Privacidade em Redes Sociais

Monografia de Segurança de Dados

Aluno: Marcos Paulo Cayres Rosa
Matrícula: 14/0027131

Professor: Pedro Rezende
Universidade de Brasília

Introdução

Aplicações de redes sociais são estruturas formadas por diferentes indivíduos que se relacionam por interdependências, assim como relacionamentos, amizades e contatos de serviço. Dessa forma, permitem que pessoas estabeleçam conexões e façam intercâmbio de informações baseado em seus vários e distintos interesses. Diversas plataformas comerciais com esse modelo tem surgido e ganhado extrema popularidade em âmbito internacional, mas, em contraposição às vantagens claras na questão de comunicação rápida e independente da localidade proporcionada, cresce a preocupação em relação à proteção e à privacidade dos usuários [1].

A popularidade se deve a algumas funcionalidades comuns, assim como:

- Permitir a criação de representações digitais do usuário;
- Articulação de conexões com outros usuários:
  - Estabelecimento de novas conexões, através de proximidade ou interesses em comum;
  - Manter conexões já existentes;
- Exploração do espaço digital, encontrando novas atividades ou ocupação do tempo livre.

Entretanto, isso fomenta o uso indevido, causando riscos como o de acesso não autorizado, o roubo de identidade, o assédio sexual, a propagação de “malwares” e o auxílio para efetuação de crimes. Esses são alguns dos diversos problemas detectados pelas empresas que confeccionam esses produtos, porém, assim surge outra questão: o limiar entre a privacidade e o controle que se deve ter sobre os usuários.

Outros tópicos inerentes para as empresas responsáveis são: a proteção de senhas e dos dados pessoais do usuário, principalmente com a possibilidade de invasão do banco de dados correspondente, além de determinar o conhecimento que os usuários têm sobre os diversos riscos relativos à utilização de redes sociais. Mesmo que os fornecedores procurem assegurar certos méritos, o comércio sobrepõe a eficiência e, assim, há uma predileção em angariar novos utilizadores do que informar falhas ou modos de operar com cautela, fatores que podem afastá-los. No caso, isso leva ao descuido (como deixarem páginas abertas em locais públicos com o perfil acessado) e à exposição de detalhes pessoais que pode trazer prejuízos, especialmente com crianças [3].

Novos mecanismos são investigados, a fim de resolver clássicos problemas de segurança e gerenciamento de confiança semelhante a sistemas distribuídos, aproveitando da informação armazenada nas plataformas da rede social. Tais problemas vão desde a confiança na criação de sistemas auto-organizados para o gerenciamento de chaves, sem infraestrutura para a cooperação em sistemas P2P. Como também, surgem afirmativas [4] de que as estruturas centralizadas vigentes colocam em risco a privacidade do usuário e que os fornecedores não têm a intenção de correção para não ir contra seus modelos de negócio.

Desenvolvimento

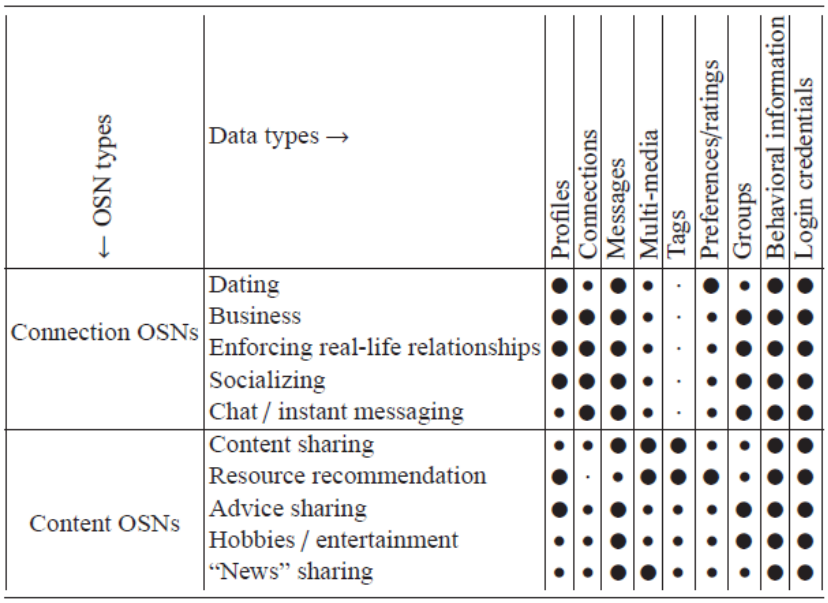
Tipos de dados e classificações

Seguindo a definição de Boyd e Ellison [5], pode-se deduzir que os dados de um usuário contém:

- Perfil: representação do usuário ao mundo exterior, como uma descrição pessoal (ou de um alter ego. Geralmente inclui uma breve descrição, foto e atributos (idade, gênero, dentre outros).
- Conexões: existente entre dois usuários, podendo ser categorizada como amizade, seguidor, etc.
- Mensagens: qualquer pedaço de dado intercambiado entre usuários (ou grupo de usuários), podendo conter texto ou multimídia. Em alguns casos pode ser instantânea ou de vida curta, em outros pode ser armazenada por tempo indefinido, sendo que isso não é algo que o usuário vai ter conhecimento do modo operativo.
- Multimídia: conteúdo que pode ser anexado a mensagens, carregado de modo privado ou em espaços públicos ou associado a um perfil. Exemplos comuns são fotos, vídeos, músicas e gravações de voz.

- Tags: sistema colaborativo de filtragem, determinado por palavras-chaves que são associadas a conteúdos por usuários.
- Preferências, classificações e interesses: funcionalidade de correspondência ou recomendação, muitas vezes descritas explicitamente pelos usuários para apresentar em um perfil público ou, de modo restrito, derivado de seu comportamento nos aplicativos.
- Grupos: conjunto de usuários que compartilham atributos, recursos ou privilégios em comum, como preferências, documentos colaborativos ou acesso a um espaço virtual específico.
- Informação comportamental: relacionado ao histórico de pesquisas, configurações do perfil e qualquer ação executada dentro da rede social.
- Credenciais: modo de "logar" no serviço fornecido. Liga o perfil ao usuário que o determinou e procura diferenciá-lo dos demais.

Os dados indicados acima podem estar todos ou somente alguns presentes nas redes sociais, mas são os vistos como mais comuns. Ademais, abrange a questão da privacidade reconhecida pelo usuário e da capacidade que essas informações podem fornecer tanto para empresas quanto para apropriações indevidas.



↓ OSN types	Data types →	Profiles	Connections	Messages	Multi-media	Tags	Preferences/ratings	Groups	Behavioral information	Login credentials
Connection OSNs	Dating	●	•	●	•	·	●	•	●	●
	Business	●	●	●	•	·	•	●	●	●
	Enforcing real-life relationships	●	●	●	•	·	•	●	●	●
	Socializing	●	●	●	•	·	•	●	●	●
	Chat / instant messaging	•	●	●	•	·	•	●	●	●
Content OSNs	Content sharing	•	•	●	●	●	•	•	●	●
	Resource recommendation	●	·	•	●	●	●	•	●	●
	Advice sharing	●	•	●	•	•	•	●	●	●
	Hobbies / entertainment	•	•	●	•	•	•	●	●	●
	"News" sharing	•	•	●	●	•	•	•	●	●

Figura 1. Tipos de dados encontrados em diferentes tipos de redes sociais [6], sendo que quão maior for o círculo indicado, maior será a correlação entre os tipos mencionados.

Observando a figura 1, pode-se determinar a correlação entre os tipos de dados mencionados previamente e algumas classificações das redes sociais, estas que servem para estruturar a análise a ser feita na questão da privacidade nesses meios e especificar possíveis funcionalidades. Além disso, a ordem das informações da tabela (em inglês) segue a mesma apresentada nas descrições.

Redes sociais de conexão focam na interação entre os utilizadores destas, provendo listas de contato, vias de conversa ou sistemas de combinação. Abaixo seguem as subdivisões correspondentes:

- Encontros: procura ajudar os usuários a encontrar pares românticos, possuindo credenciais e um perfil, com as conexões sendo estabelecidas procurando um potencial romance ou amizade para iniciar uma troca de mensagens (mantidas privadas entre os envolvidos), sendo que grupos também podem existir e o sistema é baseado em navegação, pesquisa e recomendação (podendo utilizar fatores comportamentais para melhora).
- Negócio: almejam providenciar contatos úteis para profissionais. Nem sempre necessitam de credenciais quando se restringir a pesquisas, mas quando possuem tal fator geralmente associam a um perfil que possui a área de trabalho, as experiências nesta e as formas de contato (como por mensagens). Em alguns casos há a possibilidade de adicionar outros usuários da mesma área.
- Reafirmação de relacionamentos já firmados: não busca estabelecer novas amizades, mas reconectar pessoas conhecidas. Por exemplo, há redes que focam em família, colegas de emprego ou da escola.
- Socialização: modo mais tradicional, no qual pode-se conectar com novas ou antigas amizades. O retorno financeiro vem de propagandas e venda de informações (em alguns casos até de inscrições para funcionalidades adicionais).
- Chat/mensagem instantânea: contém uma lista de amigos e um perfil para se conectar por chats com os demais (em diversos casos por meio de vídeo).

