contenu de la page (tailoring) et dont le destinataire sera uniquement le site lui-même (ours). La catégorie state signifie que les cookies permettent de gérer des états dans un protocole qui est sans état (http) :

```
<appel :RULE behavior="request">
      <p3p :POLICY>
            <p3p :STATEMENT>
                  <p3p :RECIPIENT appel :connective="and">
                        <p3p :ours/>
                  </p3p :RECIPIENT>
                  <p3p :PURPOSE appel :connective="non-and">
                        <p3p :tailoring/>
                  </p3p :PURPOSE>
                  <p3p :DATA-GROUP>
                        <p3p :DATA ref="#dynamic.cookies">
                              <p3p :CATEGORIES appel :connective="or">
                                    <state/>
                              </p3p :CATEGORIES>
                        </p3p :DATA>
                  </p3p :DATA-GROUP>
            </p3p :STATEMENT>
      </p3p :POLICY>
</appel :RULE>
```

Figure II.7: Exemple d'un fichier APPEL **[45]**

Cet exemple montre que le langage APPEL utilise les mêmes balises que celles utilisées dans le langage P3P. La structure du fichier des préférences utilisateur est très proche de celle d'une politique P3P, ce qui facilite la comparaison de ces deux fichiers. **[45]**

Voir **Annexe C** pour plus de détaille.

III.2. XPref (XPath-based preference language)

Le langage de préférence XPref utilise le langage d'interrogation XPath[17] de XML. Xpath définit l'adressage normalisé des parties d'un document de XML et semble un choix valable pour l'évaluation des politiques P3P basées sur XML.

Compatible à P3P, XPref offre une alternative intéressante pour APPEL. Xpref réutilise plusieurs éléments d'APPEL, tels que RULESET, RULE et behavior. Représentant le noyau de XPref.

Les conditions d'une règle sont exprimées par des expressions de XPath, contenues par l'état d'attribut. La figure suivant montre un exemple d'une règle XPref:

```
<RULESET>
  <RULE behavior="block"
    condition ="/POLICY/STATEMENT/PURPOSE/*
        [(name(.) = "contact" or
          name(.) = "telemarketing")]" />
</RULESET>
```

Figure II.8: Exemple d'une règle XPref **[49]**

L'attribut "condition" commence par un chemin qui adresse tous les nœuds enfants d'un nœud supérieur "PURPOSE" d'une politique p3p.

La condition d'une règle de XPref est satisfaite, si au moins un de ces buts s'assortit. Les opérateurs additionnels de Xpath facilitent l'évaluation des rapports multiples d'une politique de P3P.

À la différence d'APPEL, les caractéristiques de XPref permettent à des utilisateurs de définir des conditions acceptables et inacceptables, qui contribuent à l'expressivité du langage. Mais XPref ne garantit pas l'uniformité sémantique des ensembles de règle. Car Xpref suit la même orientation de syntaxe qu'APPEL, les mêmes contradictions sont susceptibles de se produire pendant l'évaluation des règles. **[49]**

[17] Un langage d'expression pour la sélection, le tri et la comparaison des données dans les documents XML, souvent utilisé avec XSLT pour la transformation et le mapping des données.

III.3. Rei

Adressant l'expressivité limitée et la contradiction sémantique des langages orientés par syntaxe (APPEL, XPref,…), un langage de politique flexible Rei est apparait.
Rei est appliqué dans le contexte des préférences d'utilisateur. Une ontologie spécifique de domaine fournit les classes et les propriétés appropriées pour la définition des préférences de la vie privée. Beaucoup d'éléments d'ontologie correspondent aux éléments d'APPEL. Les conditions préalables additionnelles permettent le filtrage des règles, avant que les conditions soient évaluées.
Comme décrit dans les langages de préférence, les conditions permettent la référence aux éléments d'une politique de P3P. Pour cela, des rapports des ontologies additionnels peuvent être employés, qui facilitent l'expression des pratiques de la vie privée.
En plus le langage permet la définition des priorités d'une règle, qui aident des utilisateurs en déterminant le comportement d'évaluation. Rei fournit également des éléments pour les spécifications des engagements qui sont liés aux actions accordées.
Comparé aux langages orientés par syntaxe, Rei qui se base sur les ontologies offre une variété maximum de préférences de la vie privée. **[49]**

