

República Federativa do Brasil  
Ministério do Desenvolvimento, Indústria  
e do Comércio Exterior  
Instituto Nacional da Propriedade Industrial

(21) **PI0610325-1 A2**



\* B R P I 0 6 1 0 3 2 5 A 2 \*

(22) Data de Depósito: 30/03/2006

(43) Data da Publicação: 15/06/2010  
(RPI 2058)

(51) *Int.Cl.:*

H04N 7/167

(54) Título: **JARDINS MURADOS.**

(30) Prioridade Unionista: 28/04/2005 US 11/116.925

(73) Titular(es): MICROSOFT CORPORATION

(72) Inventor(es): LILI CHENG, RICHARD L. HUGHES, RYSZARD  
K. KOTT, SEAN U. KELLY, WILLIAM L. PORTNOY

(74) Procurador(es): ALEXANDRE FERREIRA

(86) Pedido Internacional: PCT US2006011938 de 30/03/2006

(87) Publicação Internacional: WO 2006/115692 de 02/11/2006

(57) **Resumo:** A presente invenção provê um sistema e método único que facilitam um ambiente de comunicação controlada, permitindo a um usuário participar de uma pluralidade de contextos de privacidade com outras pessoas de uma maneira simultânea. Um usuário poderá atribuir ou definir níveis de privacidade à sua informação, de modo a controlar a visibilidade de tais informações por parte de outras pessoas. Em particular, um primeiro usuário poderá manter um ou mais "jardins" de conteúdo que podem ser acessíveis a pelo menos um subconjunto da comunidade em linha. O acesso aos conteúdos de qualquer um jardim poderá se basear no nível de privacidade do jardim e no nível de privacidade (por exemplo, os parâmetros de acesso) concedidos à pessoa. Os níveis de privacidade e a disposição do conteúdo podem ser hierárquicos e/ou não sobrepostos. Deste modo, um usuário poderá se comunicar com múltiplos usuários ao mesmo tempo, sem restrições, independente do seu contexto ou nível de privacidade, ao mesmo tempo mantendo os limites de privacidade de cada jardim.



**PI0610325-1**

"JARDINS MURADOS"

CAMPO DA INVENÇÃO

A presente invenção refere-se, de modo geral, a redes de informação e, em particular, a sistemas e métodos  
5 que provêm aos usuários um ambiente de comunicação controlada, incluindo vários níveis de privacidade e/ou segurança que permitem ao usuário se comunicar com outros usuários nestes vários níveis de privacidade ou segurança ao mesmo tempo.

10 FUNDAMENTOS DA INVENÇÃO

Um dos canais mais eficazes para disseminar e obter informações é através de relações diretas ou pessoais referidas como rede social. Uma rede social consiste de pessoas e suas relações pessoais com outras pessoas, através do  
15 que informações e oportunidades são trocadas. A relação direta, pessoal implica no fato de duas pessoas "se conhecerem" e de tipicamente possuírem uma certa quantidade de confiança mútua. Uma pessoa pode ter mais de uma ou diversas redes sociais diferentes, o que é similar a uma pessoa ter  
20 diferentes grupos de amigos (por exemplo, amigos familiares, amigos de trabalho, amigos de escola, amigos de festas, etc.).

O valor de uma rede social pode ser demonstrado, por exemplo, pelo fenômeno dos "seis graus de separação", o que significa que a distância entre quaisquer duas pessoas  
25 em termos de relações diretas pessoais é relativamente pequena (por exemplo, de 6 graus ou menos). As redes sociais são freqüentemente empregadas por pessoas, muitas vezes, sem uma idéia consciente. Por exemplo, uma pessoa pode estar

pesquisando um trabalho e contata seus amigos a fim de determinar se os mesmos sabem de cargos disponíveis. Esses amigos são capazes de prover informações confiáveis sobre cargos dos quais diretamente têm conhecimento. Esses amigos  
5 podem também recomendar cargos disponíveis ao amigo que está procurando trabalho. Além disso, essas relações diretas pessoais podem ser empregadas para se obter informações sociais e/ou oportunidades, tais como, informações sobre parceiros românticos possíveis, bons filmes, restaurantes, e/ou a compra, a venda, ou a troca de artigos ou serviços.  
10

As relações diretas pessoais são particularmente úteis na obtenção de informações e oportunidades, tendo em vista a confiabilidade das informações associada e as pessoas envolvidas. Por exemplo, uma pessoa tipicamente ficará,  
15 com frequência, mais à vontade para intercambiar uma casa de veraneio (intercâmbio de casa) com o amigo de um amigo, mesmo que ela não conheça pessoalmente o amigo do amigo, do que fazer o intercâmbio da casa com um estranho. Um base para tal confiança é que a pessoa pode confiar no fato de que seu  
20 amigo imediato não se ligaria a uma pessoa que oferece um intercâmbio de casa (por exemplo, o amigo de um amigo) se este amigo do amigo não fosse confiável ou digno de confiança. De modo geral, pode se ter confiança no amigo imediato no sentido de que este oferece uma avaliação honesta da  
25 confiança com relação à terceira parte. As redes sociais com frequência se baseiam em informações baseadas em opiniões, como, por exemplo, sobre filmes, restaurantes, locais para viagem, ou coisa do gênero. Estas informações compartilhadas

entre um grande número de pessoas em geral são tipicamente mais confiáveis que nas palavras de uma crítica profissional.

No contexto de uma rede social em linha, permanece o problema da manutenção, do controle, e da regulação do usuário com relação aos recursos limitados do sistema e ao comportamento do usuário.

### SUMÁRIO DA INVENÇÃO

A seguir apresenta-se um sumário simplificado da presente invenção a fim de prover um entendimento básico de alguns aspectos da presente invenção. Este sumário não vem a ser um resumo introdutório extensivo da presente invenção. Não se pretende identificar os elementos chaves / críticos da presente invenção ou delinear o âmbito da presente invenção. O seu único propósito é apresentar alguns conceitos, de uma forma simplificada, como uma introdução à descrição mais detalhada que será apresentada mais adiante.

A presente invenção se refere a um sistema e/ou metodologia que facilitam um ambiente de comunicação controlada que permita a um usuário interagir com outros usuários de uma comunicação em linha em diferentes níveis de privacidade, de uma maneira simultânea. O sistema e método permitem a um usuário atribuir ou definir níveis variados de privacidade a sua informação ou conteúdo a fim de controlar a visibilidade e o acesso de tais informações por parte de outras pessoas. Em particular, um primeiro usuário poderá manter um ou mais "jardins" ou armazenadores de conteúdo que poderão se tornar acessíveis ou visualizáveis a pelo menos um subconjunto de comunidade. O acesso aos conteúdos de qualquer

um jardim poderá se basear no nível de privacidade (por exemplo, parâmetros de acesso) concedido a uma outra pessoa que se registra na comunidade. Os níveis de privacidade podem variar desde público (por exemplo, não privativo) a completamente privativo (por exemplo, nenhum acesso permitido a outros usuários) com graus de privacidade dispersados entre os mesmos. Essencialmente, um usuário poderá se comunicar sem restrição com múltiplos usuários ao mesmo tempo independente de seu contexto ou nível de privacidade, embora mantendo controle sobre os limites de privacidade de cada jardim.

Os sistemas de comunicação convencionais que permitem algum tipo de troca de informação entre usuários requerem que o usuário (por exemplo, o proprietário do conteúdo) se movimente entre um contexto público ou privativo (por exemplo, similar aos modos de comutação) baseado no contexto do outro usuário (por exemplo, a pessoa que busca acesso ao conteúdo). Isto pode, muitas vezes, causar confusão ao usuário, assim como também muitos outros problemas de comunicação e segurança. Outros sistemas de comunicação convencionais apenas oferecem um ambiente totalmente público ou um ambiente totalmente seguro, em que, nos dois casos, os usuários têm acesso a todas as informações do sistema ou de uma maneira não restrita ou de uma maneira segura, respectivamente. Diferentemente estes sistemas convencionais, a presente invenção facilita a comunicação simultânea em ambos os contextos público ou privado, os quais ficam efetivamente transparentes para as partes que se comunicam.

Por exemplo, um primeiro usuário poderá postar um

grupo de fotos, designando algumas públicas e outras privadas. Um segundo usuário com direitos de acesso apenas público poderá visualizar as fotos públicas, mas não vê ou sabe a respeito das fotos privadas. Ao mesmo tempo, um terceiro usuário com direitos de acesso privativo poderá visualizar as fotos privadas e conversar com o primeiro usuário sobre estas fotos privadas.

Diferentes abordagens podem ser empregadas para que isto venha ocorrer. Em uma abordagem, isto pode ser feito em parte ao inicialmente determinar os direitos de acesso, caso algum, das segunda e terceira pessoas. Quando os direitos de acesso são reconhecidos, o segundo e terceiro usuários poderão receber o respectivo conteúdo disponível para cada um. Quando não são encontrados direitos de acesso, apenas o acesso público ou apenas o conteúdo público poderá se tornar disponível para aquela pessoa. De maneira alternativa, nenhum acesso poderá ser oferecido quando não são encontrados direitos de acesso. Em uma outra abordagem, o sistema poderá automaticamente colocar o segundo e terceiro usuários "em" seus respectivos jardins por meio da identificação de seus direitos de acesso de acordo com as suas informações de identificação. Nesta abordagem, o acesso à comunidade poderá automaticamente conceder acesso ao segundo ou ao terceiro usuário a pelo menos o conteúdo público e, deste modo, colocar o usuário apropriado em seu jardim apropriado após identificação.

O acesso a qualquer jardim ou armazenador em particular poderá prover ao usuário a capacidade de blogar ou

postar mensagens, fotos, e/ou outro conteúdo dentro daquele jardim. Além disso, o usuário poderá visualizar o conteúdo de outros usuários postado naquele jardim e/ou adicionar comentários ou anotações sobre o conteúdo postado ou publicado por outros usuários dentro daquele jardim.

De acordo com um aspecto da presente invenção, os jardins ou armazenadores podem ser acessíveis a partir de uma rede pública, como, por exemplo, a Rede Mundial (World Wide Web), ou a partir de uma rede privada para um conjunto mais discreto de usuários. Por conseguinte, a comunidade de usuários pode ser o público em geral ou um grupo mais específico de usuários, como, por exemplo, um grupo social de pessoas, os empregados de uma empresa, ou os alunos de uma universidade.

De acordo com um outro aspecto da presente invenção, os jardins ou armazenadores de conteúdo podem ser organizados de uma maneira hierárquica, assim como de uma maneira não sobreposta. Sendo assim, os direitos de acesso se sobrepõem ao mutuamente excluem o acesso a outros jardins com níveis mais baixos de privacidade. Além disso, um usuário pode ser "localizado" em vários jardins diferentes e se comunicar a partir dos mesmos ao mesmo tempo. Deste modo, a apresentação do conteúdo de cada jardim ao usuário dependerá de que jardim está se considerando naquele momento. Ou seja, o conteúdo apresentado ao usuário poderá depender dos diversos jardins diferentes.

Para a realização dos fins acima e de fins relacionados, certos aspectos ilustrativos da presente invenção

serão descritos no presente documento com relação à descrição e aos desenhos em anexo. Estes aspectos são indicativos, contudo, de apenas algumas dentre as diversas maneiras nas quais os princípios da presente invenção podem ser empregados, e a presente invenção pretende incluir todos estes aspectos e seus equivalentes. Outras vantagens e aspectos novos da presente invenção poderão se tornar aparentes a partir da descrição detalhada a seguir da presente invenção, quando considerados em conjunto com os desenhos.

10                    BREVE DESCRIÇÃO DOS DESENHOS

A Figura 1 é um diagrama em blocos de alto nível de um sistema de comunicação controlada que facilita a comunicação simultânea em ambos os contextos privado ou público de acordo com um aspecto da presente invenção.

15                    A Figura 2 é um diagrama em blocos de um sistema de comunicação controlada que facilita a comunicação simultânea entre um usuário e outras pessoas em ambos os contextos privado ou público de acordo com um aspecto da presente invenção.

20                    A Figura 3 é um diagrama em blocos de um sistema de comunicação automatizado controlado que automaticamente propõe ou atribui um novo nível de privacidade a uma pessoa que se comunica com um usuário baseado nas comunicações e/ou ações do usuário de acordo com um aspecto da presente invenção.

25

A Figura 4 é uma diagrama em blocos demonstrando a interação simultânea em ambos os contextos público e privado de acordo com um aspecto da presente invenção.

A Figura 5 é um diagrama esquemático de uma disposição de grupo / nível de privacidade exemplar de acordo com um aspecto da presente invenção.

5 A Figura 6 é um diagrama esquemático de uma disposição de grupo / nível de privacidade exemplar de acordo com um aspecto da presente invenção.

A Figura 7 é um diagrama em blocos de um subsistema que opera cooperativamente com os sistemas da Figura 1 ou da Figura 2 que facilita a resolução da imagem de conteúdo para uma pessoa com acesso a múltiplos grupos de privacidade.

A Figura 8 é um fluxograma ilustrando uma metodologia exemplar que facilita a comunicação simultânea em múltiplos contextos de privacidade de acordo com um aspecto da presente invenção.

15 A Figura 9 é um fluxograma ilustrando uma metodologia exemplar que facilita a comunicação simultânea em ambos os contextos privado e público (não privado) de acordo com um aspecto da presente invenção.

A Figura 10 é um fluxograma ilustrando uma metodologia exemplar que facilita as propostas ou atribuições automáticas de um novo nível de privacidade a uma pessoa que se comunica com um usuário baseado nas comunicações e/ou ações do usuário de acordo com um aspecto da presente invenção.

