Garantia de Políticas de Privacidade utilizando-se Certificação Digital

R. A. Gotardo, R. A. Rios, R. E. Grande, S. D. Zorzo, *Universidade Federal de São Carlos - S.P.*

Abstract — **The Brazilian legislation does not protect completely the privacy of the Web user. The issues of user privacy at the Internet access are considered introducing an architecture to guarantee information security. This architecture provides tools to warrant that the privacy policies have juridical legitimacy. This judicial quality is reached by the description of such policies in the format of P3P protocol, the checking of these policies using privacy seals and the authentication of the seal by means of digital certificates.**

Index Terms — **Internet, Privacidade, Personalização, Segurança.**

I. Introdução

O conhecimento humano é, atualmente, o principal capital da sociedade contemporânea, a chamada "sociedade da informação".

A informação é a base geradora ou transformadora do conhecimento. Portanto, é objeto de preocupação a proteção e a manutenção desta para que sua utilização seja eficiente e segura. Isto insere também a necessidade de reformulação de conceitos, busca por novos métodos e princípios que tentarão equilibrar as relações entre indivíduos dessa sociedade, considerando que, na maioria dos casos, as informações são a respeito de pessoas, sejam estas clientes, usuários, parceiros, etc. [23]

As informações pessoais requerem proteção jurídica para que não sejam utilizadas de forma indevida ou de forma não autorizada. Essa proteção também evita prejuízos significativos e danos das mais variadas formas. Neste intuito, vários movimentos pelo mundo e no Brasil incitam a defesa da privacidade.

Muitos autores citam que privacidade é um direito defendido em nossa Constituição Federal, assegurado por nossos Códigos (notadamente o Civil, o Penal, o de Defesa do Consumidor e o Comercial) e protegido por leis esparsas. Contudo, surpreende o fato da palavra privacidade não aparecer em nossa Constituição, não constar em nossos Códigos e nem ser citada pelas mencionadas leis [20].

Um conceito de privacidade amplamente difundido é que "Privacidade é o direito de estar sozinho". Além desta afirmação tem-se "O direito à privacidade termina com a divulgação de fatos pelo indivíduo ou com o seu consentimento".

Identifica-se, então, um cuidado que cada um deve ter em proteger sua privacidade, pois, uma vez que alguém divulgue ou autorize a divulgação de um fato ou informação pessoal, não há como reverter a situação [17].

Pode-se resumir grande parte dos problemas associados à privacidade do indivíduo como sendo a manipulação de informações pessoais sem autorização ou conhecimento do mesmo.

No Direito, é possível constatar que a questão da privacidade alcança várias esferas, seja Civil, Administrativa ou Penal.

Dentro destas esferas, surge a necessidade de leis que sejam relacionadas à proteção da privacidade.

No Brasil não há legislação específica, mas a manutenção da privacidade e a sua violação encontram subsídios em princípios garantidos em Códigos como o Penal, o Civil e o de Defesa do Consumidor [13].

Além de legislação específica, é necessária a regulamentação dos serviços e práticas que possam violar a privacidade das pessoas. Esse processo objetiva não só punir, como também coibir, agindo de forma ostensiva, evitando a violação da privacidade.

Existem maneiras de garantir ao usuário a proteção de sua privacidade nos mais diversos meios. Dentre estas, os chamados "Selos de Privacidade" regulam as políticas de privacidade dos sites da internet. Porém, também existem formas de confundir ou enganar o usuário, cuja confiança depositada em determinado site esteja sendo subvertida pela violação de sua privacidade.

O objetivo deste trabalho será relacionar práticas de violação e de defesa da privacidade do usuário na internet à legislação existente no Brasil, demonstrando a importância da regulamentação para coibição das práticas ilegais e garantias de melhor utilização das informações dos usuários. Neste mesmo intuito, propor-se-á uma infra-estrutura, objetivando legalizar as políticas de privacidade descritas pelos sites, assegurando ao usuário uma legítima sensação de segurança enquanto navega por estes sites.

Este trabalho foi apoiado em parte pela CAPES (Brasil).

R. A. Gotardo, Departamento de Ciência da Computação da Universidade Federal de São Carlos e CAPES (e-mail: reginaldo_gotardo@dc.ufscar.br).

R. A. Rios, Departamento de Ciência da Computação da Universidade Federal de São Carlos e CAPES (e-mail: ricardo_rios@dc.ufscar.br).

R. E. Grande, Departamento de Ciência da Computação da Universidade Federal de São Carlos e CAPES (e-mail: robson_grande@dc.ufscar.br).

S. D. Zorzo, Departamento de Ciência da Computação da Universidade Federal de São Carlos (e-mail: zorzo@dc.ufscar.br).

II. LEGISLAÇÃO

A privacidade dos usuários da internet no Brasil vem ganhando cada vez mais importância com diversos trabalhos publicados a respeito.

