(11) Número de Publicação: **PT 2751973 E**

(51) Classificação Internacional:
H04L 29/06 (2015.01) ***G06F 21/00*** (2015.01)

(12) **FASCÍCULO DE PATENTE DE INVENÇÃO**

(22) Data de pedido: **2012.08.30**

(30) Prioridade(s): **2011.09.02 US 201161530416 P 2011.11.29 EP 11191213**

(43) Data de publicação do pedido: **2014.07.09**

(45) Data e BPI da concessão: **2015.10.21 017/2016**

(73) Titular(es):
NAGRAVISION S.A.
ROUTE DE GENÈVE 22-24 1033 CHESEAUX-SUR-LAUSANNE CH

(72) Inventor(es):
CHRISTOPHE NICOLAS CH

(74) Mandatário:
ÁLVARO ALBANO DUARTE CATANA
AVENIDA MARQUÊS DE TOMAR, Nº 44, 6º 1069-229 LISBOA PT

(54) Epígrafe: **MÉTODO PARA CONTROLAR O ACESSO DE DADOS PESSOAIS DE UM UTILIZADOR**

(57) Resumo:
HÁ UMA NECESSIDADE DE SISTEMA E MÉTODO QUE SEJAM CONCEBIDOS PARA DAR CONTROLO PLENO E CONTÍNUO, GANHAR A CONFIANÇA DO INDIVÍDUO MÉDIO, ENCORAJANDO TAL INDIVÍDUO PARA SE TORNAR UM UTILIZADOR ABERTO E CONFIANTE DE TAL SISTEMA. É PROPOSTO UM MÉTODO PARA CONTROLAR O ACESSO DE DADOS PESSOAIS DE UM UTILIZADOR POR UM CENTRO DE CONFIANÇA QUE COMPREENDE PELO MENOS UMA BASE DE DADOS QUE INCLUI, PARA UM UTILIZADOR ESPECÍFICO, LOCAIS DE MEMÓRIA PARA DADOS PESSOAIS, CONDIÇÕES DE ACESSO ASSOCIADAS AOS DADOS PESSOAIS E DADOS DE GESTÃO QUE COMPREENDEM PELO MENOS UM CONTADOR, - CARREGAR, POR UM UTILIZADOR OS SEUS DADOS PESSOAIS NA BASE DE DADOS DO CENTRO DE CONFIANÇA E ATRIBUIR CONDIÇÕES DE ACESSO AOS REFERIDOS DADOS, OS REFERIDOS DADOS PESSOAIS SENDO DIVIDIDOS EM PELO MENOS DUAS CATEGORIAS COM DUAS CONDIÇÕES DE ACESSO DIFERENTES, CADA CATEGORIA SENDO ASSOCIADA COM UM VALOR DO UTILIZADOR, - PEDIR ACESSO AO CENTRO A CONFIANÇA POR UM TERCEIRO AOS DADOS PESSOAIS DE UMA PLURALIDADE DE UTILIZADORES, O REFERIDO PEDIDO COMPREENDENDO CRITÉRIOS DE BUSCA, - EXECUTAR PELO CENTRO DE CONFIANÇA OS CRITÉRIOS DE BUSCA NOS DADOS PESSOAIS DOS UTILIZADORES DE MODO A DETERMINAR UM PRIMEIRO CONJUNTO DE UTILIZADORES QUE CORRESPONDA AOS CRITÉRIOS DE BUSCA, - RETORNAR AOS TERCEIROS A INFORMAÇÃO QUE MOSTRA A QUANTIDADE DO PRIMEIRO CONJUNTO DE UTILIZADORES QUE CORRESPONDE AOS CRITÉRIOS, BEM COMO A SOMA DO VALOR DO UTILIZADOR DE CADA UTILIZADOR DO PRIMEIRO CONJUNTO, - RECONHECER TODA OU PARTE DA SOMA PELOS TERCEIROS, DEFININDO ASSIM UM SEGUNDO CONJUNTO DE UTILIZADORES QUE PODE COMPREENDER A TOTALIDADE OU PARTE DO PRIMEIRO CONJUNTO, - RETORNAR OS DADOS PESSOAIS DO SEGUNDO CONJUNTO DE UTILIZADOR PARA O QUAL A SOMA COBRE OS VALORES ACUMULADOS DOS

UTILIZADORES EXTRAÍDOS, - ACTUALIZAR O CONTADOR DO SEGUNDO CONJUNTO DE UTILIZADORES COM O CONTEÚDO DO VALOR DOS SEUS RESPECTIVOS DADOS PESSOAIS.

DESCRIÇÃO

"MÉTODO PARA CONTROLAR O ACESSO DE DADOS PESSOAIS DE UM UTILIZADOR"

Introdução

Com o desenvolvimento das redes de comunicação, os utilizadores dessas redes são cada vez mais solicitados a fornecer dados pessoais a provedores de serviços para alimentar esses dados pessoais em bases de dados.