25 A Figura 11 é um fluxograma ilustrando uma metodologia exemplar que facilita a interação entre uma pessoa e o jardim de um usuário de acordo com um aspecto da presente invenção.

A Figura 12 é um fluxograma ilustrando uma metodo-

logia exemplar que facilita a interação de uma pessoa com o jardim de um usuário de acordo com um aspecto da presente invenção.

A Figura 13 ilustra uma me para a implementação de  
5 vários aspectos da presente invenção.

#### DESCRIÇÃO DETALHADA DA INVENÇÃO

A presente invenção é agora descrita com referência aos desenhos, nos quais numerais de referência similares são usados para se referir a elementos similares em todas as  
10 figuras. Na descrição a seguir, para fins de explicação, são apresentados inúmeros detalhes específicos a fim de prover um entendimento geral da presente invenção. Pode ficar evidente, no entanto, que a presente invenção pode ser praticada sem estes detalhes específicos. Em outras instâncias, estruturas e dispositivos bem conhecidos são mostrados em forma de diagramas em blocos a fim de facilitar a descrição da  
15 presente invenção.

Conforme usado neste pedido, os termos "componente" e "sistema" pretendem se referir a uma entidade relacionada a computadores, quer ao hardware, a uma combinação de  
20 hardware e software, ao software, ou ao software em execução. Por exemplo, um componente pode ser, porém não se limita a ser, um processo executado em um processador, um processador, um objeto, um executável, um fio de execução, um  
25 programa, ou um computador. A guisa de ilustração, tanto uma aplicação que é executada em um servidor, como o servidor podem ser um componente. Um ou mais componentes pode residir dentro de um processo e/ou fio de execução, ou um componente

pode se localizar em um computador e/ou ser distribuído entre dois ou mais computadores.

A presente invenção pode incorporar vários esquemas e/ou técnicas de inferência com relação à concessão ou à  
5 provisão automática de direitos de acesso adicionais a um conteúdo protegido de um usuário, baseadas pelo menos em parte nas ações ou comunicações do usuário com uma outra pessoa (para a qual os direitos de acesso podem ser concedidos). Além disso, tais esquemas de inferência podem ser em-  
10 pregados em parte para se determinar que conteúdo exibir para uma pessoa que se comunica com o proprietário do conteúdo (usuário) - especialmente nos casos em que a pessoa tem direitos de acesso a múltiplos grupos de conteúdo, mas nem todos os grupos podem ser acessados imediatamente pela pessoa.  
15 Outros cenários, embora não apresentados aqui, podem também fazer uso de um ou mais esquemas de inferência a fim de executar a presente invenção, sendo estes contemplados como dentro do âmbito da presente invenção.

Conforme usado no presente documento, o termo "inferência" refere-se, de modo geral, ao processo de racionalizar sobre ou inferir estados do sistema, ambiente, e/ou  
20 usuário a partir de um conjunto de observações conforme capturadas através de eventos e/ou dados. A inferência pode ser empregada no sentido de identificar um contexto ou ação específica, ou pode gerar uma distribuição de probabilidade sobre estados, por exemplo. A inferência pode ser probabilística - ou seja, a computação de uma distribuição de probabilidades sobre estados de interesse baseada na considera-  
25

ção de dados e eventos. A inferência pode também se referir às técnicas empregadas para a composição de eventos de nível mais alto a partir de um conjunto de eventos e/ou dados. Estes resultados de inferência na construção de novos eventos ou ações a partir de um conjunto de eventos observados e/ou dados de eventos armazenados, quer os eventos estejam correlacionados em uma proximidade temporal estrita ou não, ou quer os eventos ou os dados venham de um evento ou fonte de dados ou de diversos eventos ou fontes de dados.

10           Em toda a descrição da presente invenção, os termos "usuário" e "pessoa" são empregados para distinguir entre as partes envolvidas. Em particular, o termo "usuário" de modo geral se refere a um proprietário ou co-proprietário do conteúdo ou grupo de conteúdos que se encontra potencialmente acessível por parte de outras pessoas através de uma comunidade em linha (por exemplo, a Rede mundial, uma rede empresarial, uma rede escolar, etc.). Cada grupo de conteúdo pode também ser referido como "jardim".

20           O termo "pessoa" de modo geral se refere a qualquer outro usuário que tem acesso à comunicação em linha e que pode potencialmente interagir com qualquer proprietário ou co-proprietário de um jardim, assim como com o próprio jardim dependendo dos direitos de acesso ou nível de privacidade concedidos ao mesmo. Cada jardim ou grupo de jardins pode também ser atribuído a um nível de privacidade. Quando o nível de privacidade de um jardim é "atendido" pelo ou corresponde ao nível de privacidade de uma pessoa, essa pessoa então terá acesso àquele jardim em particular. Em geral,

o acesso pode ser mínimo, como, por exemplo, uma visualização passiva do conteúdo de um jardim ou de pelo menos uma porção do mesmo. O acesso à ou a capacidade de visualizar qualquer jardim em particular ou pedaço de conteúdo pode ser submetido a uma ou mais regras de apresentação, conforme determinado pelo usuário para o jardim em particular ou pedaço de conteúdo.

Com referência agora à Figura 1, é mostrado um diagrama em blocos geral de um sistema de comunicação controlada 100 que provê um ambiente de comunicação no qual as informações incluídas no mesmo podem ser tanto públicas como privadas dependendo das preferências do usuário. O sistema 100 inclui um componente de análise de dados 110 que recebe e examina a entrada de acesso, como, por exemplo, os dados de login (identificação) de uma pessoa (por exemplo, nome de usuário, senha, etc.), assim como qualquer informação derivada dos mesmos. O componente de análise de dados 110 pode determinar a identidade da pessoa, assim como reconhecer as capacidades de acesso concedidas à pessoa enquanto "no" ambiente de comunicação.

A informação determinada pelo componente de análise de dados 110 pode ser comunicada ao componente de controle de contexto 120. O componente de controle de contexto 120 pode regular a interação entre os proprietários / coproprietários (usuários) do jardim e pelo menos uma pessoa correntemente "no" ambiente de comunicação. Por exemplo, imagine que um usuário tenha um conteúdo público (ou seja, não privado) e um conteúdo privado, ambos mantidos em pelo

menos dois grupos respectivos: em um grupo público e em um grupo privado. Uma pessoa A recebe direitos de acesso mínimos e, deste modo, só pode acessar o grupo público, enquanto a Pessoa B recebe um grau maior de direitos de acesso e, assim, pode ter acesso ao grupo privado. A fim de manter estes limites entre os grupos de conteúdo, limites similares podem ser empregados ao se comunicar sobre tal conteúdo com o proprietário do conteúdo. Deste modo, a comunicação pode estar em um contexto público ao lidar com o grupo público ou qualquer pessoa associada ao mesmo. De maneira similar, o proprietário do contexto ou qualquer pessoa associada ao grupo privado poderá interagir em um contexto privado.

O componente de controle de contexto 120 pode gerenciar e controlar a interação entre o usuário (ou o conteúdo do usuário) e as respectivas pessoas de modo que o contexto de privacidade (por exemplo, o contexto público, o contexto privado, o contexto muito privado, etc.) seja preservado para cada pessoa apesar da interação simultânea em ambos os contextos público e privado. Além disso, as operações do componente de controle de contexto 120 são transparentes ao usuário, assim como às pessoas que interagem com o usuário. Sendo assim, esta pessoa não poderá ficar ciente de nenhum outro grupo ao qual ela não tem acesso e o usuário não precisará se preocupar em ficar confuso sobre qual pessoa pode ver aquele conteúdo.

Além disso, um componente de comunicação de múltiplos contextos 130 facilita a interação e/ou a comunicação do usuário em uma pluralidade de contextos de uma maneira

simultânea sem precisar que o usuário (o proprietário do conteúdo) comute entre modos de privacidade para cada um dos diferentes níveis de privacidade ao qual cada pessoa pode estar atribuída. Além disso, o usuário pode se comunicar livremente com uma pluralidade de pessoas de diferentes níveis de privacidade, que são privativas para diferentes conteúdos, sem se preocupar sobre quão seguro o ambiente é ou precisa ser antes de uma comunicação poder começar com uma determinada pessoa.

10 Com referência agora à Figura 2, é ilustrado um diagrama em blocos de um sistema de comunicação controlada 200 que facilita o estabelecimento de jardins ou grupos de conteúdos, e o controle de acesso para tais conteúdos de acordo com um aspecto da presente invenção. A fim de estabelecer vários níveis de proteção para o conteúdo do usuário, 15 o sistema 200 inclui um componente de organização de conteúdo 210 que pode organizar o conteúdo do usuário em um ou mais bancos de dados (ARMAZENADOR DE CONTEÚDO<sub>1</sub> 220) e/ou até o ARMAZENADOR DE CONTEÚDO<sub>M</sub> 230), em que M é um inteiro maior 20 que ou igual a um). Cada banco de dados pode ser referido como um jardim, por meio do que cada jardim pode ser atribuído a um nível de privacidade através de um componente de atribuição de privacidade 240. O conteúdo do usuário pode ser armazenado de acordo com o nível de privacidade desejado 25 pelo usuário para cada pedaço ou tipo de conteúdo. No entanto, deve-se apreciar que o conteúdo do usuário não precisa ser organizado em armazenadores de conteúdo fisicamente separados, uma vez que a distinção dos grupos de conteúdos po-

de estar em um nível lógico. Além disso, o conteúdo pode ser atribuído à sobreposição dos armazenadores de conteúdo, tal como quando os grupos de privacidade se sobrepõem.

Usando um delineamento similar dos níveis de privacidade, o componente de atribuição de privacidade 240 pode também atribuir níveis de privacidade aos contatos do usuário ou a qualquer pessoa na rede social do usuário. Uma vez que o usuário poderá não conhecer ou ser capaz de identificar cada pessoa pelo nome na comunidade em linha, qualquer pessoa sem um nível de privacidade atribuído poderá receber o nível de privacidade mínimo (por exemplo, somente direitos de acesso público) por padrão.

Quando os jardins são estabelecidos, pelo menos uma porção do conteúdo pode se tornar disponível para outras pessoas registradas na comunicação em linha. No entanto, antes de qualquer conteúdo ser exibido, um componente de identificação de privacidade 250 poderá identificar a pessoa que deseja tal acesso a fim de determinar o seu nível de privacidade. Depois de isto ser determinado, o componente de exibição de conteúdo 260 exibirá o conteúdo apropriado ou permitirá o acesso da pessoa a tal conteúdo. Ou seja, pelo menos um jardim se torna visível à pessoa com base no nível de privacidade atribuído ao jardim e à pessoa. Quando nenhum nível de privacidade é atribuído à pessoa, um jardim considerado adequado para uma visualização pública poderá ser exibido. A seguir, um componente de comunicação de usuário-a-pessoa 270 poderá ser empregado a fim de facilitar as comunicações entre o usuário e a pessoa associados ao jardim em

particular no vídeo. Como um resultado, o usuário não precisa adivinhar a que conteúdo a pessoa está se referindo em sua comunicação e poderá prontamente se comunicar com mais de uma pessoa de uma vez só, independente do nível de privacidade envolvido. Exemplos de comunicações incluem, porém não se limitam a, blogs, bate-papos, troca de mensagens instantâneas, troca de e-mails, e/ou conversa.

Voltando agora para a Figura 3, é mostrado um diagrama em blocos de um sistema de comunicação controlada automatizado 300 de acordo com um aspecto da presente invenção. Em particular, o sistema 300 pode ser empregado de modo a determinar ou ajustar automaticamente o nível de privacidade de um jardim ou de qualquer conteúdo, em geral, baseado pelo menos em parte nas ações do usuário. De maneira similar, o sistema 300 pode automaticamente permitir às pessoas acessarem um determinado jardim pertencente ou co-pertencente ao usuário com base pelo menos em parte nas ações do usuário que envolvem ou as comunicações que são trocadas com tais pessoas.

A fim de realizar o acima apresentado, o sistema automatizado 300 inclui um componente de monitor 310 que pode observar e coletar as comunicações de usuário-a-pessoa 320, tais como comentários ou mensagens trocadas entre o usuário e a pessoa (ou pessoas) em questão. Por exemplo, suponha que o usuário mencione à George, um amigo de um amigo e colecionador de arte, que ele é também um colecionador de arte e que recentemente comprou alguns quadros de uma liquidação. O usuário pode continuar, mencionando os nomes do ar-

tista e do quadro nas trocas subseqüentes com George. O componente do monitor 310 pode comunicar tais informações para um componente de análise 330. O componente de análise 330 pode consumir e processar estas informações e reconhecer que  
5 o usuário previamente estabeleceu um jardim (por exemplo, um jardim de pinturas), incluindo fotos de quadros (baseado na organização de jardim 340) e que George não tem acesso ao mesmo naquele momento (de acordo com o banco de atribuição de privacidade 330). Um componente de inteligência artificial (AI) 360 pode ser treinado para automaticamente sugerir  
10 ou atribuir a pessoas como George direito de acesso apropriado a fim de obter acesso a este jardim particular. De maneira alternativa ou em adição, o componente AI 360 pode propor ou atribuir a George um nível de privacidade apropriado que possa prover ao mesmo acesso ao jardim apropriado,  
15 assim como a outros jardins com o mesmo nível de privacidade.