Apesar de no Brasil não existir lei específica sobre a proteção à privacidade, há tipificações incluindo crimes que atentam contra a privacidade das pessoas. Na câmara dos deputados há um Projeto de Lei específica sobre privacidade (P.L. n.o 3.360/00), mas ainda não integra as regulamentações a respeito do assunto, nem inclui a criação ou definição de órgão de defesa e normatização dos serviços que lidam com informações dos usuários. A proposta deveria estabelecer uma multa maior do que aquela que foi submetida à apreciação, oscilando entre trezentos reais a um mil reais.

O primeiro princípio de proteção à privacidade está contido no artigo 5º da Constituição Federal do Brasil, onde se afirma que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". Como já mencionado, não há a palavra privacidade em nenhuma parte da nossa Constituição, porém, entende-se que a violação da vida privada e da intimidade atente contra o princípio da privacidade [13].

Segundo o Artigo 159 do Código Civil Brasileiro "todo aquele que, por ação ou omissão voluntária, negligência, ou imprudência, violar direito, ou causar prejuízo a outrem, fica obrigado a reparar o dano". Desta forma, considerando-se que a violação da privacidade de alguém poderá causar-lhe dano, ao autor caberá a reparação.

De acordo o artigo 6º do Código de Defesa do Consumidor, "são direitos básicos do consumidor a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços". Assim, mesmo não definida lei específica, ao consumidor é assegurada a proteção contra práticas abusivas. Nestas práticas, mecanismos colhem informações dos usuários que são utilizadas de forma ilegal ou sem consentimento do mesmo. Ainda neste artigo, é garantido ao consumidor "a efetiva prevenção e reparação de danos patrimoniais e morais, individuais e coletivos" (inciso VI).

A. Mecanismos de personalização que violam a privacidade na Web

Alguns mecanismos de coleta de informações são os *Cookies*, os *Web Bugs* e o *Clickstream*. Estes mecanismos são chamados de coleta implícita, pois muitas vezes os usuários não têm conhecimento do funcionamento destes ou não são informados sobre isto. Existem também mecanismos explícitos de coleta, como formulários para preenchimento, não só de dados pessoais, mas também de informações sobre preferências do usuário. O *Data Mining*, é um mecanismo de análise de informações coletadas, sejam estas explícitas ou implícitas.

Esta análise pode, em alguns casos, gerar novas informações, incoerentes ou incorretas. Isto pode caracterizar difamação (prevista no Código Penal no artigo 139) ou injúria (Código Penal, artigo 140) caso o método de análise destas informações falhe ao inferir resultados incorretos, imprecisos ou incoerentes.

Um exemplo disto seria um usuário que acessa um site de vendas de livros, procurando sempre por livros relacionados à doenças, como a Aids. Uma falha no mecanismo do *Data Mining* poderia concluir que o usuário é uma pessoa portadora do vírus HIV, acarretando prejuízos à pessoa que pode sofrer preconceitos caso estas informações sejam divulgadas.

O principal objetivo dos *Cookies* é a manutenção da sessão do usuário quando acessa algum *Web* site, porém insere informações no computador do usuário e depois se vale delas, freqüentemente, sem seu consentimento. Os *Web Bugs* tem como objetivo verificar se determinado usuário acessou algum artefato da *Web*. Estes dispositivos são importantes para a criação de perfis de usuários, controles estatísticos e, posteriormente, envio de formas de propaganda, que podem ser caracterizadas como *Spam*.

A função do *Clickstream* é a criação de perfis de usuários com base na sua navegação entre as páginas da *Web*.

Violam, assim, o artigo 5º, inciso X da Constituição Federal do Brasil bem como o Código de Defesa do Consumidor em seu artigo 43, parágrafo 2º, além de seu caput – defendendo o acesso às informações dos consumidores e que a abertura de cadastro, registro e dados pessoais e de consumo (principalmente) devem ser comunicadas ao consumidor por escrito, caso não solicitadas por ele. Ainda neste artigo, no 3º parágrafo, ao consumidor é assegurado o direito de corrigir estes dados quando julgá-los incorretos ou incoerentes.

Continuando no Código de Defesa do Consumidor, no artigo 53, onde legisla sobre o que é o Contrato de Adesão e que limitações de direitos devem ser redigidas com destaque. Verifica-se, desta forma, a existência de artigos que garantam o direito à privacidade das informações dos usuários, do acesso destes a estas informações e da punição em caso de violação destes direitos, mesmo que indiretamente [20] [21].

O *Spam* é uma forma de correspondência indesejada. O direito da vida íntima, ou seja, o direito à privacidade também inclui o direito de ser deixado só. Logo, o *Spam* caracteriza uma violação da privacidade das pessoas. Viola o artigo 5º, inciso X da Constituição Federal do Brasil; o artigo 6º do Código de Defesa do Consumidor, onde versa sobre práticas de propaganda enganosa e abusiva; os artigos 146, 147, 265 e 266 do Código Penal; bem como o artigo 65 da Lei de Contravenções Penais [20].