À medida que o ambiente informatizado aumenta em importância e desempenho, o utilizador médio é cada vez mais frustrado pelos motores de computador de má qualidade que se preocupam muito pouco com as suas necessidades de privacidade.

Antecedentes da técnica

Algumas terceiras partes põem um alto valor nos dados pessoais que um indivíduo põe em vários sistemas conectados que fazem parte da sua vida quotidiana. A utilização que esses terceiros podem fazer vai desde estudos de mercado até a publicidade direccionada à mineração de dados e afins.

Até agora, não houve nenhuma base ou estrutura para:

1) permitir que o utilizador mantenha total controlo dos seus dados pessoais;

2) convencer o utilizador de que ele não corre um risco desproporcional em fornecer esses dados;

3) como uma etapa adicional possível, rentabilizar formalmente os dados pessoais anunciados, graças à confiança do utilizador, como benefício directo ao referido utilizador.

A qualidade das bases de dados pode ser negativamente afectada pela desconfiança dos indivíduos. No caso de um censo por exemplo, alguns utilizadores livres-pensadores adoptar comportamentos contrários à ordem estabelecida,

fornecendo dados falsos, apenas porque não confiam na entidade governamental que lhe está a solicitar o fornecimento desses dados.

Quando os dados fornecidos são claramente fora-de-alcance, a limpeza do fluxo de resultados é relativamente fácil e pode ser feita de forma automatizada, por exemplo, através de simples verificações cruzadas entre as respostas fornecidas por um único utilizador. No entanto, quando o livre-pensador é mais sofisticado e sabe como ser mais esperto do que os controlos automáticos, há muito pouco que pode ser feito para obter dados verdadeiros e uma boa qualidade resultante de bases de dados agregados.

Há, portanto, uma necessidade de um sistema que é concebido para dar controlo pleno e continuado dos seus dados por um utilizador, ganhar a confiança do indivíduo médio, encorajando tal indivíduo para se tornar um utilizador aberto e confiante de tal sistema.

O problema tornou-se mais agudo com a crescente popularidade, especialmente entre jovens adultos, das redes sociais. Os gestores de inúmeras dessas redes sociais tendem a ter pouca consideração por quaisquer desvantagens futuras da falta de experiência desses jovens adultos perante os problemas de percepção que um visitante de tais redes sociais pode encontrar.

Por exemplo, um jovem descuidado pode anunciar no seu armazenamento pessoal, organizado por uma rede social, algumas imagens que, em reconsideração ou anos mais tarde, prefeririam restringir o acesso. Tais imagens podem ser, por exemplo, vídeos ou fotografias tiradas durante uma festa privada, durante as quais o álcool, ou mais geralmente substâncias capazes de modificar o estado de consciência, foram ingeridas de inaladas.

Quando o referido jovem descuidado torna-se um graduado em busca de um trabalho, o facto de que a rede social concedeu acesso, para audiências não-restritas ou não suficientemente restritas, para as pistas do referido modo de vida ilustrado pelas imagens acima mencionadas pode ser uma desvantagem em encontrar um emprego desejado.

Se o referido jovem abraçar a carreira política, o efeito pode ser ainda mais grave, com evidências de uma vida passada como um jovem ou uma jovem que é exibido/a pela imprensa para um grande público, especialmente um público mais velho ou idoso com pouca inclinação para perdão, afectando assim a credibilidade da pessoa em questão, mesmo que essa pessoa possa ter crescido e se arrependido de seu comportamento passado como um jovem. O armazenamento contínuo, em bases de dados fora-de-alcance, de extractos de anúncios feitos por jovens pode, assim, tornar-se muito prejudicial para o seu futuro profissional ou político.

O problema torna-se mais grave pelo fato de que os gestores das redes sociais, por vezes, têm uma tendência para proteger em excesso a sua organização, no caso de se tornarem cientes de questões de propriedade de dados, alterando os termos legais aplicáveis a cada um dos membros de uma determinada rede social.

Neste caso, uma falta de consideração quanto aos interesses desses membros individuais pode resultar em danos graves aos referidos interesses. Por exemplo, condições legais são por vezes modificadas sem aviso prévio, reivindicando a posse pela rede de quaisquer e todos os dados anunciados no armazenamento pessoal do indivíduo.

Mesmo se a informação sobre uma mudança desses termos legais for comunicada aos assinantes, há uma grande

probabilidade de que uma vasta maioria dos utilizadores mais jovens não vai reagir e, portanto, aceita implicitamente tal mudança. E mesmo que alguns reajam e exijam a eliminação dos dados incriminados, eles enfrentam a perspectiva de uma acção judicial custosa contra a referida rede social, com sucesso incerto. O custo para um indivíduo de tal acção legal, em comparação com os recursos disponíveis, muitas vezes desproporcionados para a rede social como réu, pode impedir o indivíduo de iniciar essa acção, o que provoca um sentimento de frustração de sua parte. O número de casos em que a credibilidade, ou a vida pessoal, ou o futuro profissional de um indivíduo foi prejudicada, ou deteriorado, ou comprometido está em ascensão, e igualmente a cobertura pela imprensa de tais histórias, assim como a resultante conscientização do público.