IV. Quelques outils existants

IV.1. PrivacyBird

L'opérateur AT&T[18] propose un outil baptisé PrivacyBird[19] (l'oiseau de la vie privée) pour connaître d'un coup d'œil, la politique concernant les données personnelles, du site Web visité.
Disponible en version bêta, PrivacyBird s'installe comme une extension à Internet Explorer. Il repose sur la norme P3P (Platform for PrivacyPreferences) qui permet à un site Web d'inclure sous forme de code XML (non visible par l'internaute) sa politique de gestion des données personnelles.
A chaque arrivée sur un site Web, l'oiseau analyse les informations fournies par le site au format P3P et les compare aux préférences fixées par l'internaute. Un utilisateur

[18] Le leader Américain des télécommunications de tous types : vocale, vidéo, données et Internet pour les particuliers et les entreprises.
[19] Pour plus d'information, visitez le site: **www.privacybird.org/.**

peut, par exemple, choisir d'autoriser la collecte et la revente de ses données personnelles.

Selon le niveau de sécurité, PrivacyBird sonne l'alerte : de couleur verte, et accompagné d'un gazouillis pour les sites conformes en tout point au souhait de l'internaute, jusqu'au rouge et au croassement pour les sites prenant trop de liberté avec ses données personnelles.

PrivacyBird va au-delà du signal sonore et visuel. Un menu déroulant permet d'accéder à une version résumée des règles appliquées par le site visité, ainsi qu'un lien direct vers la page d'inscription/désinscription à d'éventuelles newsletters.

Si le site n'a pas traduit au format P3P sa politique sur les données personnelles, le signal passe au jaune, et le chant est moins " enjoué ". C'est d'ailleurs le cas de la majorité des sites aujourd'hui. En effet, le P3P est aujourd'hui très peu utilisé ce qui limite l'intérêt de PrivacyBird.

Enfin, l'oiseau ne fait que signaler les données récoltées par le site, sans intervenir. C'est à l'internaute de choisir s'il accepte de surfer sur un site non respectueux de sa vie privée. **[50]**

IV.2. Microsoft Internet Explorer

Le navigateur web Microsoft Internet Explorer inclut la gestion des cookies qui permet aux utilisateurs de spécifier des règles du cookie-blocage qui sont basés sur les politiques compactes P3P.

Internet Explorer est préconfiguré avec six paramètres : bloquez tous les cookies, autorisez tous les cookies, hauts, moyen-haut, moyens, et bas. Comme le montre la figure II.9, les utilisateurs peuvent sélectionnez leur cookie et voir une description courte de chaque cadre. Internet explorer est configuré par défaut au niveau moyen. **[51]**