De maneira similar, as ações dos usuários 370 podem ser também monitoradas. Estas ações podem incluir atribuições de privacidade previamente feitas a outros conteúdos  
20 (por exemplo, um conteúdo relacionado) ou a outras pessoas que possam pertencer à mesma rede social, lista de distribuição, ou lista de contato como a pessoa em questão. Por exemplo, George pode ser incluído ou adicionado à mesma lista de distribuição que Paul. O usuário já pôde ter dado a Paul  
25 um nível de privacidade que permita a Paul acessar um grupo de seleção de jardins. Deste modo, o componente AI 360 pode aprender a também atribuir a George ou a qualquer outra pessoa adicionada à lista de distribuição um nível de privaci-

dade similar (ou igual). Uma vez que algumas pessoas podem estar incluídas em mais de uma lista de distribuição ou ser atribuídas a vários direitos de acesso e níveis de privacidade, uma lista de distribuição ou qualquer outra lista pode  
5 ser atribuída a um nível particular de privacidade. Sendo assim, quando uma pessoa nova é adicionada à lista, esta pessoa pode ser atribuída ao nível de privacidade da lista - ao invés de ao nível de privacidade de outra pessoa na lista. Isto pode ser importante, uma vez que pelo menos uma  
10 pessoa em qualquer lista pode ter sido atribuída a níveis de privacidade adicionais.

O usuário pode treinar o componente AI 360 de acordo com as suas preferências. Outros exemplos de ações de usuário 370 incluem, porém não se limitam a, mudanças na rede social do usuário às quais os jardins são associados e  
15 mudanças nas restrições de nível de privacidade de pelo menos um subconjunto dos jardins.

Indo para a Figura 4, é ilustrado um diagrama esquemático que demonstra um ambiente de comunicação controlada 400 de acordo com um aspecto da presente invenção. O ambiente 400 inclui os itens de conteúdo ou os itens armazenados do usuário 410, os quais podem ser ainda agrupados de acordo com o tipo de conteúdo, assunto, etc., conforme desejado pelo usuário. Cada grupo pode, em seguida, ser atribuído a um nível de privacidade por parte do usuário. Por exemplo,  
20 um grupo pode ser considerado itens públicos 420 que podem ser acessíveis por todos os demais na comunidade. De maneira alternativa, o usuário pode marcar uma mensagem, uma

conversação, ou qualquer outro objeto com um nível de privacidade conforme surge (por exemplo, "on the fly" ("instantâneo")). Por exemplo, o usuário pode estar "batendo papo" com uma pessoa e decidir naquele momento que a conversa é ou se  
 5 tornou muito privativa e marcar a mesma com um nível de privacidade apropriado. Sendo assim, o conteúdo pode receber um nível de privacidade em uma base por item ou como um grupo.

Além disso, estes itens públicos 420 pode ser visualizáveis (por exemplo, uma visualização passiva) por parte de outras pessoas fora da comunidade, conforme determinado pelo usuário. Por exemplo, se a comunidade for definida como uma rede escolar constituída apenas de alunos e funcionários de uma escola, os itens públicos 420 ou uma porção dos mesmos podem se tornar disponíveis para uma visualização  
 10 passiva por aqueles fora da comunidade escolar.

Os outros grupos de conteúdo do usuário podem ser caracterizados por graus variados de privacidade, como, por exemplo, os ITENS PRIVATIVOS<sub>1</sub> 430, aos quais visualizadores selecionados podem acessar, e os ITENS PRIVATIVOS<sub>2</sub> 440, aos  
 20 quais um subconjunto dos visualizadores selecionados ou outros visualizadores selecionados podem acessar. Conforme mostrado na figura, Bob obteve acesso aos itens públicos 420 do usuário, enquanto Mary obteve acesso aos itens públicos 420 do usuário e também aos ITENS PRIVATIVOS<sub>1</sub> 430. Quando é  
 25 dado acesso a qualquer grupo de conteúdo, tal acesso pode incluir: permitir que a pessoa (por exemplo, Bob ou Mary) envie pelo correio um conteúdo 450 para tal grupo ou para um item em particular no grupo, a fim de visualizar outros con-

teúdos postados 460 no grupo ou anotar o conteúdo previamente postado 470. No mínimo, o acesso pode incluir a visualização passiva do conteúdo. Em alguns casos, Bob e Mary poderão exportar pelo menos uma porção do conteúdo ao qual eles  
 5 tiveram acesso fora do grupo designado baseado nas preferências do usuário.

Além disso, o usuário pode se comunicar com Bob e Mary simultaneamente, deste modo, em diferentes contextos de privacidade, sem a necessidade de ativa ou conscientemente  
 10 comutar entre contextos para assim se comunicar com os mesmos. Além disso, estas mudanças de contexto podem ocorrer de forma transparente ao usuário, assim como tanto ao Bob quanto à Mary.

Em geral, o conteúdo do usuário pode ser organizado de uma maneira hierárquica, sobreposta, conforme demonstrado pelo diagrama exemplar 500 da Figura 5, ou de uma maneira não sobreposta, conforme ilustrado pelo diagrama 600 da Figura 6. Por exemplo, na Figura 5, o conteúdo é agrupado e cada grupo recebe um nível de privacidade. Neste caso, o  
 15 NÍVEL DE PRIVACIDADE<sub>0</sub> 510 representa um conteúdo com uma privacidade mínima, ou, em outras palavras, o conteúdo se encontra disponível ao público. Os NÍVEIS DE PRIVACIDADE<sub>(1-M)</sub> (520, 530, e 540, respectivamente, nos quais M é um inteiro maior que ou igual a um) representam o conteúdo com níveis  
 20 crescentes de privacidade. As pessoas com acesso ao conteúdo de NÍVEL DE PRIVACIDADE<sub>1</sub> 520 também terão acesso ao conteúdo de NÍVEL DE PRIVACIDADE<sub>0</sub> 510. Ou seja, as pessoas com acesso ao conteúdo de NÍVEL DE PRIVACIDADE<sub>M</sub> 540 também terão acesso

ao conteúdo com níveis mais baixos de privacidade.

De maneira alternativa, os grupos de conteúdo podem ser não sobrepostos e, deste modo, mutuamente exclusivos entre si, conforme demonstrado na Figura 6. Com a exceção do conteúdo público 610, as pessoas com acesso ao conteúdo com algum nível de privacidade indicado (por exemplo, os níveis crescentes de privacidade de 1 (620), 2 (630), 3 (640) e/ou a K (650) (sendo K um inteiro maior que ou igual a um) não implicitamente terão acesso a outro conteúdo privado independente do seu nível de privacidade. Sendo assim, quando uma pessoa tem acesso ao conteúdo de NÍVEL DE PRIVACIDADE<sub>3</sub> 640, o usuário também precisará explicitamente atribuir algum nível de privacidade inferior (por exemplo, NÍVEL<sub>1</sub> 620, e/ou NÍVEL<sub>2</sub> 630) para que a pessoa tenha acesso àquele conteúdo também. Deve-se entender que o conteúdo pode ser organizado de outras maneiras, como, por exemplo, por uma combinação de grupos hierárquicos e não sobrepostos.

Devido à natureza da presente invenção, o usuário poderá ser ativo ou interagir com múltiplas pessoas em vários contextos de privacidade - alguns públicos, alguns ligeiramente privados, e outros muito privados. Durante tais interações, o usuário poderá ser apresentado ao conteúdo relevante à interação que ocorre naquele momento. A apresentação do conteúdo relevante poderá lembrar ao usuário sobre o nível de privacidade atribuído ao conteúdo ou simplesmente prover ao usuário um quadro de referência para tal interação. A interação com mais de uma pessoa em mais de um contexto de privacidade ao mesmo tempo pode se tornar relativa-

mente caótico para o usuário. A fim de manter um senso de ordem para o usuário, um componente de reconciliação 710, conforme mostrado na Figura 7, poderá ser empregado e incluído nos sistemas de comunicação controladas 100, 200 das Figuras 1 e 2, respectivamente, supra.

O componente de reconciliação 710 pode determinar a apresentação de conteúdo e/ou jardins ao usuário com base pelo menos em parte sobre quais jardins se encontram ativos no momento. Por exemplo, alguns jardins podem ser estabelecidos pelo usuário com regras de apresentação que determinam como o conteúdo será exibido ao usuário, assim como à pessoa que se comunica com o usuário sobre aquele conteúdo. Em geral, o componente de reconciliação 710 pode resolver questões relativas à exibição de conteúdo quando este afetar o usuário assim como as pessoas que interagem com o usuário.

Várias metodologias de acordo com a presente invenção serão agora descritas através de uma série de atos, devendo-se entender que a presente invenção não se limita à ordem dos atos, uma vez que alguns atos poderão, de acordo com a presente invenção, ocorrerem em diferentes ordens e/ou concorrentemente com outros atos a partir dos mostrados e descritos no presente documento. Por exemplo, os versados na técnica entenderão e apreciarão que uma metodologia pode, de maneira alternativa, ser representada como uma série de estados ou eventos inter-relacionados, como, por exemplo, em um diagrama de estados. Além disso, nem todos os atos ilustrados podem ser requeridos no sentido de implementar uma metodologia de acordo com a presente invenção.

A seguir, com referência à Figura 8, é mostrado o fluxograma de um método exemplar 800 que facilita a comunicação simultânea em múltiplos contextos de privacidade de acordo com um aspecto da presente invenção. O método 800 envolve o recebimento de entrada de acesso de uma pessoa, como, por exemplo, as informações de identificação (login) da pessoa a fim de ter acesso a uma comunidade em linha, na etapa 801. A comunicação em linha pode ser expansiva, como, por exemplo, a Rede mundial (World Wide Web) ou mais restrita, como, por exemplo, a comunidade de uma empresa, uma comunidade escolar, ou uma comunidade de pessoas somente.

Na etapa 820, a entrada de acesso pode ser analisada a fim de identificar e autenticar a identidade da pessoa e os direitos de acesso à comunidade em geral e/ou ao conteúdo específico dos usuários da comunidade. Na etapa 830, o contexto de privacidade da pessoa pode ser determinado com relação ao conteúdo pertencido por outras pessoas da comunidade, e, assim, a interação com tal conteúdo poderá se iniciar. Será apreciado que mais de uma pessoa poderá se registrar na comunidade de uma maneira similar.

Na etapa 840, comunicações simultâneas em diferentes contextos de privacidade podem acontecer entre pelo menos um usuário ou uma ou mais pessoas que interagem com o conteúdo do usuário. Ou seja, o usuário pode sem dificuldade interagir com pelo menos duas pessoas diferentes que têm um contexto de privacidade diferente associado ao usuário ao mesmo tempo sem que seja necessário comutar conscientemente entre contextos ou modelos de privacidade. O mesmo é verda-

deiro quando apenas uma pessoa se comunica com o usuário. Isto acontece porque é possível que uma pessoa seja atribuída a mais de um nível de privacidade. Por conseguinte, o usuário pode interagir com tal pessoa em ambos os níveis de privacidade sem problema. O método 800 permite que o usuário ignore o contexto corrente (o contexto da pessoa) ao se ajustar automaticamente o contexto do usuário, conforme necessário.

A seguir, com referência à Figura 9, é mostrado o fluxograma de um método exemplar 900 que facilita a comunidade simultânea de ambos os contextos privado e público (por exemplo, o não privado ou de privacidade mínima) de acordo com um aspecto da presente invenção. O método 900 envolve o estabelecimento de um jardim de usuário na etapa 910. Isto pode ser feito em parte ao se carregar o conteúdo do usuário de modo a torná-lo disponível para uma comunidade em linha sujeita a várias restrições. Por exemplo, um ou mais níveis de privacidade podem ser atribuídos ao conteúdo. Os níveis de privacidade podem incluir graus de privacidade privativos e/ou públicos. O usuário poderá atribuir um nível apropriado de privacidade ao conteúdo, ou, de maneira alternativa, o sistema ou método poderá reconhecer o contexto do conteúdo e automaticamente atribuir um nível de privacidade apropriado. Neste último caso, certos tipos de conteúdo só podem ser "colocados" em jardins com um nível de privacidade adequado. Por exemplo, o sistema ou método pode ser treinado a reconhecer informações médicas ou relacionadas à medicina e automaticamente atribuir o nível de privacidade mais elevado.

Como um resultado, estas informações podem ser colocadas no jardim apropriado.

Na etapa 920, o usuário pode atribuir níveis de privacidade ou conceder direitos de acesso às pessoas da rede social ou da comunidade em linha do usuário. Por exemplo, qualquer pessoa da comunidade em linha do usuário pode ter acesso ao conteúdo "público" do usuário. Este acesso público pode ser dado por padrão ou explicitamente pelo usuário. Outras pessoas da comunidade conhecidas do usuário podem ser atribuídas a um ou mais níveis de privacidade que correspondem aos níveis de privacidade atribuídos ao conteúdo do usuário.

Na etapa 930, os dados de login de uma pessoa podem ser recebidos e o nível de privacidade daquela pessoa pode ser identificado na etapa 940. Na etapa 950, o acesso ao conteúdo de um respectivo usuário pode ser obtido com base no nível de privacidade da pessoa. A autenticação da identidade da pessoa e os níveis de privacidade (por exemplo, da etapa 930 a 950) podem ser repetidos para cada pessoa que se registra na comunidade na etapa 960. Na etapa 970, qualquer usuário pode se comunicar ou de outra forma interagir com uma ou mais pessoas em diferentes níveis de privacidade ao mesmo tempo.