Os artigos 146 e 147 do Código Penal tratam do constrangimento ilegal e ameaça, respectivamente, pois, através do *Spam*, pode-se constranger alguém por grave ameaça a fazer algo ilegal ou deixar de fazer algo legal. Também é possível ameaçar pessoas com o uso do *Spam*, utilizando-se de informações enganosas.

Já os artigos 265 e 266 do Código Penal versam sobre

"atentado contra a segurança de serviço de utilidade pública" e a "interrupção ou perturbação de serviço telegráfico ou telefônico", perfeitamente cabíveis, considerando a internet um serviço de utilidade pública (talvez o maior deles em abrangência) e, muitas vezes, com infra-estrutura dependente dos serviços telefônicos.

O artigo 65 da Lei de Contravenções Penais refere-se a "molestar alguém ou perturbar-lhe a tranqüilidade, por acinte ou por motivo reprovável", onde o *Spam* enquadra-se muito bem como motivo reprovável.

Também existem práticas utilizando *Web Bugs* onde sites terceiros podem ser informados sobre a comunicação dos usuários com o site original.

B. *Garantindo sua própria privacidade na Web*

Existem mecanismos ou ferramentas que visam à garantia da privacidade dos usuários. Garantia esta prevista na Constituição Federal do Brasil. Sendo assim, são formas de proteger um direito pessoal e que, apenas por isto, não deveriam violar nenhuma lei. Porém, como contradições podem ocorrer no ordenamento jurídico, tratar-se-á aqui sobre a legalidade destes mecanismos.

1) A Criptografia: A criptografia é uma forma de "disfarçar" informações de acordo com um algoritmo e protegê-las por uma chave única e dificilmente decifrável.

Como todo cidadão tem o direito de expressar-se e sua comunicação não pode ser interceptada, a criptografia apresenta-se como um mecanismo legal.

No artigo 5º, inciso XII é assegurada a inviolabilidade do sigilo da correspondência e outros tipos de comunicações (onde se incluem as de dados), salvo por ordem judicial ou para investigação criminal ou instrução penal em formas estabelecidas por lei. Sendo assim, a criptografia não pode ser considerada ilegal, pois não há lei que impeça seu uso nas comunicações, mesmo havendo lei que possibilite a interceptação de comunicações, por meio de ordem judicial, estando esta criptografada ou não [21].

2) Agente de Privacidade e Filtros: Agentes de privacidade são programas "inteligentes" que informam aos usuários a respeito da violação de sua privacidade enquanto navegam pelos sites da *Web*.

Filtros são ferramentas seletivas que podem bloquear e-mails, páginas *Web*, *Cookies*, propagandas, *JavaScript* e outros conteúdos.

Como são ferramentas para o usuário manter o controle de sua privacidade não possuem restrições legais.

3) Anonimato, Pseudônimos e Máscaras: A palavra anonimato, derivada do latim *anonymus* (sem nome, sem assinatura), é a forma de navegação por sites de *Web* onde o usuário utiliza algum mecanismo para que sua identidade não seja revelada. Por identidade, considera-se o número do IP (*Internet Protocol*) de sua máquina, que poderia, mediante investigação, levar à identificação do usuário.

No artigo 5º, inciso IV, da Constituição Federal é respeitada a manifestação do pensamento com veto ao anonimato. Porém, nada é afirmado sobre o anonimato de trânsito, ou seja, na manifestação do pensamento é necessária a identificação de seu autor, porém, ao locomover-se pelas ruas, ao entrar em lojas, restaurantes, ou ao navegar na internet não há obrigatoriedade de identificação do usuário. Não sem o consentimento do mesmo.

E, como no inciso II deste mesmo artigo, "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei", a utilização de mecanismos que tornem a navegação dos usuários pela internet anônima não é ilegal.

Os Pseudônimos são melhorias no anonimato, garantindo melhor personalização dos serviços oferecidos ao usuário.

Com o uso do anonimato, um site não pode identificar os usuários a cada visita e, assim, não pode propor personalização de seus serviços.

O conceito de máscara [24] reflete o modelo da personalidade pública do indivíduo. Uma espécie de interface entre o indivíduo e a interação (comunicação) com o meio social.

Ishitani [8] utiliza esse conceito para construção de um sistema de navegação anônimo denominado MASKS. Este sistema é uma versão melhorada de pseudônimos e garante melhor personalização para os usuários, sem prejudicar sua privacidade, buscando um equilíbrio entre os dois.

Nenhum deles possui impedimentos legais, estando relacionados ao comportamento social do indivíduo e não constituindo crime de falsidade documental (Código Penal, artigos 296 até 305) e nem crime de falsa identidade (artigos 307 e 308) quando tratar-se de trânsito do indivíduo e em defesa da sua privacidade.

III. POLÍTICAS DE PRIVACIDADE

As políticas de privacidade dos sites da *Web* são documentos descrevendo a importância dada por uma determinada entidade (seja pessoa física, jurídica ou o próprio governo) à privacidade de quem está utilizando o site. Neste documento, são detalhadas informações sobre a coleta dos dados (quais mecanismos utilizados) e sobre o destino destes mesmos.