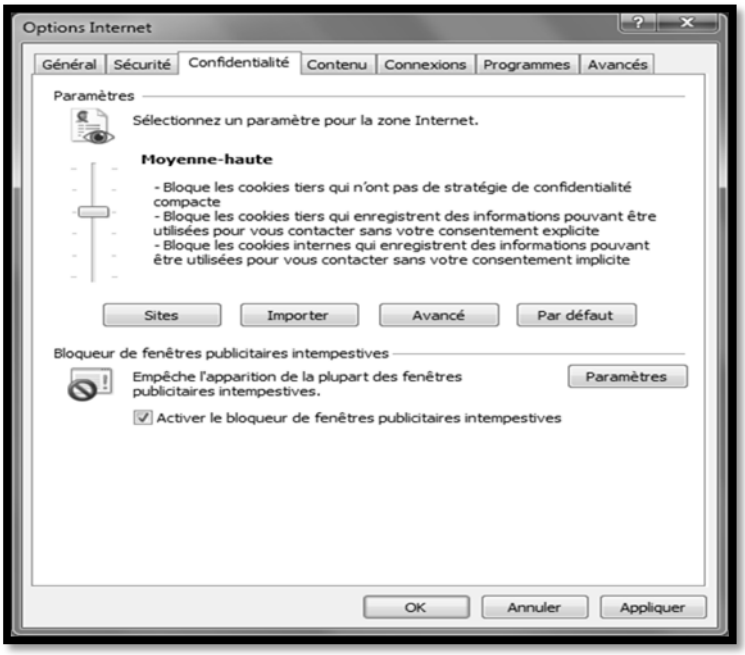

Figure II.9 : Forme de configuration d'internet explorer **[51]**

IV.3. Netscape Navigator

Netscape Navigator 7 inclut la gestion des cookies qui permet aux utilisateurs de spécifier les règles du cookie-blocage qui sont basé sur les politiques compactes de P3P qui sont semblable à ceux trouvé dans IE6.

L'interface de la spécification des préférences des utilisateurs du Netscape montré dans la figure II.10, utilise un langage similaire à celui utilisé par l'interface d'IE6. **[51]**

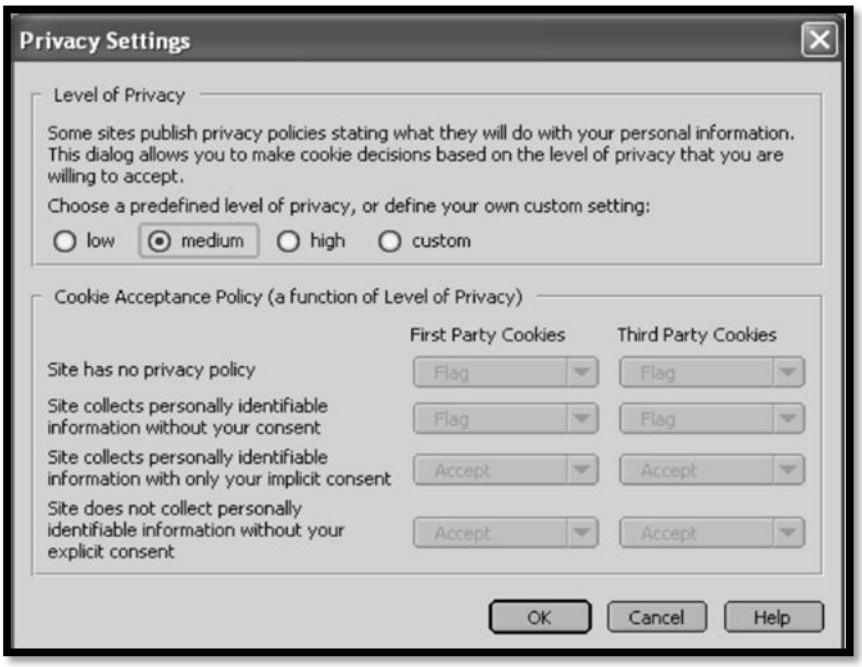

Figure II.10 : Interface de préférences de Netscape **[51]**

V. Conclusion

Bien que les langages de politiques de la vie privée fournissent un moyen technique permettant aux utilisateurs d'être informés des politiques de confidentialité avant de confier des renseignements personnels, ils n'offrent aucun mécanisme technique qui garantisse le comportement des sites conformément à leurs politiques. Les produits qui mettent en œuvre cette spécification peuvent fournir une aide dans ce sens, selon les mises en œuvre en question, mais cela n'est pas traité par cette spécification. Toutefois, le protocole P3P complète les lois et les programmes auto-règlementés définissant des mécanismes d'application. En outre, le protocole P3P ne comprend aucun mécanisme de transport des données ou de sécurisation des données personnelles en transit ou stockées. On peut intégrer P3P à des outils conçus pour faciliter le transport des données. Ces outils devraient inclure les sécurités appropriées.