Voltando agora para a Figura 10, é mostrado o fluxograma de um método exemplar 100 que facilita a proposta ou a atribuição automáticas de um nível de privacidade a uma pessoa que se comunica com um usuário com base nas comunicações e/ou ações do usuário de acordo com um aspecto da pre-

sente invenção. O método 1000 envolve o monitoramento das ações do usuário e/ou das comunicações do usuário com relação a qualquer pessoa em questão na etapa 1010. Exemplos de ações de usuário incluem as atribuições de nível de privacidade previamente feitas a outras pessoas da mesma lista de distribuição que a pessoa em questão, as atribuições de nível de privacidade já feitas pela pessoa em questão para um conteúdo similar, a reorganização da rede social ou jardins do usuário, ou coisa do gênero. As comunicações de usuário podem incluir as interações entre o usuário e a pessoa em questão, como, por exemplo, as discussões, as mensagens, as conversas específicas, ou coisa do gênero.

As informações coletadas enquanto se monitora na etapa 1010 podem ser analisadas na etapa 1020 de modo a determinar se devem ser feitas alguma mudança nos níveis de privacidade atribuídos e, caso positivo, que tipos de mudanças devem ser feitas ou sugeridas ao usuário. Na etapa 1030, o método pode ser treinado para automaticamente sugerir ou atribuir o nível de privacidade mais apropriado para uma pessoa em particular com base pelo menos em parte nas ações do usuário e/ou nas comunicações que o usuário tem com a pessoa. Como um resultado, o usuário pode ficar mais confiante de que os níveis de privacidade atribuídos às pessoas foram atribuídos de uma maneira consistente.

Voltando para a Figura 11, é mostrado o fluxograma de um método exemplar 1100 que facilita a interação entre uma pessoa e o jardim de um usuário de acordo com um aspecto da presente invenção. O método 1000 envolve a provisão de

que pelo menos duas pessoas se registram em uma comunidade baseada em jardins na etapa 1110. Em particular, pelo menos uma primeira pessoa é atribuída a um primeiro nível de privacidade e pelo menos uma segunda pessoa é atribuída a um  
5 segundo nível de privacidade - diferente do primeiro nível de privacidade. Por exemplo, os níveis de privacidade dados 0-2, em que 0 é o menos privado (por exemplo, público) e 2 é o mais privado para este uso em particular, o primeiro nível de privacidade podendo ser "0" e o segundo nível de privaci-  
10 dade podendo ser "2". Na etapa 1120, o conteúdo de jardim para o primeiro e segundo níveis de privacidade pode ser exibido para a primeira e segunda pessoas, respectivamente.

A seguir, o usuário (proprietário ou co-proprietário do conteúdo de jardim) pode interagir ou de outra  
15 tra forma se comunicar com a primeira e a segunda pessoas ao mesmo tempo nos dois níveis de privacidade diferentes (na etapa 1130). Será apreciado que a comunicação entre o usuário e as duas pessoas pode se iniciar ao mesmo tempo, como, por exemplo, através de uma IM (mensagem instantânea), e-  
20 mail, programa de bate-papo, e/ou blogging; no entanto, o acesso aos jardins do usuário pode ser concedido depois de se estabelecer o nível de privacidade apropriado de cada pessoa. Na prática, por exemplo, imagine que John e Jane são amigos de Tim e desejam acesso aos jardins de Tim. Tim dá  
25 acesso a John ao seu jardim público e acesso a Jane ao seu jardim de nível de privacidade 1. Os três podem "conversar" entre si em linha a qualquer momento, no entanto, os níveis de privacidade de John e Jane devem ser identificados antes

de lhes permitir acesso a seus respectivos jardins a fim de visualizar o conteúdo ou as mensagens de correio, comentários, etc. em seus respectivos jardins.

Com referência, a seguir, à Figura 12, é ilustrado  
5 um fluxograma que ilustra um método exemplar 1200 que facilita a interação de uma pessoa com o jardim de um usuário de acordo com um aspecto da presente invenção. O método 1200 se inicia ao prover acesso a uma pessoa ao jardim de um usuário na etapa 1210. Na etapa 1220, a pessoa pode realizar pelo  
10 menos um dentre o seguinte com relação ao seu jardim: blogar ou postar textos, fotografias, ou outro conteúdo para o jardim do usuário; visualizar o conteúdo postado por outras pessoas; visualizar o conteúdo postado pelo usuário; e/ou fazer anotações no conteúdo previamente postado por outras  
15 pessoas ou pela pessoa. Além disso, o usuário poderá tornar o conteúdo disponível para visualização passiva fora do conteúdo de jardim de uma maneira controlada, tal como, através de alimentações sindicalizadas (por exemplo, a RSS). Os jardins podem ser de propriedade de mais de um usuário; sendo  
20 assim, os mesmos podem ser controlados por múltiplos usuários.

A fim de prover um contexto adicional para vários aspectos da presente invenção, a Figura 13 e a apresentação a seguir pretendem prover uma breve descrição geral de um  
25 ambiente operacional adequado 1310 no qual vários aspectos da presente invenção podem ser implementados. Embora a presente invenção seja descrita no contexto geral de instruções executáveis em computador, tais como, módulos de programa,

executadas por um ou mais computadores ou outros dispositivos, os versados na técnica reconhecerão que a presente invenção pode também ser implementada em combinação com outros módulos de programa e/ou como uma combinação de hardware e  
5 software.

De modo geral, no entanto, os módulos de programa incluem rotinas, programas, objetos, componentes, estruturas de dados, etc. que realizam tarefas particulares ou implementam tipos de dados particulares. O ambiente operacional  
10 1310 é apenas um exemplo de um ambiente operacional adequado e não pretende sugerir nenhuma limitação quanto ao âmbito de uso ou funcionalidade da presente invenção. Outros sistemas, ambientes e/ou configurações de computador bem conhecidos que podem ser adequados para uso com a presente invenção in-  
15 cluem, porém não se limitam a, computadores pessoais, dispositivos de computação do tipo laptop ou portáteis, sistemas multiprocessadores, sistemas baseados em microprocessadores, equipamentos eletrônicos programáveis pelo consumidor, PC de rede, minicomputadores, computadores de grande porte, ambi-  
20 entes computacionais distribuídos que incluem os sistemas ou dispositivos acima, ou coisa do gênero.

Com referência à Figura 13, um ambiente exemplar 1310 para a implementação dos vários aspectos da presente invenção inclui um computador 1312. O computador 1312 inclui  
25 uma unidade de processamento 1314, uma memória de sistema 1316, e a um barramento de sistema 1318. O barramento de sistema 1318 acopla os componentes de sistema, incluindo, mas sem se limitar, a memória de sistema 1316 à unidade de

processamento 1314. A unidade de processamento 1314 pode ser qualquer um dentre os vários processadores disponíveis. Os microprocessadores duais ou outras arquiteturas de multiprocessador podem também ser empregados como a unidade de processamento 1314.

O barramento de sistema 1318 pode ser qualquer um dentre os diversos tipos de estruturas de barramento, incluindo o barramento de memória ou a controladora de memória, um barramento periférico ou barramento externo, e/ou um barramento local que usa qualquer uma dentre uma variedade de arquiteturas de barramento, incluindo, porém sem se limitar, o barramento de 11 bits, a Arquitetura de Padrão Industrial (ISA), a Arquitetura de Micro Canal (MCA), a arquitetura ISA Aperfeiçoada (EISA), os equipamentos Eletrônicos de Acionamento Inteligente (IDE), o Barramento Local da Associação VESA (VLB), a Interconexão de Componentes Periféricos (PCI), o Barramento Serial Universal (USB), a Porta Gráfica Avançada (AGP), o barramento da Associação Internacional dos Cartões de Memória do Computador Pessoal (PCMCIA), e a Interface de Sistemas de Computadores Pequenos (SCSI).

A memória de sistema 1316 inclui a memória volátil 1320 e a memória não volátil 1322. O sistema de entrada / saída básico (BIOS), contendo as rotinas básicas para transferir informações entre elementos dentro do computador 1312, como, por exemplo, durante a inicialização, é armazenado na memória não volátil 1322. A guisa de ilustrados, e não de limitação, a memória não volátil 1322 pode incluir uma memória de leitura (ROM), uma memória programável (PROM), uma

memória eletricamente programável (EPROM), uma memória ROM eletricamente apagável (EEPROM), ou uma memória flash. A memória volátil 1320 inclui a memória de acesso aleatório (RAM), que atua como uma memória de cache externa. A guisa  
5 de ilustração, e não de limitação, a memória RAM encontra-se disponível em muitas formas, tais como, a memória RAM estática (SRAM), a memória DRAM estática (SDRAM), a memória SDRAM de taxa de dados duplos (DDR SDRAM), a memória SDRAM aperfeiçoada (ESDRAM), a memória DRAM Synchlink (SLDRAM), e  
10 o barramento de memória Ram direto (DRDRAM).

O computador 1312 inclui ainda os meios de armazenamento em computador removíveis / não removíveis, voláteis / não voláteis. A Figura 13 ilustra, por exemplo, um armazenamento de disco 1324. O armazenamento de disco 1324 inclui,  
15 porém não se limita aos, dispositivos tais como uma unidade de disco magnético, uma unidade de disco flexível, uma unidade de fita, uma unidade Jaz, uma unidade Zip, uma unidade LS-100, um cartão de memória flash, ou um bastão de memória. Além disso, o armazenamento de disco 1324 pode incluir meios  
20 de armazenamento separados ou em combinação com outros meios de armazenamento, incluindo, porém não se limitando, a unidade de disco ótico, tal como o dispositivo de memória ROM de disco compacto (CD-ROM), a unidade de gravação em CD (Unidade CD-R), a unidade de regravação em CD (Unidade CD-RW),  
25 ou a unidade de memória ROM de disco versátil digital (DVD-ROM). Para facilitar a conexão dos dispositivos de armazenamento de disco 1324 ao barramento de sistema 1317, uma interface removível ou não removível é tipicamente usada, co-

mo, por exemplo, a interface 1326.

Deve-se apreciar que a Figura 13 descreve um software que atua como um intermediário entre usuários e os recursos básicos de computador descritos no ambiente operacional adequado 1310. Este software inclui um sistema operacional 1328. O sistema operacional 1328, que pode ser armazenado no armazenamento de disco 1324, atua de modo a controlar e alocar os recursos do sistema computacional 1312. As aplicações de sistema 1330 se aproveitam do gerenciamento de recursos por parte do sistema operacional 1328 através dos módulos de programa 1332 e dos dados de programa 1334 armazenados na memória de sistema 1316 e no armazenamento de disco 1324. Deve-se apreciar que a presente invenção pode ser implementada com vários sistemas operacionais ou combinações de sistemas operacionais.

Um usuário entra comandos ou informações no computador 1312 através dos dispositivos de entrada 1336. Os dispositivos de entrada 1336 incluem, porém não se limitam a, um dispositivo de indicação, como, por exemplo, um mouse, um trackball, uma caneta, uma mesa sensível ao toque, um teclado, um microfone, um joystick, uma controladora de jogos, uma antena parabólica para satélite, um cartão sintonizador de TV, uma câmera digital, uma rede câmera, ou coisa do gênero. Estes e outros dispositivos de entrada são conectados à unidade de processamento 1314 através do barramento de sistema 1318 através de uma porta de interface 1338. As portas de interface 1338 incluem, por exemplo, uma porta serial, uma porta paralela, uma porta de jogos, ou um barramento

serial universal (USB). Os dispositivos de saída 1340 usam alguns dentre os mesmos tipos de portas que os dispositivos de entrada 1336. Sendo assim, por exemplo, uma porta USB pode ser usada para prover entrada ao computador 1312, e para  
5 emitir informações do computador 1312 para um dispositivo de saída 1340. Um adaptador de saída 1342 é provido a fim de ilustrar que há alguns dispositivos de saída 1340, como monitores, alto-falantes, e impressoras, entre outros dispositivos de saída 1340 que requerem adaptadores especiais. Os  
10 adaptadores de saída 1342 incluem, a guisa de ilustração, e não de limitação, os cartões de som e vídeo que provêm um meio de conexão entre o dispositivo de saída 1340 e o barramento de sistema 1318. Deve-se notar que outros dispositivos e/ou sistemas de dispositivos provêm capacidades de entrada  
15 e de saída, tais como os computadores remotos 1344.

O computador 1312 pode operar em um ambiente de rede utilizando conexões lógicas com um ou mais computadores remotos, tais como, com o computador remoto 1344. O computador remoto 1344 pode ser um computador pessoal, um servidor,  
20 um roteador, um PC de rede, uma estação de trabalho, um aparelho baseado em microprocessador, um dispositivo de rede não hierárquica ou outro nó de rede comum, ou coisa do gênero, e tipicamente inclui muitos dos ou todos os elementos descritos acima com relação ao computador 1312. Para fins de  
25 brevidade, apenas um dispositivo de armazenamento de memória 1346 é ilustrado com o computador remoto 1344. O computador remoto 1344 é logicamente conectado ao computador 1312 através de uma interface de rede 1348 e em seguida fisicamente

conectado via uma conexão de comunicação 1350. A interface de rede 1348 abrange as redes de comunicação, tais como, as redes de área local (LAN) e as redes de área remota (WAN). As tecnologias de rede LAN incluem a Interface de Dados Distribuídos de Fibra (FDDI), a Interface de Dados Distribuídos de Cobre (CDDI), a Ethernet/IEEE 1102.3, a rede Token Ring/IEEE 1102.5, e similares. As tecnologias de rede WAN incluem, mas não se limitam a, enlaces ponto a ponto, redes de comutação de circuito, tais como as Redes Digitais de Serviços Integrados (ISDN) e suas variações, as redes de comutação de pacotes, e as Linhas Digitais de Assinante (DSL).