O maior objetivo das Políticas de Privacidade é aumentar a sensação de segurança dos usuários. Também, desta forma, as políticas de privacidade são atividades de Marketing [10].

Legalmente, não havendo regulamentação destas políticas não poderão ser consideradas válidas.

Para que os usuários não tenham que ler toda a política de privacidade em cada site visitado, escolhendo o que melhor lhe convier, foi criado o conceito de protocolos de negociação, através dos quais são automatizadas tais políticas e, assim, ferramentas podem ser criadas para leitura e análise automáticas.

A. *Protocolos de Negociação - a P3P*

A Plataforma para Preferências de Privacidade (P3P - *Plataform for Privacy Preferences*) é uma tentativa de padronização de protocolo de negociação e permite a negociação do usuário com o site, desenvolvida pelo Consócio

da *World Wide Web*.

É um conjunto de especificações sobre práticas de coleta e uso da informação por uma organização e visam assegurar ao usuário a garantia de não ter sua privacidade prejudicada ao acessar serviço disponibilizado por algum site na *Web*.

A P3P possibilita que agentes do usuário avaliem as políticas de privacidade de um site, desde que elas estejam disponíveis no formato estabelecido pela proposta.

A P3P pode ser considerada um complemento e um mecanismo de reforço às leis e aos programas de auto-regulamentação [34].

O protocolo introduzido pela Plataforma 3P é projetado em um formato XML, conhecido como política P3P de privacidade.

A P3P pode ser implementada pelos sites *Web* em seus servidores através da tradução de suas políticas de privacidade escritas numa linguagem humana para a sintaxe P3P. No final cria-se um ou mais arquivos-textos que contém suas políticas de privacidade traduzidas para essa sintaxe no formato XML.

Depois de publicar esses arquivos resultantes, um arquivo de referência da política é publicado junto desta para indicar quais partes do site a política será aplicada. Para auxiliar os operadores a desempenhar a tradução das políticas de privacidade para um formato padrão, existem diversas ferramentas automáticas.

Alguns aplicativos de navegação na *Web* já oferecem mecanismos para a leitura de políticas de privacidades dos sites, desde que estejam no formato P3P.

IV. SELOS DE PRIVACIDADE E CERTIFICAÇÃO DIGITAL

Um Selo de Privacidade é fornecido por uma empresa independente que verifica em uma página da *Web* as políticas de privacidade, a maneira como os dados pessoais são coletados, processados e compartilhados [10]. Com isso, sempre que um usuário entrar em um site o qual exibe um Selo de Privacidade, saberá que a entidade emissora de tal selo verifica periodicamente esse sistema *Web*. Esta verificação é realizada para que as informações contidas nas políticas de privacidade sejam respeitadas e a manipulação dos dados pessoais de um usuário não viole sua confiança.

Desta forma, os Selos de Privacidade são afirmações positivas a respeito das políticas de privacidade de um site.

Os Selos de Privacidade começaram a ser desenvolvidos com o objetivo de acompanhar o forte crescimento das vendas de produtos pela internet e, assim, tiveram o seu conceito intrinsecamente ligado à definição de B2C (*Business-to-Commerce*). As Empresas de comércio eletrônico sentiram a necessidade de aumentar a confiança dos usuários que visitavam seus *Web* Sites e garantir que os dados de cada cliente fossem mantidos de forma segura e confidencial.

Assim, a confiança dos consumidores tornou-se um fator de grande relevância para a estratégia das empresas de comércio eletrônico [15].

Além de garantir ao usuário que seus dados serão respeitados de acordo com as informações contidas na política de privacidade, os Selos de Privacidade permitem, ainda, por intermédio das coletas e análises dos dados, diferenciar cada cliente. Tornou-se possível traçar um perfil dos usuários, que deixaram de ser anônimos, baseando-se no histórico de acesso. A personalização de sites *Web* não serviu apenas para oferecer aos usuários produtos que eram de seu interesse, mas também se tornou um grande utilitário das empresas que passaram a oferecer produtos diferenciados, limitando as ofertas de acordo com o perfil e influenciando as intenções de cada cliente [10]. Aproveitando-se da aceitabilidade dos Selos por parte dos usuários, as empresas passaram a usar este mecanismo como uma solução baseada no Marketing [10] e obtiveram um tratamento diferenciado em relação às concorrentes que não ofereciam este recurso.

Existem diversas entidades que emitem Selos de Privacidade, mas as três mais proeminentes são *TRUSTe*, *WebTrust* e *BBBOnline* [12]. Mesmo com um grande número de entidades, existem requisitos padrões que são exigidos por todas, como a escrita de uma política de privacidade e uma garantia de que os dados armazenados estarão seguros. A segurança das informações é extremamente relevante, pois informações que estão desprotegidas não podem ser consideradas privadas, existindo assim uma estreita relação entre privacidade e segurança [12].