Com o aumento neste número de casos, uma consequência dos factos acima mencionados é um aumento do desafio contra as redes sociais no público em geral. No entanto, as redes sociais estão na moda e estão a ganhar força entre o público mais jovem. Isso as torna inevitáveis, em grande medida a personalidades ambiciosas, que nem sempre percebem o perigo que representam para a sua futura vida social.

O documento US 2010/0088364 descreve conteúdos de redes sociais que podem ser servidos a um conjunto de utilizadores de redes sociais. O conteúdo das redes sociais servido pode incluir conteúdos semânticos associados com conteúdos específicos dos utilizadores da rede social. O conteúdo semântico pode ser compartilhado entre diferentes utilizadores da rede social durante o serviço. Pelo menos uma parte do conteúdo semântico pode ser armazenado num armazenamento local de dados associado

com um dispositivo informático do utilizador específico para quem o conteúdo semântico se aplica.

Breve descrição da invenção

É proposto um método para controlar o acesso de dados pessoais de um utilizador por um centro de confiança que compreende pelo menos uma base de dados que inclui, para um utilizador específico, locais de memória para dados pessoais, condições de acesso associadas aos dados pessoais e dados de gestão que compreendem pelo menos um contador,

- carregar, por um utilizador os seus dados pessoais na base de dados do centro de confiança e atribuir condições de acesso aos referidos dados, os referidos dados pessoais sendo divididos em pelo menos duas categorias com duas condições de acesso diferentes, cada categoria sendo associada com um valor do utilizador,
- pedir acesso ao centro a confiança por um terceiro aos dados pessoais de uma pluralidade de utilizadores, o referido pedido compreendendo critérios de busca,
- executar pelo centro de confiança os critérios de busca nos dados pessoais dos utilizadores de modo a determinar um primeiro conjunto de utilizadores que corresponda aos critérios de busca,
- retornar aos terceiros a informação que mostra a quantidade do primeiro conjunto de utilizadores que corresponde aos critérios, bem como a soma do valor do utilizador de cada utilizador do primeiro conjunto,
- reconhecer toda ou parte da soma pelos terceiros, definindo assim um segundo conjunto de utilizadores que pode compreender a totalidade ou parte do primeiro conjunto,

- retornar os dados pessoais do segundo conjunto de utilizador para o qual a soma cobre os valores acumulados dos utilizadores extraídos,
- actualizar o contador do segundo conjunto de utilizadores com o conteúdo do valor dos seus respectivos dados pessoais.

Breve descrição do desenho

A presente invenção será melhor compreendida graças às figuras anexas em que:

- a figura 1 mostra um sistema com o centro de confiança ligado à Internet
- a figura 2 mostra um sistema no qual o centro de confiança desempenha o papel de um proxy (procurador).

Descrição detalhada

A invenção consiste num sistema de assinatura para um centro de confiança TC (*Trusted Center*) aberto a pelo menos uma parte do público em geral, no qual um membro subscritor é incentivado, por recursos do sistema definidos, a manter o pleno controlo dos seus dados pessoais, uma vez que os mesmos são alimentados para o sistema. O membro subscritor é, portanto, encorajado a fornecer dados verdadeiros para o centro de confiança.

Tais características definidas do centro de confiança TC pode consistir em padrões mínimos de qualidade no processamento dos referidos dados fornecidos. Por exemplo, os sistemas existentes são capazes de rastrear o facto de que um utilizador de internet navegou por locais de hotéis na Itália, e imediatamente propõe ofertas de viagens com desconto para a Itália para aquele utilizador. Essas ofertas podem ser percebidas como publicidade intrusiva e indesejada. Um padrão mínimo de qualidade pode consistir na definição, com cada utilizador individual, em que

medida tais ofertas automatizadas podem ser geradas e exibidas.

Outra característica definida do sistema pode também consistir em fornecer a possibilidade de realmente e de forma confiável apagar um histórico de dados para o utilizador individual.

Numa forma de realização particular da invenção, um recurso do sistema está concebido para proporcionar uma transparência total a um utilizador inscrito.

Numa forma de realização particular da invenção, o sistema proporciona um nível diferenciado de controlo para um utilizador inscrito, para o tipo de dados com os quais ele alimenta o sistema.

Como primeiro exemplo, uma primeira categoria de nível de controlo é atribuído às preferências do utilizador em desporto. Tais dados de preferência podem consistir nas suas avaliações pessoais no desporto. Por exemplo, um utilizador A pode deixar que o sistema saiba que ele prefere basquete ao futebol, futebol ao ténis, e ténis ao windsurf. Tais dados de preferência também podem consistir em avaliações pessoais em diversas equipes em competição num determinado desporto. Como outro exemplo, um utilizador B pode divulgar, com um certo nível de propriedade e controlo, as informações que ele prefere um determinado time de basquete a outro time de basquete.