A conexão de comunicação 1350 se refere ao hardware / software empregado para conectar a interface de rede 1348 ao barramento 1318. Embora a conexão de comunicação 1350 seja mostrada, para clareza ilustrativa, dentro do computador 1312, a mesma pode também ser externa ao computador 1312. O hardware / software necessários para conexão à interface de rede 1348 incluem, tão-somente para fins de exemplo, tecnologias interna e externa, tais como, os modems, incluindo os modems da grade telefônica regular, os modems a cabo e os modems de linha DSL, os adaptadores de rede ISDN, e os cartões da Ethernet.

O que se encontra descrito acima inclui exemplos da presente invenção. Evidentemente, não é possível descrever toda a combinação de componentes ou metodologias concebível para fins de descrição da presente invenção, contudo, uma pessoa com habilidade simples na técnica poderá reconhecer que são possíveis muitas outras combinações e permutas

da presente invenção. Por conseguinte, a presente invenção pretende abranger todas estas alterações, modificações, e variações que recaiam no espírito e âmbito das reivindicações em apenso. Além disso, na extensão do termo "inclui" 5 usado na descrição detalhada ou nas reivindicações em apenso, tal termo pretende ser inclusivo à maneira similar do termo "compreende", uma vez que "compreende" é interpretado, quando empregado, como uma palavra transicional em uma reivindicação.

## REIVINDICAÇÕES

1. Sistema de comunicação controlada,  
**CARACTERIZADO** pelo fato de compreender:

- um componente de análise de dados que examina  
5 pelo menos um dentre o seguinte: a entrada de acesso de pelo  
menos uma pessoa e as informações derivadas desta entrada a  
fim de determinar o contexto de privacidade da pessoa com  
relação ao conteúdo pertencente a pelo menos um usuário; e

- um componente de controle de contexto que regula  
10 a comunicação entre o pelo menos um usuário e a pelo menos  
uma pessoa, por meio do que o pelo menos um usuário poderá  
se comunicar com a pelo menos uma pessoa em mais de um con-  
texto de privacidade, simultaneamente.

2. Sistema, de acordo com a reivindicação 1,  
15 **CARACTERIZADO** pelo fato de que o contexto de privacidade  
compreende pelo menos dois níveis de privacidade.

3. Sistema, de acordo com a reivindicação 1,  
**CARACTERIZADO** pelo fato de que a entrada de acesso compreen-  
de os dados de identificação (login) da pessoa.

20 4. Sistema, de acordo com a reivindicação 1,  
**CARACTERIZADO** pelo fato de que o conteúdo é organizado em um  
ou mais grupos, de tal modo que o um ou mais grupos seja um  
dentre o seguinte: distinto ou sobreposto.

5. Sistema, de acordo com a reivindicação 4,  
25 **CARACTERIZADO** pelo fato de que cada grupo é atribuído a um  
nível de privacidade.

6. Sistema, de acordo com a reivindicação 1,  
**CARACTERIZADO** pelo fato de que o conteúdo é atribuído a pelo

menos um nível de privacidade.

7. Sistema, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de compreender ainda um componente de comunicação de múltiplos contextos que facilita a comunicação do usuário com outras pessoas registradas em uma comunidade em linha em uma pluralidade de contextos de privacidade ao mesmo tempo e que mitiga a um usuário a comutação explícita entre diferentes contextos de privacidade.

8. Sistema, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o contexto de privacidade da pessoa determina se a pessoa tem acesso a pelo menos uma porção do conteúdo do usuário.

9. Sistema, de acordo com a reivindicação 1, **CARACTERIZADO** adicionalmente pelo fato de compreender:

15           - um componente de monitor que monitora pelo menos uma dentre as ações do usuário e as comunicações do usuário com a pelo menos uma pessoa; e

          - um componente de inteligência artificial que é treinado para automaticamente atribuir à pelo menos uma pessoa um contexto de privacidade para o conteúdo do usuário baseado em pelo menos uma dentre as ações do usuário e as comunicações do usuário com a pelo menos uma pessoa.

10. Sistema, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o conteúdo do usuário é organizado em pelo menos uma dentre as seguintes maneiras: hierárquica, não sobreposta, não hierárquica, parcialmente sobreposta, ou completamente sobreposta.

11. Método que facilita a comunicação controlada

em uma pluralidade de contextos de privacidade, o método sendo **CARACTERIZADO** pelo fato de compreender as etapas de:

- analisar pelo menos um dentre o seguinte: a entrada de acesso de pelo menos uma pessoa e as informações derivadas desta entrada a fim de determinar o contexto de privacidade da pessoa com relação ao conteúdo pertencente a pelo menos um usuário; e

- controlar a comunicação entre o pelo menos um usuário e a pelo menos uma pessoa, por meio do que o pelo menos um usuário poderá se comunicar com a pelo menos uma pessoa em mais de um contexto de privacidade, simultaneamente.

12. Método, de acordo com a reivindicação 11, **CARACTERIZADO** pelo fato de que o contexto de privacidade compreende pelo menos dois níveis de privacidade.

13. Método, de acordo com a reivindicação 11, **CARACTERIZADO** pelo fato de que a entrada de acesso compreende os dados de identificação (login) da pessoa.

14. Método, de acordo com a reivindicação 11, **CARACTERIZADO** adicionalmente pelo fato de compreender a etapa de organizar o conteúdo do usuário em um ou mais grupos.

15. Método, de acordo com a reivindicação 14, **CARACTERIZADO** adicionalmente pelo fato de compreender as etapas de:

- atribuir à cada grupo um contexto de privacidade;  
- atribuir à cada pessoa um contexto de privacidade.

16. Método, de acordo com a reivindicação 11, **CARACTERIZADO** adicionalmente pelo fato de compreender a etapa de atribuir o conteúdo de pelo menos um nível de privaci-

dade.

17. Método, de acordo com a reivindicação 11, **CARACTERIZADO** adicionalmente pelo fato de compreender as etapas de:

5                   - monitorar pelo menos uma dentre as ações do usuário e as comunicações do usuário com a pelo menos uma pessoa; e

                  - atribuir automaticamente à pelo menos uma pessoa um contexto de privacidade para o conteúdo do usuário baseado em pelo menos uma dentre as ações do usuário e as comunicações do usuário com a pelo menos uma pessoa.

10

18. Método, de acordo com a reivindicação 11, **CARACTERIZADO** adicionalmente pelo fato de compreender as etapas de:

15                   - exibir pelo menos uma porção do conteúdo do usuário para a pelo menos uma pessoa quando o contexto de privacidade do conteúdo corresponde ao contexto de privacidade da pessoa; e

                  - permitir que pessoa realize pelo menos um dentre o seguinte quando o acesso ao conteúdo é obtido pela pessoa: blogar ou postar pelo menos um dentre textos, fotografias, ou qualquer outro conteúdo; visualizar o conteúdo postado por outras pessoas; visualizar o conteúdo postado pelo usuário; e/ou fazer anotações no conteúdo previamente postado.

20

25                   19. Sistema de comunicação controlada, **CARACTERIZADO** pelo fato de compreender:

                  - um meio para examinar pelo menos um dentre o seguinte: a entrada de acesso de pelo menos uma pessoa e as

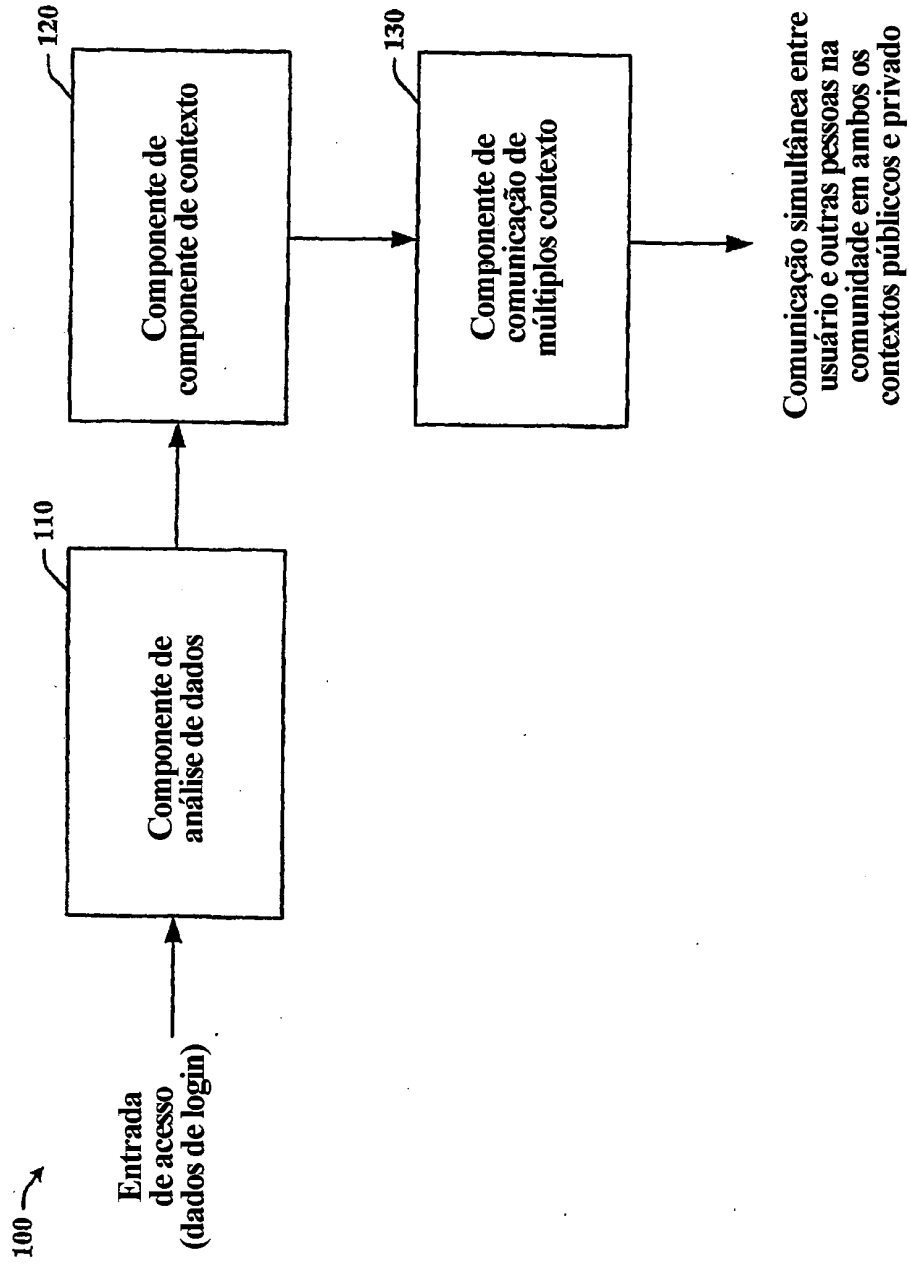
informações derivadas desta entrada a fim de determinar o contexto de privacidade da pessoa com relação ao conteúdo pertencente a pelo menos um usuário; e

- um meio para regular a comunicação entre o pelo menos um usuário e a pelo menos uma pessoa, por meio do que o pelo menos um usuário poderá se comunicar com a pelo menos uma pessoa em mais de um contexto de privacidade, simultaneamente.

20. Sistema, de acordo com a reivindicação 19,  
10 **CARACTERIZADO** adicionalmente pelo fato de compreender:

- um meio para monitorar pelo menos uma dentre as ações do usuário e as comunicações do usuário com a pelo menos uma pessoa; e

- um meio para automaticamente atribuir à pelo menos uma pessoa um contexto de privacidade para o conteúdo do usuário baseado em pelo menos uma dentre as ações do usuário e as comunicações do usuário com a pelo menos uma pessoa.