O uso de Selos de Privacidade tem sido criticado principalmente porque poucos sites comerciais possuem alguma declaração de privacidade. E, entre os sites que adotam esse sistema, existem casos de abusos no uso ilegítimo dos Selos de Privacidade.

Outra crítica é que usuários não entendem completamente a forma ou função dos Selos de Privacidade, poucos podem reconhecer um selo como verdadeiro e poucos deles reconhecem como uma ferramenta importante na decisão para confiar em sites *Web*.

Apesar destes dados negativos, os usuários da *Web* estão começando a reconhecer os Selos de Privacidade e seu significado. *Cheskin Research* reportou que 69% dos usuários *Web* reconheceram o selo da *TRUSTe* e 37% o selo da *BBBOnline* [14]. O selo da *TRUSTe* aumentou a confiança em um site *Web* para 55% segundo esta mesma pesquisa. Esse sucesso tem origem no aumento de adoção dos Selos pelos sites.

Os fatos e resultados de pesquisas mostram que há muito a ser explorado nesse contexto para melhorar algumas características e levar a uma maior adoção destas práticas.

O Certificado Digital é um documento eletrônico especificado pelo padrão internacional X509 que tem como principal objetivo associar chaves públicas às diversas informações de uma entidade [4].

Os certificados digitais são enviados sempre que o servidor necessite criptografar as informações contidas em uma requisição, ou quando for necessário reconhecer a identidade de uma entidade.

A Certificação Digital pode ser definida como um conjunto de técnicas para fornecer segurança às comunicações e às transações eletrônicas [18].

Um dos grandes benefícios trazidos pelo uso de Certificação Digital é a possibilidade de disponibilização de serviços fáceis de acessar, com maior agilidade e custos reduzidos [19].

O que torna um certificado digital confiável é a assinatura e a identificação da entidade que o emitiu. Para ter a sua validade garantida, os certificados devem ser emitidos por uma Autoridade Certificadora (CA - *Certificate Authority*) [3].

As principais características de um Certificado Digital emitido por uma CA, podem ser resumidas, na ligação da chave publica ao nome que o certificado identifica, evitando a falsificação das chaves, na inclusão do nome da CA, data de expiração e assinatura digital da CA emissora [4].

Para emitir um certificado, uma CA deve respeitar deveres e obrigações descritos em um documento público chamado de Declaração de Práticas de Certificação [19].

Para garantir a validade da Autoridade Certificadora que assinou o certificado, é necessária a definição de uma infra-estrutura técnica e legal, normatizando práticas que suportem as transações eletrônicas com técnicas eficientes no combate aos problemas de segurança do próprio meio.

A solução apresentada é a chamada Infra-estrutura de Chave Pública (ICP ou PKI - *Public Key Infrastructure*) que fornece, através da internet, meios para identificação segura das pessoas e garante a integridade dos registros e sigilo da informação. A PKI associa pessoas a chaves para a criação de uma assinatura digital, visando à realização de negócios eletrônicos eficazes e seguros.

A validade jurídica da certificação digital no Brasil foi regulamentada em 24 de agosto de 2001, pela Medida Provisória 2.200-2, que constituiu a chamada Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil).

As diretrizes propostas na medida têm efeito de lei e desde então não sofreram modificações significativas.

De acordo com o artigo 10, parágrafo 1º desta MP, "os documentos eletrônicos produzidos com a utilização de certificação disponibilizados pela ICP-Brasil" possuem validade jurídica.

A autoridade certificadora raiz da cadeia da ICP-Brasil tem como função básica a execução das políticas de certificados e normas técnicas e operacionais. No Brasil, é representada unicamente pelo Instituto Nacional de Tecnologia da Informação.

Além das vantagens citadas, o uso de certificados deve fornecer uma garantia de sigilo e privacidade, identificação do remetente de uma mensagem, não havendo mais dúvidas sobre a identidade do emissor, e garantia do não-repúdio, fazendo com que um documento eletrônico possua uma validade jurídica, impossibilitando que um usuário afirme que não realizou determinada transação [18].

V. ARQUITETURA DE AUTENTICAÇÃO DE SELOS DE PRIVACIDADE

Reconhecida a importância da regulamentação das atividades relacionadas à coleta de informações dos usuários na Internet, a existência de mecanismos e entidades que garantam segurança das informações dos usuários é justificada, pois a legislação garante a proteção da privacidade, mesmo não havendo lei específica sobre o assunto.

Na existência de invasão da privacidade do usuário, mecanismos podem ser utilizados para evidenciar e provar o abuso. Essas ferramentas policiam as atitudes de sites e garantem segurança de dados do usuário no acesso a serviços da *Web*.