As redes sociais de conteúdo, por outro lado, se destacam no que é providenciado ou relativo aos usuários, podendo ser de teor informativo, notícias, conselhos ou multimídia. Sendo que as interações são feitas por meio de pesquisas e câmbio de mídias. Dividem-se nas categorias abaixo:

- Compartilhamento de conteúdo: pode ocorrer dentro de um grupo ou para um público mais abrangente, geralmente sendo multimídia e, em diversos casos, de tamanho incapaz de ser enviado por meios como o e-mail. Normalmente, o usuário deve estar logado para essas funcionalidades (dependendo do caso, apenas para envio, mas sendo comum também para visualização). Mensagens e tags podem estar associadas, podendo ser inclusive uma parte integral disso.
- Recomendação de recursos: usualmente profissional, atua pelo aconselhamento de conteúdos e mecanismos, associado a links, tags e avaliações, sem criação ou envio de um objeto efetivo.
- Compartilhamento de conselhos: local para partilhar experiências e conhecimentos ou procurar ajuda em uma área específica.
- Hobbies/entretenimento: audiência com interesses similares, envolvendo o envio de arquivos multimídia e recomendações de compartilhamento. Dessa forma, possui um apelo específico e um público homogêneo, com o retorno financeiro advindo de propagandas, vendas diretas ou inscrições.
- Compartilhamento de notícias: usado especialmente para disseminar opiniões e experiências, num contexto similar a blogs.

Arquiteturas de uma Rede Social

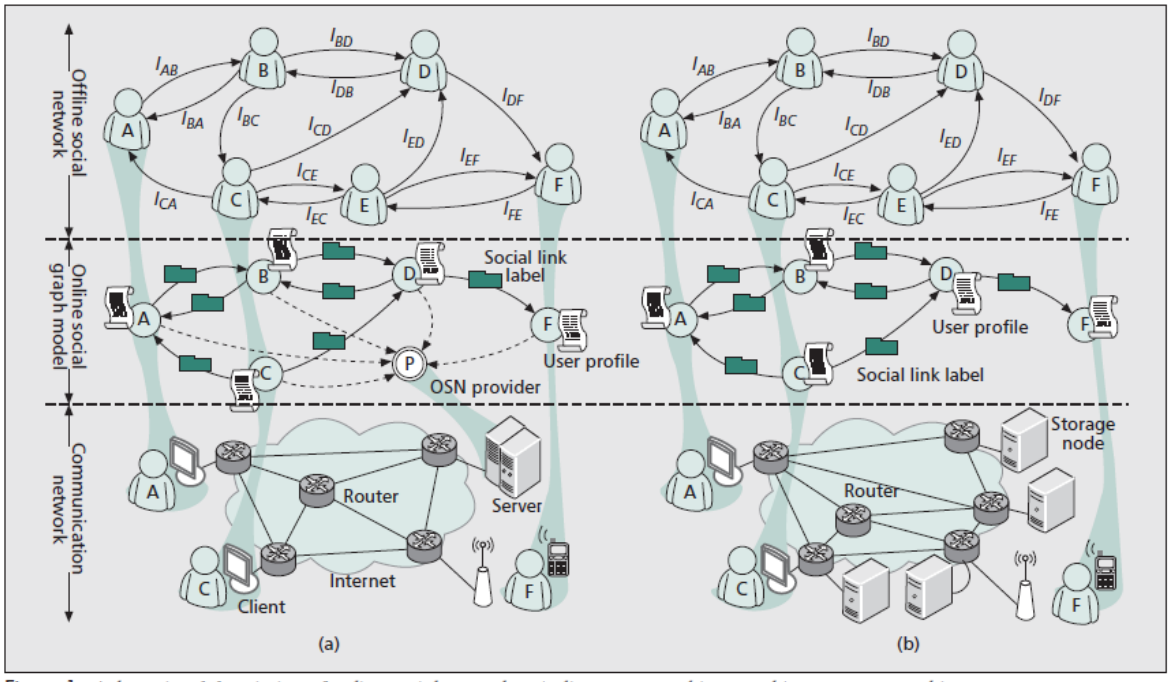


Figura 2. Uma descrição de distintos sistemas de redes sociais [2]:

a) arquitetura cliente-servidor, b) arquitetura P2P.