**FIG. 1**

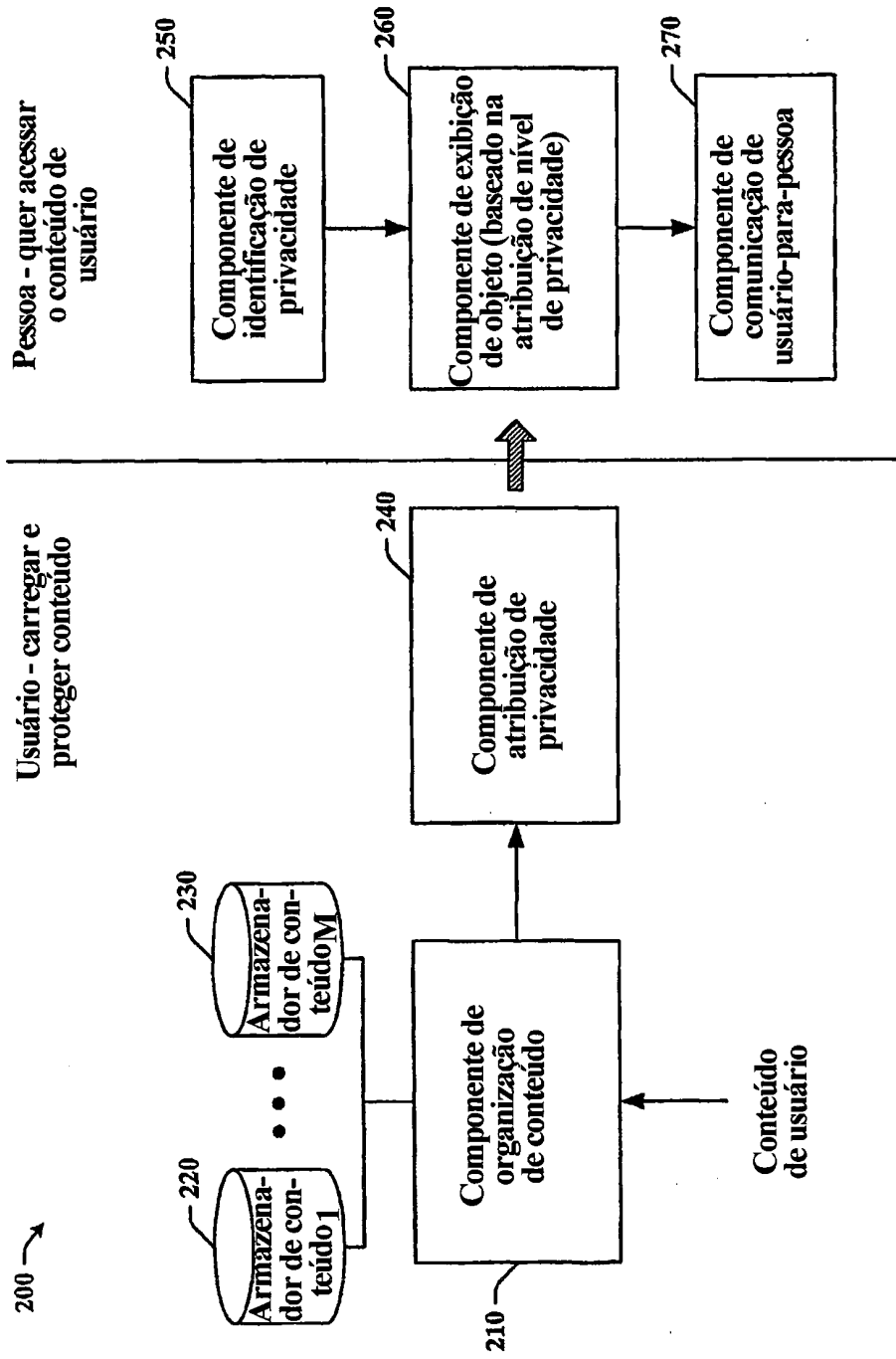


FIG. 2

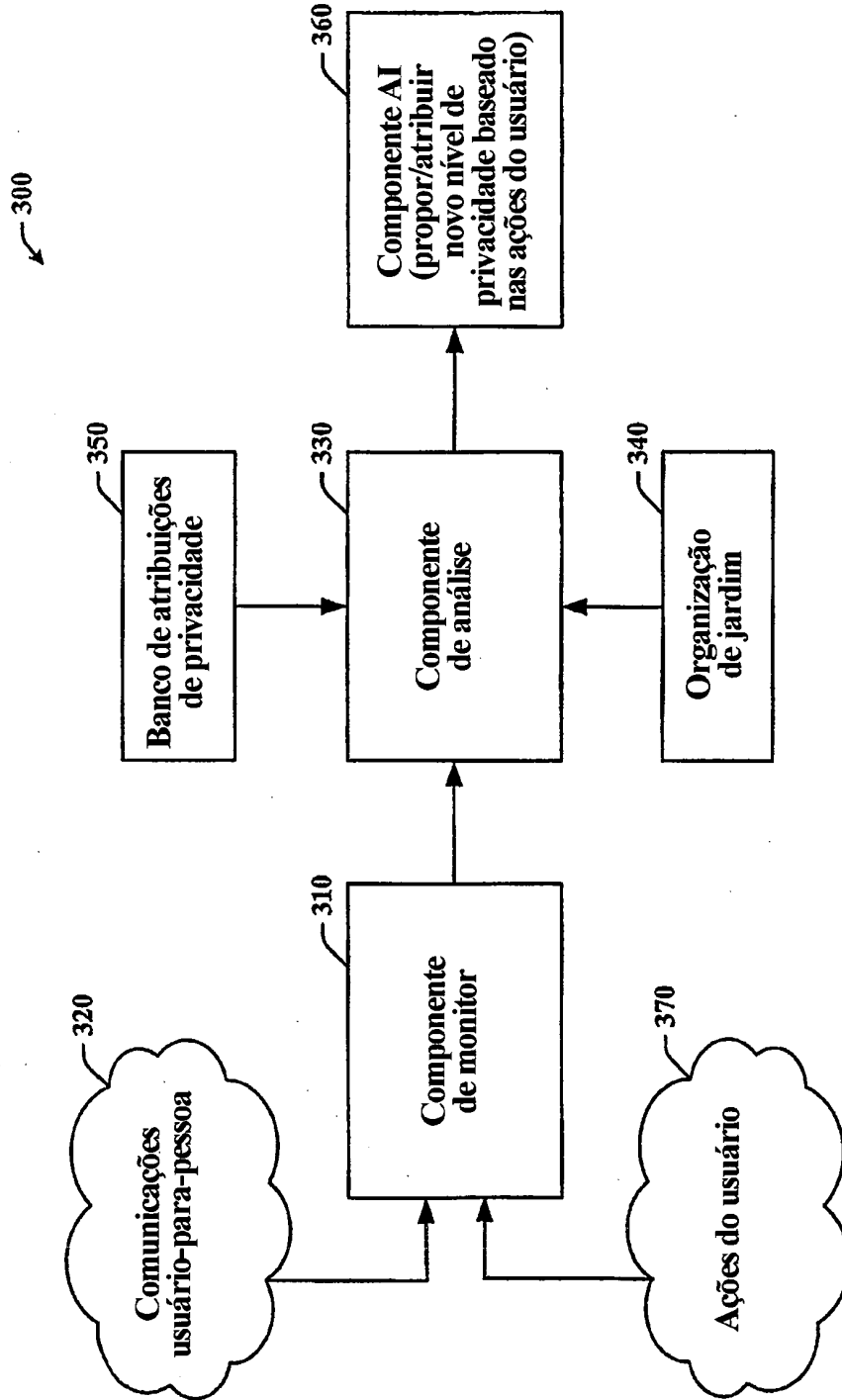


FIG. 3

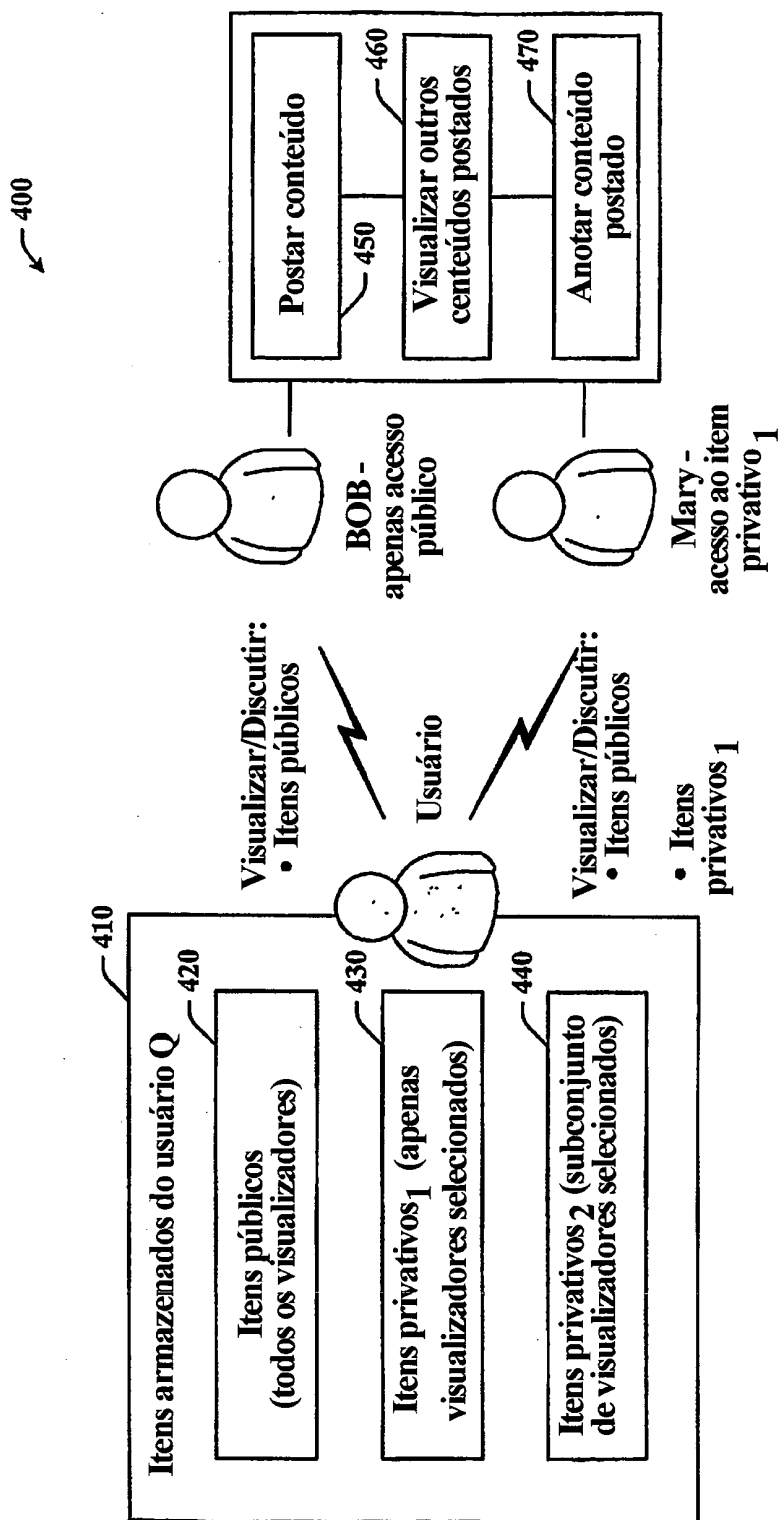
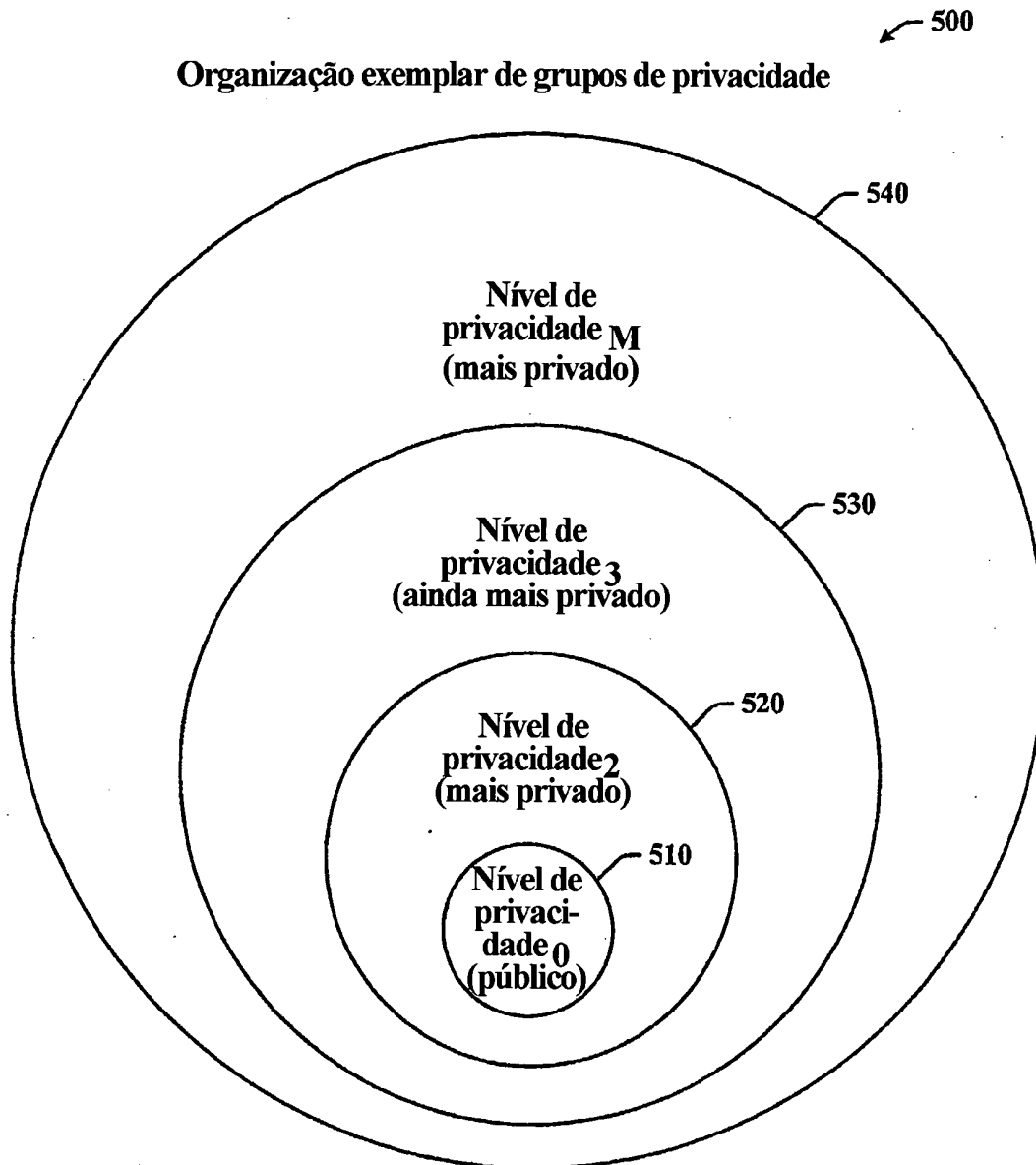
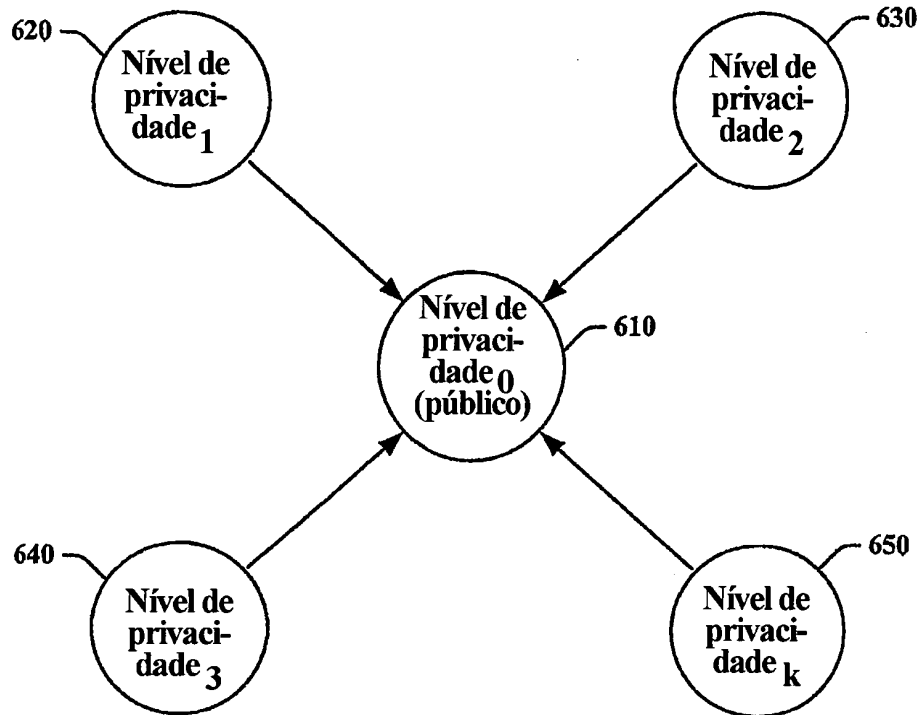