Como segundo exemplo, uma segunda categoria ou nível de controlo é atribuído aos passatempos do utilizador.

Como terceiro exemplo, um segundo nível de controlo é atribuído à orientação política do utilizador. Os dados sobre a orientação política podem, portanto, ser considerados, pelo utilizador, como mais sensíveis do que as preferências de desportos ou passatempos, e sejam

atribuídos um nível mais restritivo de protecção contra acesso externo de não-utilizador.

Como quarto exemplo, um terceiro nível de controlo é atribuído às preferências, orientação ou hábitos sexuais do utilizador.

Como exemplo adicional, um nível de controlo é atribuído às características do perfil de investidor do utilizador. Tais características podem ser conservadorismo financeiro, tolerância aos riscos, inclinação para investimentos de esquema alternado, comércio equitativo ou preferências de conservação da natureza em opções de investimento, ou semelhantes.

Numa forma de realização particular da invenção, o sistema proporciona um nível diferenciado de controlo sobre os diferentes tipos de dados, como acima mencionado.

Esse controlo pode ser exercido por diferentes formas:

a) directamente através de escolhas explícitas,
b) indirectamente, por exemplo através da definição de regras de acesso,
c) por procuração, ou seja, através da subcontratação de um nível de controlo a um terceiro confiável.

Para cada categoria, o utilizador pode definir o valor de um utilizador que representa o valor desta informação para a referida categoria. Para preencher esse valor podem ser aplicadas maneiras diferentes.

- O utilizador pode definir livremente o valor
- O sistema propõe valores pré-definidos, e o utilizador selecciona um
- O valor será adicionado automaticamente pelo sistema e simplesmente reconhecido pelo utilizador.

Vale a pena observar que o utilizador pode decidir não compartilhar uma categoria específica de seus dados pessoais.

De facto, quando uma categoria corresponde aos critérios de busca do terceiro, não é a categoria que é enviada de volta para o terceiro, mas a identificação do utilizador. Para uma determinada categoria, por exemplo, desporto, o utilizador também pode decidir que parte da sua identificação é enviada. Ele pode seleccionar um endereço de e-mail, um nome, um local, uma conta de Twitter ou Facebook, isto é, informações que podem ser usadas para permitir que o terceiro proponha serviços ou bens para o referido utilizador.

O método descrito acima pode ser utilizado num nível mais abstracto e de forma anónima. O terceiro poderia estar interessado apenas no número de acertos relativos a critérios de pesquisa específicos. Por exemplo, uma empresa, antes de abrir uma loja de desporto num lugar específico, pode solicitar ao centro de confiança, com a finalidade de obter o número de pessoas que são regulares em desporto numa zona geográfica perto da futura loja. Neste caso, o centro de confiança não envia de volta a identificação do utilizador.

Para este caso, cada uma das categorias dos dados pessoais pode ter, de facto, dois valores do utilizador, um para ter acesso à identificação do utilizador e outro para simplesmente participar nesta pesquisa anónima.

O resultado da pesquisa pode dar um grande número de acertos. É por isso que o presente método propõe algumas características de optimização. No caso em que o valor do utilizador pode ter um conteúdo diferente, isto é, para um utilizador, de 0,1 cento e outro utilizador, 0,2 cento, o centro de confiança organizará os dados transmitidos aos terceiros agrupando os utilizadores que tenham o mesmo valor. O centro de confiança apresenta a informação por quantidade, por exemplo, 1200 utilizadores em 0,1 porcento

e 2300 utilizadores em 0,2 porcento (dos utilizadores que satisfazem os critérios de pesquisa). Os terceiros podem então decidir refinar a pesquisa acrescentando critérios de pesquisa adicionais e executar novamente a solicitação para o centro de confiança ou podem aceitar o acordo proposto para o primeiro conjunto de utilizador.

Nos critérios de pesquisa enviadas pelo terceiro, este último pode incluir um valor limite. Este valor definirá quantos acertos serão retornados para os terceiros pelo centro de confiança. Este valor limite corresponde ao valor do utilizador acumulado até o valor limite ser atingido.

É do conhecimento geral que o interesse pelos dados pessoais é mais elevado, se os mesmos forem precisos. É por isso que o centro de confiança pode realizar várias verificações sobre os dados pessoais, com ou sem a ajuda do utilizador. O utilizador pode ter interesse que os seus dados sejam validados, permitindo, assim, um valor mais elevado para cada uma das categorias. A verificação incidirá sobre a idade, sexo, endereço e outros dados pessoais. É mais difícil verificar as preferências tais como a cor preferida, destino de férias etc.

Quando o perfil do utilizador é verificado pelo centro de confiança, o centro de confiança pode aumentar o valor do utilizador. Os terceiros também podem incluir nos critérios de pesquisa a possibilidade de aceder apenas aos utilizadores validados (e geralmente pagam mais) ou a totalidade dos utilizadores.