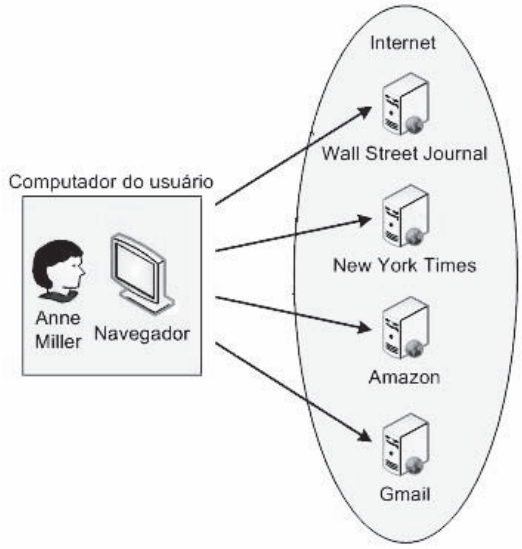

Fig. 1. Usuário acessa diretamente sites da internet

Realizando-se a regulamentação necessária aos serviços relacionados à coleta e manipulação de informações dos usuários, a apresentação de provas materiais será facilitada.

Quando houver a ocorrência de delitos que violem o direito à privacidade do usuário, uma estrutura de autenticação com validade jurídica garante o não-repúdio das ações.

Dessa forma, uma estrutura que permita supervisionar e garantir o comportamento correto de sites na coleta e no manuseio de informações é apresentada. Através das leis existentes, esse mecanismo impõe um regime de boa conduta a empreendimentos on-line.

Num cenário comum, o usuário acessa sites diversos utilizando um navegador da *Web* de forma direta, como demonstrado na Figura 1.

A descrição formal apresentada pela Plataforma 3P é usada para descrever as políticas de privacidade. Um agente do usuário pode analisar estas políticas e informá-lo, garantindo-lhe um poder de escolha sobre o site. A Figura 2 demonstra a navegação com o auxílio de um agente do usuário.

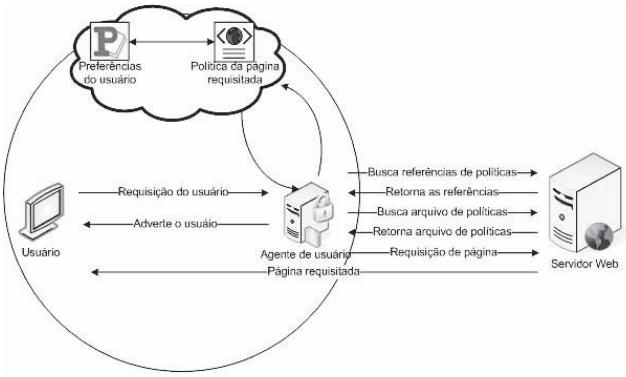

Fig. 2. Acesso com auxílio de agente do usuário para leituras das políticas de privacidade descritas em P3P

Através do uso de selos de privacidade, como demonstrado na Figura 3, a análise feita pelo agente de usuário fica garantida, pois tais selos são fornecidos por uma entidade confiável e conhecida.

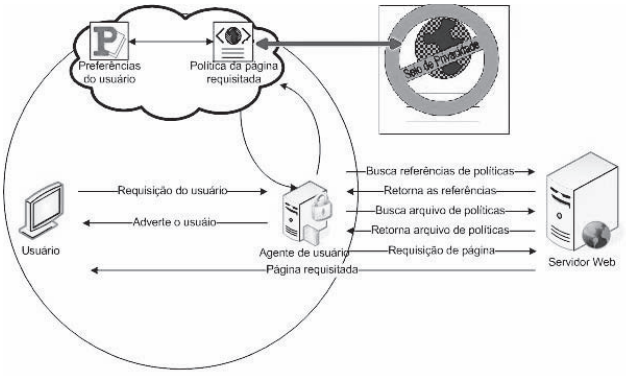

Fig. 3. Utilização de Selo de Privacidade na Política Descrita pelo Site *Web*

A utilização de selos de privacidade garante aos usuários certo nível de confiabilidade nas políticas descritas pelos sites. Políticas estas, que muitas vezes nem são lidas pelos usuários, mas que podem ganhar maior relevância na melhoria de suas declarações e na criação de garantias de privacidade.

As declarações da política devem ser objetivas e estarem escritas em um linguajar apropriado para os visitantes de um site específico. As garantias são providas por entidades confiáveis que supervisionam as atitudes irregulares de coleta e manuseio de informações de usuários da *Web*.

Um problema que ocorre é que os selos não possuem validade legal, para tanto é necessário algo que o valide.

Sendo assim, nessa estrutura de verificação, os certificados digitais são utilizados para delimitar os selos de privacidade.

Como descrito na figura 4, as propriedades da criptografia assimétrica asseguram a confiabilidade e a autenticidade da identidade do site, da entidade que emitiu o selo e do próprio selo. Informações que identificam o site são inseridas nesse novo selo de privacidade. A assinatura da entidade de privacidade, que atua como uma autoridade certificadora, garante a autenticidade do selo.