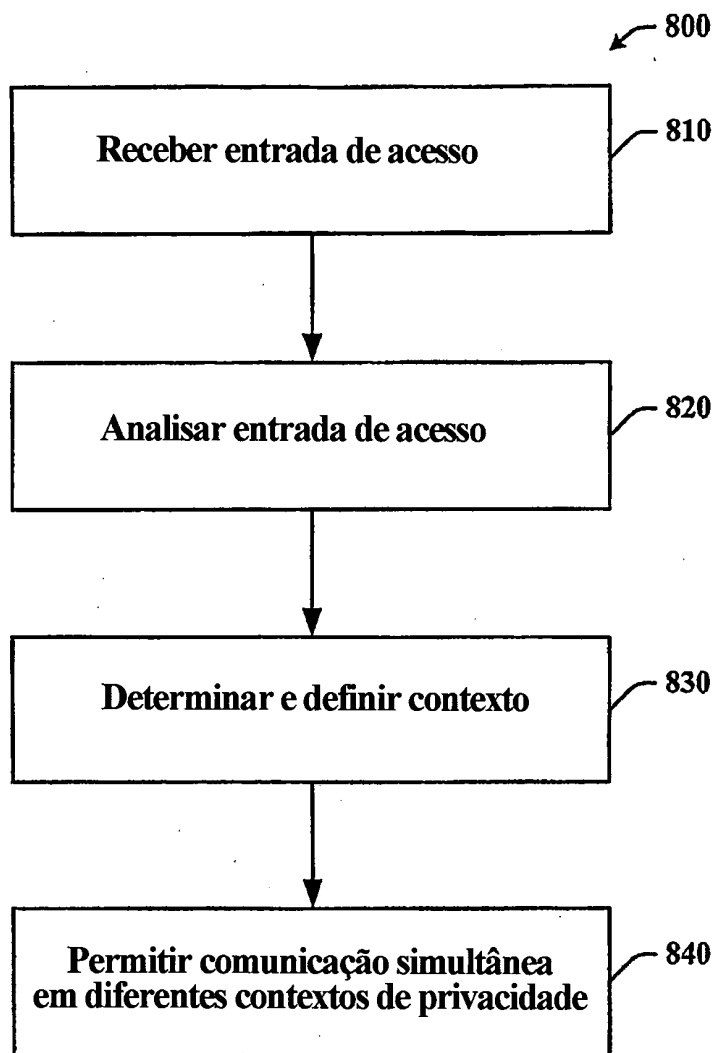
FIG. 4

**FIG. 5**

**Organização exemplar de grupos de privacidade**

Nenhuma sobreposição entre os níveis de privacidade 1-k

**FIG. 6****FIG. 7**

**FIG. 8**

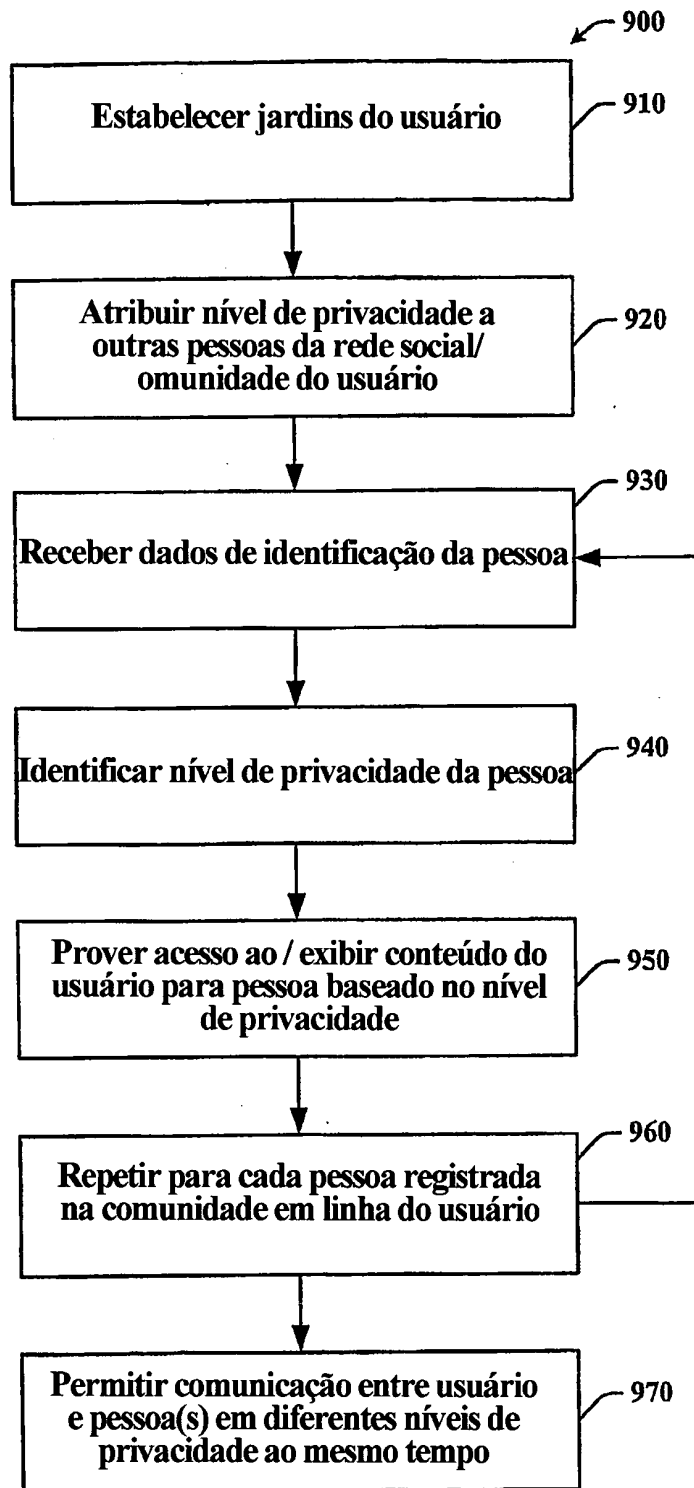
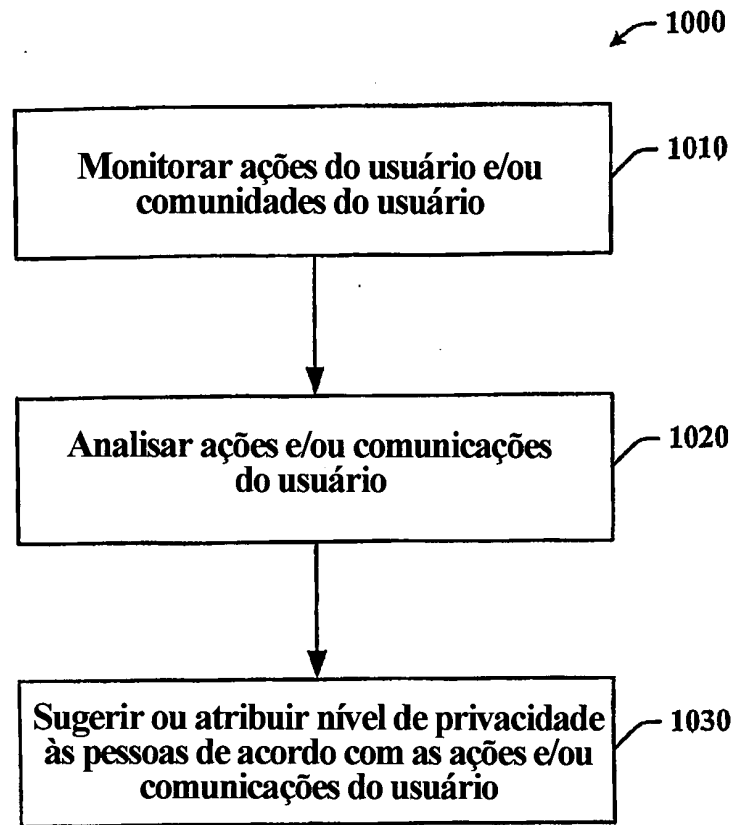