Na figura 2, a forma de realização ilustra o caso onde o centro de confiança TC desempenha o papel de um proxy. Os vários utilizadores UT1, UT2 primeiro conectam ao centro de confiança TC e a partir deste centro, têm acesso a sites de terceiros TPWS1, TPWS2. Neste caso, o utilizador

primeiro se conecta através do centro de confiança TC a um site de terceiros TPWS. Nessa altura, a funcionalidade do TC pode ser transparente e a identificação e autenticação do utilizador terão lugar numa fase posterior.

Noutra forma de realização, o proxy autentica o utilizador antes de aceder ao TPWS.

O TPWS em seguida solicita a identificação do utilizador e este pedido é passado para o TC. Este último pode verificar se os dados pessoais (todos ou parte) do utilizador são acessíveis a este TPWS. Em caso positivo, os dados pessoais são enviados de volta para o TPWS. Além disso, o utilizador pode ser identificado por um identificador único para o referido TPWS, este identificador sendo o mesmo cada vez que o utilizador se liga ao TPWS mas único para o referido TPWS.

Numa forma de realização particular da invenção, o sistema proporciona um nível diferenciado de controlo sobre os dados através de diferentes recursos de codificação aplicados sobre os dados. De acordo com uma primeira forma de execução da invenção, o utilizador, através do terminal UT do seu utilizador, conecta-se a um cento de confiança TC e carrega os seus dados pessoais, graças a uma comunicação segura entre o utilizador e o centro de confiança.

Como explicado acima, os dados pessoais são divididos em categorias e cada categoria é atribuída a determinados direitos de acesso. No direito de acesso, vários dados pode ser definidos tais como os terceiros permitidos a aceder a estes dados. Esta configuração pode ser na forma de uma lista de sites de terceiros (por exemplo, Facebook™, Twitter™, LinkedIn™) que o utilizador se une se os dados desta categoria fores acessíveis a este site de terceiros.

Os dados pessoais também poderiam ser imagens, textos ou filmes.

Além disso, é possível definir regras para a exploração dos dados pessoais, tais como a definição de uma compensação financeira no caso dos dados pessoais serem transferidos para terceiros. Para cada categoria de dados pessoais, uma quantidade particular pode ser definida.

O serviço de web de terceiros TPWS também pode se inscrever na base de dados confiáveis TDB. Um perfil pode ser definido, assim como uma descrição do tipo de actividade (por exemplo actividades desportivas, informação). Estes terceiros podem definir o tipo de utilizadores nos quais estão interessados tais como jovem do sexo masculino ou uma pessoa com animais de estimação.

Este serviço de web também pode definir a compensação de acesso aos dados pessoais do utilizador que correspondem às categorias de interesse por este serviço de web, esta compensação poderia ser associada a todo o registo do utilizador ou dividida por categoria de dados do utilizador.

Numa segunda etapa, o utilizador acede um site de terceiros TPWS e é convidado a identificar-se. A fim de obter os dados pessoais pelo site dos terceiros, este último inicia um link seguro com o centro de confiança e transmite a identidade do utilizador, bem como um identificador do site dos terceiros.

O centro de confiança, então, autenticará o utilizador através deste link e irá solicitará a credencial do utilizador. Isso pode ser na forma de uma palavra-passe ou com base numa operação mais segura envolvendo uma palavra-passe de uma só vez (utilizando um cartão pessoal que gera esta palavra-passe de uma só vez). Uma vez que o utilizador tenha sido autenticado, o centro de confiança

verifica as condições de acesso aos dados pessoais utilizando o identificador do site dos terceiros. Em vista desta verificação, os dados pessoais são (ou não são) retornados ao site dos terceiros.

O pedido para o centro de confiança também pode incluir informações do filtro. O site dos terceiros pode estar interessado em apenas uma parte dos dados pessoais (utilizando o descritor dos dados) ou também pode limitar o tipo do tamanho dos dados. No caso de que os dados pessoais compreenda um filme de 500 Mbytes, o site dos terceiros pode especificar o tamanho máximo dos dados solicitados. Em vez ou para além do tamanho, o site dos terceiros pode especificar o tipo de dados no qual está interessado, por exemplo, preferências, imagens, etc.

A fim de identificar o utilizador, os terceiros podem receber um identificador exclusivo do centro de confiança, por um lado sendo este identificador para identificar o utilizador, mas por outro lado sendo único para os terceiros. Neste caso, os terceiros recebem os dados pessoais do utilizador acedendo presentemente seus serviços sem conhecer a verdadeira identidade do utilizador. Durante o processo de autenticação, os terceiros também podem adicionar alguma(s) categoria(s) de interesse e transmiti-la(s) para o centro de confiança. Este último pode, então, verificar se o utilizador autenticado no momento coincide com a categoria identificada pelos terceiros e, em caso positivo, os dados pessoais do utilizador podem ser transmitidos aos terceiros. No caso em que uma compensação financeira foi definida pelo utilizador, e aceite pelos terceiros, um crédito é feito na conta do utilizador, sendo o crédito fornecido pelos terceiros. O contador do utilizador será então incrementado.