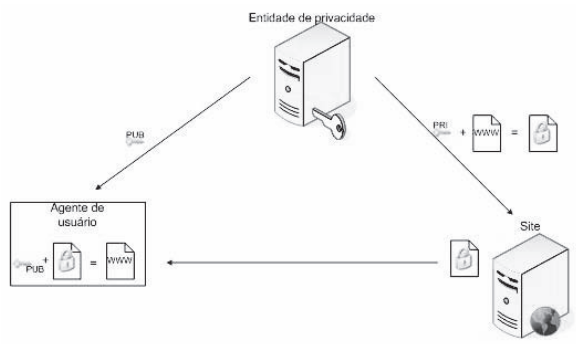

Fig. 4. Processo de Verificação da Autenticidade de um Selo de Privacidade

Essa verificação do selo concedido insere validade jurídica na transação entre o usuário e os sites *Web*. Esse processo de análise de políticas de privacidade e de verificação de uma entidade de privacidade propicia maior confiança ao usuário de que o comportamento dos sites que ele visita é correto.

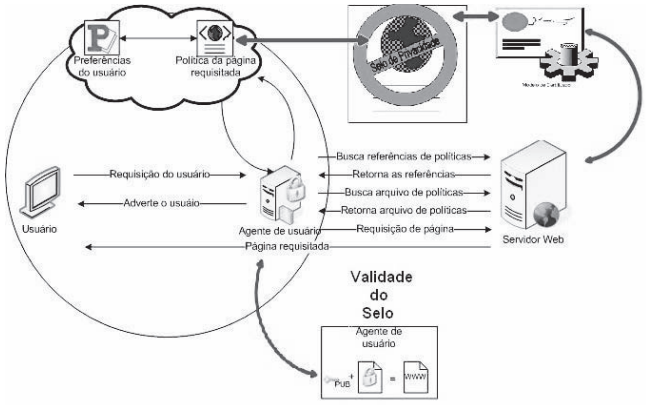

Fig. 5. Visão Geral da Arquitetura

Portanto, a estrutura composta pela verificação automática de políticas de privacidade, pela validação de selos e pela certificação digital, na Figura 5, garante para o usuário segurança de suas informações nas transações no acesso a serviços na *Web*.

VI. CONCLUSÃO

Através do exposto, pode-se verificar que é de suma importância a regulamentação das atividades relacionadas à coleta de informações dos usuários na internet, pois a legislação brasileira garante, de certa forma, a proteção da privacidade, mesmo não havendo lei específica sobre o assunto.

Ressaltando-se que, por proteção entende-se a garantia de reparação de dano – e, algumas vezes, a tipificação penal -, mas não o policiamento para assegurar a privacidade dos usuários.

Mesmo assim, a adequação de leis apenas será efetiva quando houver mudanças em âmbitos sociais, culturais e políticas.

Realizando-se a regulamentação necessária aos serviços

relacionados à coleta e manipulação de informações dos usuários tornar-se-á mais fácil a apresentação de provas materiais, quando houver a ocorrência de delitos que violem o direito à privacidade dos usuários.

A utilização de selos de privacidade garante aos usuários certo nível de confiabilidade nas políticas descritas pelos sites. Políticas estas, que muitas vezes não são lidas pelos mesmos.

Utilizando-se políticas descritas através da Plataforma 3P e validando-as com selos de privacidade de entidades confiáveis, conhecidas e com validade jurídica, traria aos usuários uma melhor sensação de que sua privacidade é respeitada. Garantindo, através do mecanismo de certificação digital, que um selo emitido a um site não seja forjado, também será garantida a identidade do site, da entidade que emitiu tal selo e do próprio selo.

Não há, no Brasil, órgão competente e não é conhecido projeto de lei sobre a criação de órgão regulador no uso de selos de privacidade com validade jurídica.

Assim, a criação de órgão competente para gerenciar as políticas de privacidade, estabelecendo regras de conduta sobre o tratamento da privacidade dos usuários é sugerida.
Esta possível entidade poderia, além de realizar a regulamentação, receber denuncias de usuários sobre violação de privacidade, realizar treinamentos, divulgações com sugestões, cartilhas, etc.

REFERÊNCIAS

[1] M. S. Ackerman e L. F. Cranor, "*Privacy critics safeguarding users personal data*". Web Techniques, Setembro 1999. Disponível em: http://www.webtechniques.com/archives/1999/09/ackerman

[2] G. M. Almeida, *"As Empresas podem "grampear" o e-mail de seus funcionários?"*. Módulo e-Security News. Rio de Janeiro. 1999. Disponível em: http://www.modulo.com.br

[3] M. Bond, D. Haywood, D. Law, A. Longshaw e P. Roxburgh, *"Yourself J2EE in 21 Days"*, I Edição, Pearson Education Inc.

[4] S. Cable, *"Professional Java Web Services"*. Capítulo 6. AltaBooks, 2002.

[5] J. A. Harvey, K. M. Sanzaro, *"P3P and IE 6: Good privacy medicine or mere placebo?"* Computer and Internet Lawyer, 19(4):1–6, April 2002.