FIG. 9

**FIG. 10**

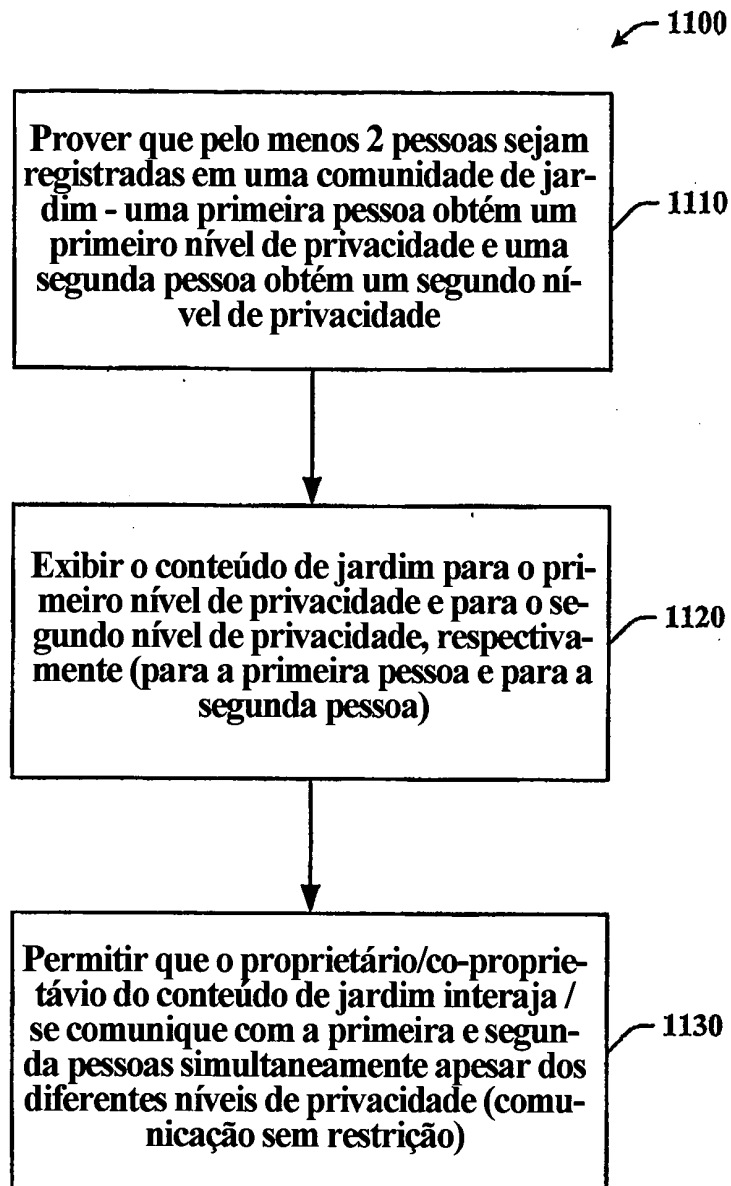


FIG. 11

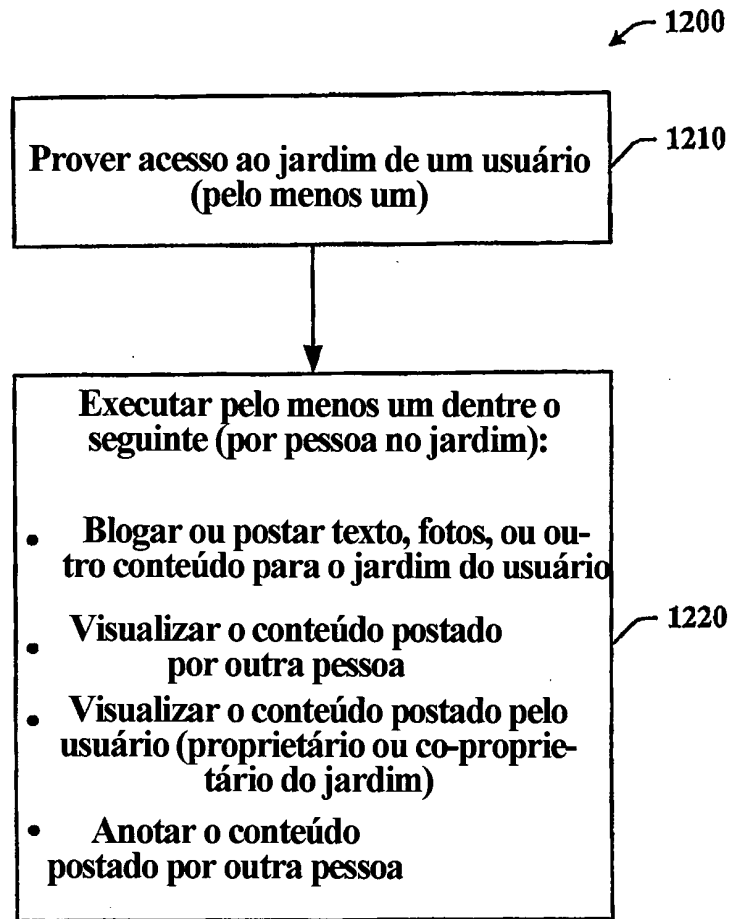


FIG. 12

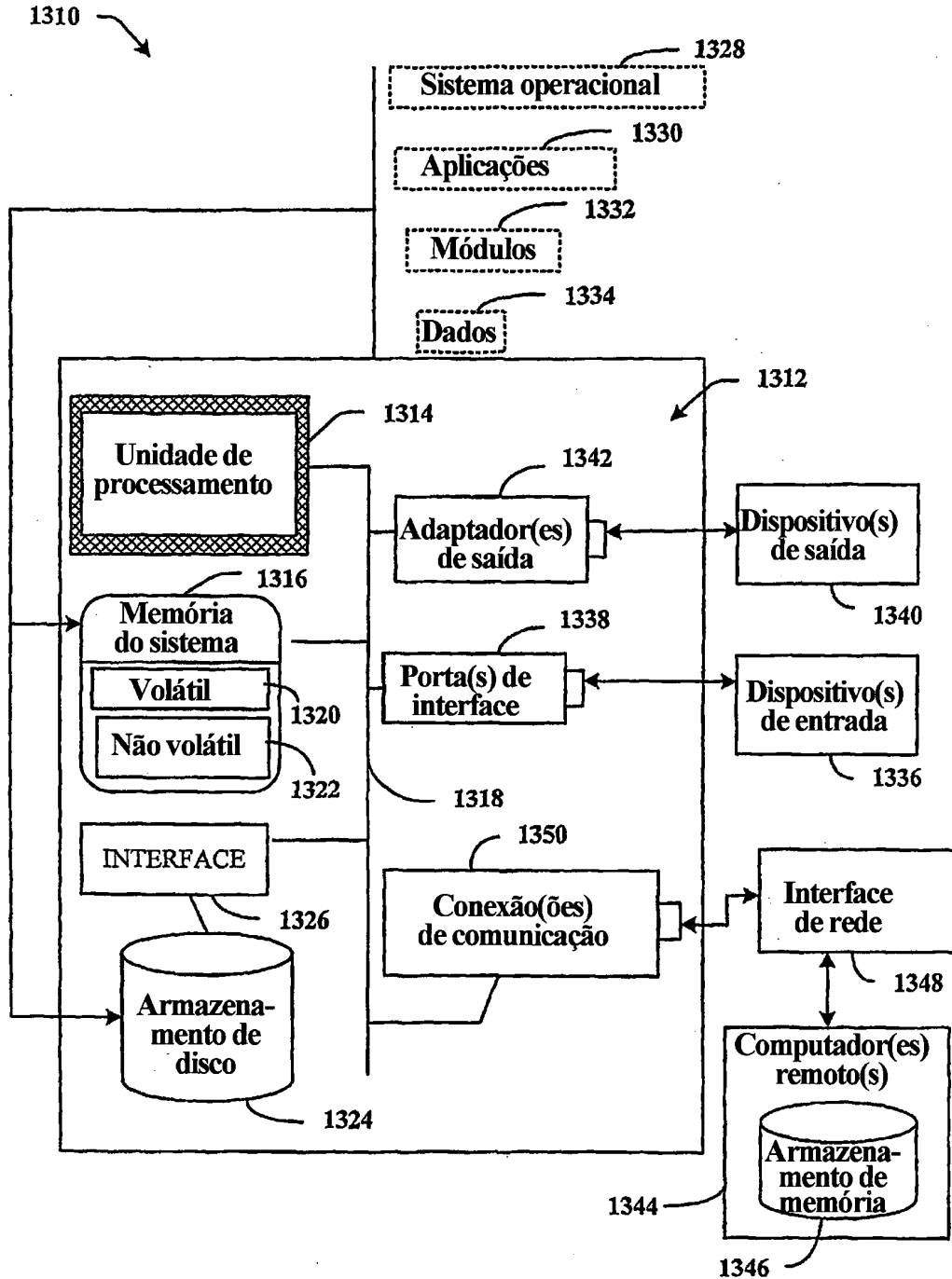


FIG. 13

# RESUMO

## "JARDINS MURADOS"

A presente invenção provê um sistema e método único que facilitam um ambiente de comunicação controlada, permitindo a um usuário participar de uma pluralidade de contextos de privacidade com outras pessoas de uma maneira simultânea. Um usuário poderá atribuir ou definir níveis de privacidade à sua informação, de modo a controlar a visibilidade de tais informações por parte de outras pessoas. Em particular, um primeiro usuário poderá manter um ou mais "jardins" de conteúdo que podem ser acessíveis a pelo menos um subconjunto da comunidade em linha. O acesso aos conteúdos de qualquer um jardim poderá se basear no nível de privacidade do jardim e no nível de privacidade (por exemplo, os parâmetros de acesso) concedidos à pessoa. Os níveis de privacidade e a disposição do conteúdo podem ser hierárquicos e/ou não sobrepostos. Deste modo, um usuário poderá se comunicar com múltiplos usuários ao mesmo tempo, sem restrições, independente do seu contexto ou nível de privacidade, ao mesmo tempo mantendo os limites de privacidade de cada jardim.

REIVINDICAÇÕES

1. Sistema de comunicação controlada,  
**CARACTERIZADO** pelo fato de compreender:

5 - um componente de análise de dados que examina  
pelo menos um dentre o seguinte: a entrada de acesso de pelo  
menos uma pessoa e as informações derivadas desta entrada a  
fim de determinar o contexto de privacidade da pessoa com  
relação ao conteúdo pertencente a pelo menos um usuário; e

10 - um componente de controle de contexto que regula  
a comunicação entre o pelo menos um usuário e a pelo menos  
uma pessoa, por meio do que o pelo menos um usuário poderá  
se comunicar com a pelo menos uma pessoa em mais de um con-  
texto de privacidade, simultaneamente.

15 2. Sistema, de acordo com a reivindicação 1,  
**CARACTERIZADO** pelo fato de que o contexto de privacidade  
compreende pelo menos dois níveis de privacidade.

3. Sistema, de acordo com a reivindicação 1,  
**CARACTERIZADO** pelo fato de que a entrada de acesso compreen-  
de os dados de identificação (login) da pessoa.

20 4. Sistema, de acordo com a reivindicação 1,  
**CARACTERIZADO** pelo fato de que o conteúdo é organizado em um  
ou mais grupos, de tal modo que o um ou mais grupos seja um  
dentre o seguinte: distinto ou sobreposto.

25 5. Sistema, de acordo com a reivindicação 4,  
**CARACTERIZADO** pelo fato de que cada grupo de conteúdo é a-  
tribuído a um nível de privacidade.

6. Sistema, de acordo com a reivindicação 1,  
**CARACTERIZADO** pelo fato de que o conteúdo é atribuído a pelo

menos um nível de privacidade.

7. Sistema, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de compreender ainda um componente de comunicação de múltiplos contextos que facilita a comunicação do usuário com outras pessoas registradas em uma comunidade em linha em uma pluralidade de contextos de privacidade ao mesmo tempo e que mitiga um usuário para comutação explicitamente entre diferentes contextos de privacidade.

8. Sistema, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o contexto de privacidade da pessoa determina se a pessoa tem acesso a pelo menos uma porção do conteúdo do usuário.

9. Sistema, de acordo com a reivindicação 1, **CARACTERIZADO** adicionalmente pelo fato de compreender:

15 - um componente de monitor que monitora pelo menos uma dentre as ações do usuário e as comunicações do usuário com a pelo menos uma pessoa; e

- um componente de inteligência artificial que é treinado para automaticamente atribuir à pelo menos uma pessoa um contexto de privacidade para o conteúdo do usuário baseado em pelo menos uma dentre as ações do usuário e as comunicações do usuário com a pelo menos uma pessoa.

10. Sistema, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o conteúdo do usuário é organizado em pelo menos uma dentre as seguintes maneiras: hierárquica, não sobreposta, não hierárquica, parcialmente sobreposta, ou completamente sobreposta.

11. Método que facilita a comunicação controlada

em uma pluralidade de contextos de privacidade, o método sendo **CARACTERIZADO** pelo fato de compreender as etapas de:

- analisar pelo menos um dentre o seguinte: a entrada de acesso de pelo menos uma pessoa e as informações derivadas desta entrada a fim de determinar o contexto de privacidade da pessoa com relação ao conteúdo pertencente a pelo menos um usuário; e

- controlar a comunicação entre o pelo menos um usuário e a pelo menos uma pessoa, por meio do que o pelo menos um usuário poderá se comunicar com a pelo menos uma pessoa em mais de um contexto de privacidade, simultaneamente.

12. Método, de acordo com a reivindicação 11, **CARACTERIZADO** pelo fato de que o contexto de privacidade compreende pelo menos dois níveis de privacidade.

15 13. Método, de acordo com a reivindicação 11, **CARACTERIZADO** pelo fato de que a entrada de acesso compreende os dados de identificação (login) da pessoa.

14. Método, de acordo com a reivindicação 11, **CARACTERIZADO** adicionalmente pelo fato de compreender a etapa de organizar o conteúdo do usuário em um ou mais grupos.

15. Método, de acordo com a reivindicação 14, **CARACTERIZADO** adicionalmente pelo fato de compreender as etapas de:

- atribuir à cada grupo um contexto de privacidade;  
- atribuir à cada pessoa um contexto de privacidade.

16. Método, de acordo com a reivindicação 11, **CARACTERIZADO** adicionalmente pelo fato de compreender a etapa de atribuir o conteúdo de pelo menos um nível de privaci-

dade.

17. Método, de acordo com a reivindicação 11, **CARACTERIZADO** adicionalmente pelo fato de compreender as etapas de:

5 - monitorar pelo menos uma dentre as ações do usuário e as comunicações do usuário com a pelo menos uma pessoa; e

- atribuir automaticamente à pelo menos uma pessoa um contexto de privacidade para o conteúdo do usuário baseado em pelo menos uma dentre as ações do usuário e as comunicações do usuário com a pelo menos uma pessoa.

10

18. Método, de acordo com a reivindicação 11, **CARACTERIZADO** adicionalmente pelo fato de compreender as etapas de:

15 - exibir pelo menos uma porção do conteúdo do usuário para a pelo menos uma pessoa quando o contexto de privacidade do conteúdo corresponde ao contexto de privacidade da pessoa; e

- permitir que a pessoa realize pelo menos uma dentre o seguinte quando o acesso ao conteúdo é obtido pela pessoa: blogar ou postar pelo menos uma dentre textos, fotografias, ou qualquer outro conteúdo; visualizar o conteúdo postado por outras pessoas; visualizar o conteúdo postado pelo usuário; e fazer anotações no conteúdo previamente postado.

20

25

19. Sistema de comunicação controlada, **CARACTERIZADO** pelo fato de compreender:

- um meio para examinar pelo menos um dentre o seguinte: a entrada de acesso de pelo menos uma pessoa e as informações derivadas desta entrada a fim de determinar o contexto de privacidade da pessoa com relação ao conteúdo  
5 pertencente a pelo menos um usuário; e

- um meio para regular a comunicação entre o pelo menos um usuário e a pelo menos uma pessoa, por meio do que o pelo menos um usuário poderá se comunicar com a pelo menos uma pessoa em mais de um contexto de privacidade, simultaneamente.  
10

20. Sistema, de acordo com a reivindicação 19, **CARACTERIZADO** adicionalmente pelo fato de compreender:

- um meio para monitorar pelo menos uma dentre as ações do usuário e as comunicações do usuário com a pelo menos uma pessoa; e  
15

- um meio para automaticamente atribuir à pelo menos uma pessoa um contexto de privacidade para o conteúdo do usuário baseado em pelo menos uma dentre as ações do usuário e as comunicações do usuário com a pelo menos uma pessoa.