Procurando uma base mais técnica para auxiliar na análise proposta, é importante saber que os sistemas online de redes sociais são centralizados na ligação entre servidor e web (Figura 2.a), com todas as funcionalidades de armazenamento, manutenção e acesso dependentes do provedor comercial. Esse modelo traz a vantagem de ser mais direto e de fácil implementação, mas sofre de inconvenientes como de ser um único ponto de falha, um gargalo na performance ou um alvo para ataques de negação de serviço (DoS).

Em contraponto, existe uma forte tendência ao desenvolvimento da arquitetura P2P [16] para a próxima geração desses sistemas (Figura 2.b). Com isso, seria adotado um padrão descentralizado dependente da cooperação entre partes independentes que também são utilizadoras da rede. Assim, espaços pessoais são armazenados e mantidos de modo distribuído, possibilitando aproveitar-se da proximidade do suporte de serviços locais, inclusive quando não há acesso à internet disponível.

Requisitos para as Redes Sociais

Primordialmente, há alguns requisitos pressupostos na maioria das redes sociais, funcionando como um contrato entre o fornecedor e o usuário [2] e servindo como um meio de entender os desafios que permeiam a proteção e a privacidade dos utilizadores em contraponto a usabilidade, as dificuldades de implementação e os custos viáveis.

- Confidencialidade: um dos supremos de maior importância, em vista que divulgações ilegais e o uso impróprio das informações privadas de um usuário são indesejadas e podem ser prejudiciais para a vida dos envolvidos.
    - Anonimato: em casos como o do Facebook não é um fator inerente, já que é encorajada a conexão com outros usuários já familiares. Entretanto, em redes para encontro, procura-se proteger a identidade dos usuários com o uso de pseudônimos ou divulgando apenas o primeiro nome. Por outro lado, em todos os casos é essencial é desassociação dos dados salvos em relação ao usuário, evitando o comprometimento desses.
    - Espaço privado: de modo padrão, são envoltos a mecanismos de pesquisa e são visíveis publicamente, mas podem existir restrições como só amigos ou pessoas dentro de uma mesma rede de amizades poderem visualizar o perfil completo (ou parcial). Sendo que a mesma ideia se aplica para o acesso à lista de amizades de cada usuário.

    - Privacidade na comunicação: além dos dados do espaço digital do usuário, a rede social pode acessar informações como o horário e a duração de conexões, o endereço IP associado (identificação do dispositivo), outros usuários que tenham visto o perfil, mensagens enviadas e recebidas, dentre outros. Ademais, supõe-se que entidades não autorizadas não possam ter acesso a essas informações, especialmente se identificarem os usuários, relacionando ao anonimato e a ideia de controle de acesso (que deve ser especificado pelo usuário e em partes manejáveis). Com isso, os dados armazenados ou transmitidos devem parecer aleatórios e não capacitarem vazamento de informação útil.
- Autenticação e integridade: mesmo com exceções, as redes sociais tendem a dar maior suporte a relações já existentes, sendo assim uma representação digital desse convívio. Dessa forma, pode ser modelado como um grafo social online, este que deve manter a consistência dos dados e ter como princípio que qualquer desvio é uma forma de ataque que deve ser detectada e corrigida com os mecanismos apropriados. Os ataques se dividem em: forja de identidade e nós (dos grafos) ou de ligações sociais e conexões. Sendo um exemplo disso a criação de perfis falsos, identificando-se como outrem, o que diminui a reputação do sistema como um todo e causa a necessidade de alguma forma de legitimação e autenticidade.
- Disponibilidade: conteúdo tem que se manter disponível de forma contínua.
- Prestação de contas: más condutas devem ser rastreáveis e ter resposta efetiva para cada tipo de adversário.
    - Ataques internos: aparência de usuário legítimo, mas que atua de modo malicioso. Sendo tanto usuários quanto aplicações terceirizadas ou alguém com acesso à infraestrutura.
    - Ataque exterior ou invasores: um participante ilegítimo que pode perpetrar ataques no sistema ou na infraestrutura deste.

Privacidade

Conforme há a necessidade de revelar certas informações para acessar algumas funcionalidades, existe uma proporção entre a privacidade do usuário e o funcionamento da rede social. Para analisar essa questão, encontra-se um primeiro fator: a definição de privacidade.

De acordo com a Força Tarefa de Infraestrutura da Informação (IITF, privacidade da informação consiste na [8] “revindicação de um indivíduo para controlar os termos em que informações pessoais – que identifiquem o indivíduo – são adquiridas, divulgadas ou utilizadas”. Esse conceito se relaciona a noção de confidencialidade, o sigilo ou a divulgação de peças individuais de informação, mas também considera a pessoa que é sujeito de tal informação, os efeitos da divulgação sobre esta e o controle e consentimento associados.