Como explicado acima, o centro de confiança pode desempenhar o papel de proxy. A base de dados central de confiança contém os dados pessoais e o proxy primeiro identifica o utilizador. Uma vez identificado, o centro de confiança pode supervisionar a comunicação entre o terminal do utilizador e um site. No caso em que o utilizador tenha bloqueado alguns dados pessoais, como o número de telefone, o centro de confiança pode alertar o utilizador no caso do número de telefone ser solicitado. Para o modo de proxy, o objectivo é capturar os dados pessoais que transitariam do utilizador para o site. É difícil bloquear um site que solicitaria dados pessoais, mas é fácil bloquear os dados que nós conhecemos (isto é, os dados fornecidos pelo utilizador para o centro de confiança). Neste modo o proxy atua como um dispositivo de DLP (*Data Loss Prevention*).

Numa versão mais leve, é possível carregar uma aplicação de software pequena no computador do utilizador para armazenar a identificação do seu utilizador no centro de confiança. Quando o utilizador acede a um serviço web de terceiros, tendo ele próprio uma conta com o centro de confiança, o utilizador pode autorizar esse terceiro o acesso aos seus dados pessoais (geralmente mediante compensação). Essa autorização pode ser na forma de clicar num logo do centro de confiança na página do terceiro. A fim de manter o anonimato do utilizador, os terceiros transmitem para a aplicação do utilizador um identificador (IDTP) dos terceiros. A aplicação do utilizador armazena o identificador do utilizador (IDU), uma chave pessoal (KUpr), a chave privada de um par de chaves assimétricas, e uma chave central de confiança (KTpu), a chave pública do centro de confiança.

A aplicação do utilizador gera dois criptogramas, o primeiro criptograma $(IDU)_{KTpu}$ é obtido pela codificação do identificador do utilizador IDU com a chave do centro de confiança KTpu e o segundo criptograma $(IDTP)_{KuPr}$ é obtido pela codificação do identificador dos terceiros IDTP pela chave pessoal KUpr. Deve ser observado que o segundo criptograma representa para os terceiros um identificador exclusivo que permite verificar se este utilizador já visitou estes terceiros. Em caso positivo, os dados recolhidos durante a visita anterior, bem como possíveis dados pessoais deste utilizador podem ser utilizados para personalizar a apresentação da oferta da web.

No caso em que o segundo criptograma é novo, isto significa que esse utilizador liga-se aos terceiros, pela primeira vez. Os terceiros podem aceder ao centro de confiança e podem transmitir o primeiro criptograma, bem como a sua própria identificação. O centro de confiança pode descodificar o primeiro criptograma, a fim de determinar a qual utilizador se refere. O centro de confiança pode retornar aos terceiros os dados pessoais do referido utilizador no caso que o utilizador tenha autorizado essa transmissão e as regras de compensação sejam cumpridas.

Em vez de chaves assimétricas, as chaves pessoais podem ser uma chave secreta simétrica.

De acordo com uma forma de realização da invenção, durante a inicialização dos dados pessoais com o centro de confiança, ou numa fase posterior, o utilizador pode receber material codificado na forma de um certificado electrónico ou um par de chaves assimétricas. Este material codificado é armazenado no dispositivo do utilizador, como laptop, smartphone, tablet. Este material é utilizado durante as etapas de autenticação realizadas

pelo site dos terceiros. Após o site dos terceiros ter iniciado a conexão com o centro de confiança, os dados trocados entre o utilizador e o centro de confiança são codificados usando este material criptográfico. Como consequência, o site dos terceiros não pode interferir no procedimento de autenticação e não consegue entender os dados trocados.

De acordo com uma outra forma de realização, um site de terceiros pode enviar um pedido para a obtenção de dados pessoais de utilizadores. Neste pedido, este site pode definir sua proposta em termos de compensação para aceder os dados pessoais, bem como os critérios de pesquisa. O centro de confiança, então, pesquisará através da sua base de dados para encontrar os dados do utilizador que correspondem aos critérios de pesquisa. Depois que um utilizador foi encontrado, o centro verifica se o link das condições de acesso a esses dados permitem a transmissão desses dados. Esta verificação pode levar em conta as condições gerais de acesso, tais como se essa categoria é acessível a terceiros ou se os terceiros estão explicitamente permitidos a aceder a esses dados.

Em ambos os casos, o utilizador pode definir critérios financeiros para ter acesso aos seus dados e o centro de confiança compara as expectativas do utilizador e a proposta dos terceiros. Se for encontrada uma correspondência, os dados pessoais do utilizador são transferidos para os terceiros e é creditada a compensação oferecida pelos terceiros.

Nesta forma de realização particular da invenção, o sistema fornece uma possibilidade para o utilizador de rentabilizar a comunicação, em condições pré-definidas, de alguns de seus dados pessoais a terceiros que estão prontos a compensá-lo para essa comunicação.