[6] H. Hochheiser, *"Principles for privacy protection software"*. Proc. of 10th conf. On Computer, Freedom and Privacy: challenging the assumption, pages 69–72, 2000.

[7] H. Hochheiser, *"The platform for privacy preferences as a social protocol: An examination within the U.S. policy context"*. ACM Transactions on Internet Technology, 2(4):276–306, November 2002.

[8] L. Ishitani, *"Uma Arquitetura para Controle de Privacidade na Web"*. Tese de doutorado: Departamento de Ciência da Computação da Universidade Federal de Minas Gerais, 2003.

[9] A. Kobsa, *"Personalized Hypermedia and International Privacy"*. Communications of the ACM. May, 2002.

[10] B. Mai, N. Menon, S. Sarkar, *"Online Privacy at a Premium"*. XXXVI Hawaii International Conference on Sistems Sciences, 2006.

[11] Mcbride, Baker e Coles. *"E-Commerce Spotlight"*. Summary of ECommerce Legislation. Disponível em: http://www.mbc.com

[12] T. T. Moores e G. Dhillon, *"Do privacy seals in e-commerce really work?"*. Communications of the ACM. December, 2003.

[13] L. M. Paesani, *"Direito e Internet - Liberdade de Informação, Privacidade e Responsabilidade Civil"*. São Paulo: Editora Atlas, 2003.

[14] *"Trust in the wired Americas"*. Cheskin Research (July, 2000). Disponível em: http://www.cheskin.com/think/pressreleases/fprivreport.pdf

[15] G.L. Urban, F. Sultan e W. J. Qualls. *"Placing trust at the center of your Internet strategy"*. MIT Sloan Management Review 42 1 (2000), 39–48.

[16] H. Wang, et al. *"Consumer privacy concerns about internet marketing"*. Communications of the ACM, 41(3): March 1998.

[17] S. Warren e L. D. Brandeis, *"The Right to Privacy"*. HARVARD LAW REVIEW. Vol. 04, fls. 193, 1980. Disponível em: http://www.louisville.edu/library/law/brandeis/privacy.html

[18] *"Certificação Digital – Entenda e Utilize"*. Acessado em 02 de Setembro de 2006. Disponível em: http://www.iti.br/twiki/pub/Main/Cartilhas/CertificacaoDigital.pdf

[19] *"O que é Certificação Digital?"*. Acessado em 02 de Setembro de 2006. Disponível em: http://www.iti.br/twiki/pub/Main/Cartilhas/brochura01.pdf

[20] A. M. Silva Neto, *"E-mails indesejados luz do direito"*. Editora Quartier Latin, 2002.

[21] A. M. Silva Neto, *"O anonimato na Web"*. Disponível em: http://www.advogado.com/internet/zip/anonimo.htm

[22] A. M. Silva Neto, *"Cookies, esses indigestos biscoitos"*. Disponível em: http://www.advogado.com/internet/zip/cookies.htm

[23] C, LUCENA NETO, *"Função social da privacidade"*. Módulo Security, 2002. Disponível em: www.modulo.com.br/pdf/funcaosocialpriv.pdf

[24] C. S. Hall, G. Lindzey, *"Theories of Personality"*. John Wiley & Sons,3rd edition edition, 1978.

[25] *"Constituição Federal do Brasil"*. Disponível em: https://www.planalto.gov.br/ccivil 03/Constituição/Constituicao.htm

[26] *"Código Penal Brasileiro"*. Disponível em: http://www.planalto.gov.br/CCIVIL 03/Decreto-Lei/Del2848.htm

[27] *"Lei de Contravenções Penais no Brasil"*. Disponível em: http://www.planalto.gov.br/Ccivil 03/Decreto-Lei/Del3688.htm

[28] *"Código Civil Brasileiro"*. Disponível em: http://www.planalto.gov.br/CCIVIL/leis/2002/L10406.htm

[29] *"Código de Defesa do Consumidor"*. Disponível em: http://www.planalto.gov.br/ccivil 03/Leis/L8078.htm

[30] *"Lei de Interceptação Telefônica"*. Disponível em: https://www.planalto.gov.br/ccivil 03/LEIS/L9296.htm

[31] *"Projeto de lei 3.360/00 pelo Senador Nelson Proença"*. Disponível em: http://www.camara.gov.br/sileg/Prop Detalhe.asp?id=19533

[32] *"Comitê Gestor da Internet no Brasil"*. Disponível em: http://www.cgi.br

[33] "Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil". Disponível em: http://www.cert.br

[34] *"Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil"*. Disponível em: http://www.cert.br

[35] R. E. Grande, *"Sistema de Integração de Técnicas de Proteção de Privacidade Permitindo Personalização"*. Qualificação de Mestrado: Universidade Federal de São Carlos, 2005.

[36] L. L. Lobatto, S. D. Zorzo, *"Avaliação dos Mecanismos de Privacidade e Personalização na Web"*. In: XXXII Conferencia Latino-americana de Informática CLEI 2006. Santiago, Chile. August, 2006.