Estas condições pré-definidas podem incluir a permissão, ou uma negação de permissão para revender dados pessoais a terceiros sujeitos aos níveis de controlo acima mencionados.

Para implementar o método da invenção, o centro de confiança tem capacidades de processamento e de armazenagem, bem como meios de telecomunicações. O centro de confiança é de preferência ligado à Internet de modo que os utilizadores possam anunciar seus dados pessoais. As capacidades de processamento são responsáveis por proteger os dados pessoais, organizando-os e realizando a busca solicitada pelos terceiros.

Lisboa,

REIVINDICAÇÕES

1. Método para controlar o acesso de dados pessoais de um utilizador (UT1, UT2) por um centro de confiança (TC) que compreende pelo menos uma base de dados (TDB) compreendida por um utilizador específico, locais de memória para dados pessoais, condições de acesso associadas aos dados pessoais, e dados de gestão,
   - carregar, por um utilizador os seus dados pessoais na base de dados (TDB) do centro de confiança (TC) e atribuir condições de acesso aos referidos dados, os referidos dados pessoais sendo divididos em pelo menos duas categorias com duas condições de acesso diferentes, cada categoria sendo associada com um valor do utilizador,
   - pedir acesso ao centro a confiança (TC) por um terceiro (TPWS) aos dados pessoais de uma pluralidade de utilizadores (UT), o referido pedido compreendendo critérios de busca,

   caracterizado por, os dados de gestão compreenderem ainda pelo menos um contador,

   e no caso em que os terceiros não tenham indicado um valor de terceiros:
   - executar pelo centro de confiança (TC) os critérios de busca nos dados pessoais dos utilizadores de modo a determinar um primeiro conjunto de utilizadores que corresponda aos critérios de busca,
   - retornar aos terceiros (TPWS) a informação que mostra a quantidade do primeiro conjunto de utilizadores que corresponde aos critérios, bem como a soma do valor do utilizador de cada utilizador do primeiro conjunto,
   - reconhecer toda ou parte da soma pelos terceiros, definindo assim um segundo conjunto de utilizadores

que pode compreender a totalidade ou parte do primeiro conjunto,

- retornar os dados pessoais do segundo conjunto de utilizador para o qual a soma cobre os valores acumulados dos utilizadores extraídos,

ou então:

- o referido pedido compreende ainda o valor dos terceiros,
- executar pelo centro de confiança (TC) os critérios de pesquisa nos dados pessoais dos utilizadores de modo a determinar um segundo conjunto de utilizadores que corresponda os critérios de busca para os quais o valor do utilizador é igual ou mais baixo do que o valor dos terceiros,
- retornar os dados pessoais do segundo conjunto de utilizadores,

  e
- actualizar o contador do segundo conjunto de utilizadores com o conteúdo do valor dos seus respectivos dados pessoais.

2. Método de acordo com a reivindicação 1, caracterizado por a informação que mostra a quantidade do primeiro conjunto de utilizadores corresponder aos critérios que compreendem a etapa de:
   - agrupar todos os utilizadores do primeiro conjunto de utilizadores que têm o mesmo valor de utilizador,
   - transmitir aos terceiros (TPWS), a quantidade de utilizadores por grupo.
3. Método de acordo com a reivindicação 1, caracterizado por os terceiros (TPWS) transmitirem um valor limite com o seu pedido e por outro conjunto de utilizadores ser seleccionado entre o segundo conjunto de utilizadores de modo que a soma do valor do utilizador

de cada utilizador do outro conjunto não exceda o valor limite.

4. Método de acordo com qualquer das reivindicações 1 a 3, caracterizado por o pedido pelos terceiros (TPWS) compreender os dados de filtragem, a etapa de transmitir os dados pessoais compreender uma etapa de filtrar dos dados pessoais de acordo com os dados de filtragem antes de os transmitir para o site dos terceiros.

5. Método de acordo com qualquer das reivindicações 1 a 4, caracterizado por compreender as etapas de:
   - verificar pelo menos uma parte dos dados pessoais,
   - atribuir um valor de utilizador diferente se os dados pessoais tiverem sido verificados com sucesso.

Lisboa,

RESUMO

"MÉTODO PARA CONTROLAR O ACESSO DE DADOS PESSOAIS DE UM UTILIZADOR"

Há uma necessidade de sistema e método que sejam concebidos para dar controlo pleno e contínuo, ganhar a confiança do indivíduo médio, encorajando tal indivíduo para se tornar um utilizador aberto e confiante de tal sistema. É proposto um método para controlar o acesso de dados pessoais de um utilizador por um centro de confiança que compreende pelo menos uma base de dados que inclui, para um utilizador específico, locais de memória para dados pessoais, condições de acesso associadas aos dados pessoais e dados de gestão que compreendem pelo menos um contador, - carregar, por um utilizador os seus dados pessoais na base de dados do centro de confiança e atribuir condições de acesso aos referidos dados, os referidos dados pessoais sendo divididos em pelo menos duas categorias com duas condições de acesso diferentes, cada categoria sendo associada com um valor do utilizador, - pedir acesso ao centro a confiança por um terceiro aos dados pessoais de uma pluralidade de utilizadores, o referido pedido compreendendo critérios de busca, - executar pelo centro de confiança os critérios de busca nos dados pessoais dos utilizadores de modo a determinar um primeiro conjunto de utilizadores que corresponda aos critérios de busca, - retornar aos terceiros a informação que mostra a quantidade do primeiro conjunto de utilizadores que corresponde aos critérios, bem como a soma do valor do utilizador de cada utilizador do primeiro conjunto, - reconhecer toda ou parte da soma pelos terceiros, definindo assim um segundo conjunto de utilizadores que pode compreender a totalidade ou parte do primeiro conjunto, - retornar os dados pessoais do segundo

conjunto de utilizador para o qual a soma cobre os valores acumulados dos utilizadores extraídos, - actualizar o contador do segundo conjunto de utilizadores com o conteúdo do valor dos seus respectivos dados pessoais.

FIGURAS

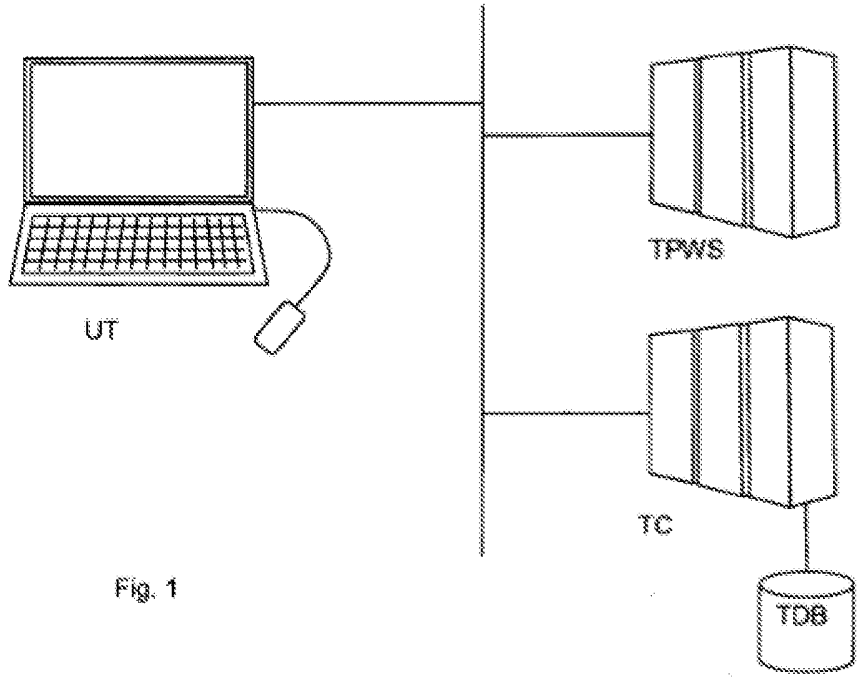

Fig. 1

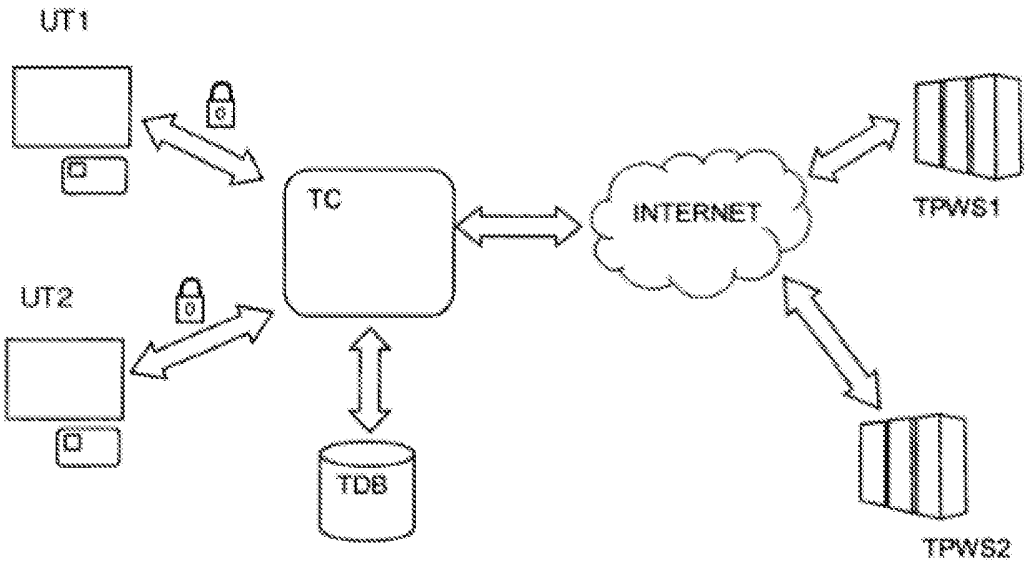

Fig. 2