Dessa forma, observa-se que os usuários têm um escopo em mente e a informação deve ser mantida no âmbito pretendido. Mais especificamente, o escopo é definido [6] pelo tamanho da audiência, a extensão permitida de uso e a duração, com uma violação ocorrendo com a falácia de qualquer uma das fronteiras mencionados, de forma acidental ou maliciosa. Ou seja, os limites da divulgação (caminho entre privado e público), da identidade (representação própria para audiências específicas) e do tempo (gerenciar ações passados com expectativas futuras).

Toda informação carregada para uma rede social é considerada dado pessoal, definido [9] como dados que relacionem a um indivíduo vivo, podendo identificá-lo diretamente a partir deles ou por outras informações em posse de quem controla esses dados. Ademais, a privacidade seria mantida [10] pela limitação do conjunto de dados, esconder identidades e restrições de acesso, mesmo que haja uma dificuldade progressiva com a quantidade de informação que é disponibilizada online.

Redes sociais têm aumentado as possibilidades de controle aparente, modificando a visibilidade para determinados indivíduos ou podendo categorizar amigos para ter acesso a determinadas informações. Esse controle é feito de forma simples e bruta, tendo em vista que, se for feita de forma detalhada, usuários podem ter dificuldade e configurar incorretamente ou ignorar as possibilidades, sem resolver questões da proteção da privacidade. Sendo que esse fator já foi verificado [11] com os usuários tendendo a não mudar as configurações padrões de privacidade providas pela rede social e, assim, divulgando uma grande porção das informações do seu perfil ao confiar implicitamente no sistema.

Outro elemento ainda é a capacidade dos provedores do serviço terem acesso a todos os dados presentes no sistema, incluindo envios privados, comportamento de buscas, mensagens e endereços IP de acesso. Sendo que ele também decide o que será armazenado, o período para isso, como será usado e distribuído e quais ferramentas serão fornecidas ao usuário nesse mérito. Em suma, isso torna imprescindível a confiança do usuário com o fornecedor, especialmente considerando os termos de serviço, nos quais, em geral, consta a licença para domínio completo dos dados, sem a preocupação de direitos autorais e demais reivindicações. Sendo que se torna especialmente preocupante ao considerar que uma das principais receitas são as vendas para terceiros e propaganda direcionada. Como exemplo, segue a declaração de direitos e responsabilidades do Facebook [12]:

"Você é proprietário de todas as informações e conteúdos que publica no Facebook e pode controlar o modo como serão compartilhados por meio de suas configurações de privacidade e de aplicativos. Além disso:

1. Para conteúdos protegidos por leis de direitos de propriedade intelectual, como fotos e vídeos (conteúdo IP), você nos concede especificamente a seguinte permissão, sujeita às suas configurações de privacidade e de aplicativos: você nos concede uma licença global não exclusiva, transferível, sublicenciável, livre de royalties para usar qualquer conteúdo IP publicado por você ou associado ao Facebook (Licença IP). Essa Licença IP termina quando você exclui seu conteúdo IP ou sua conta, exceto quando seu conteúdo é compartilhado com outras pessoas e este não é excluído por elas. [...]"

Ainda sobre esse tópico, é capaz de especificá-lo dentre os problemas expostos abaixo:

- Retenção de dados: remoção de uma informação já compartilhada pode encontrar dificuldades intencionais, com o sistema escondendo ou prevenindo tais ações. Isso pode ocorrer em casos como o do Facebook prevenir a deleção de um perfil [13], já que parte de seu retorno financeiro vem do número de usuários e dados de venda relacionados. Além disso, dados tendem a ser replicados, por compartilhamentos ou armazenamento local, referenciados, por tags, ou residir de forma desassociada, como por backups realizados pelo provedor, violando a fronteira da temporalidade.
- Funcionários da Rede Social: maliciosamente, podem encontrar formas de acesso a dados supostamente privados.

- Venda de informação: há um potencial interesse para propósitos mercadológicos, desde preferências e comportamentos a conexões. Mesmo que o façam de forma anônima, separando o dado do usuário, a identificação é um perigo que não pode ser ignorado.
- Marketing direcionado: diversas informações podem ser combinadas para organizar e explorar métodos de propaganda para usuários direcionados. Sendo, como as mencionadas anteriormente, um conflito envolvendo a confiança com o provedor e seus propósitos.

Outra preocupação é da invasão por outros usuários, de modo deliberado pelas outras partes ou acidental por erro na gerência das próprias configurações de privacidade. Pode-se subdividir em méritos como:

- Acesso de informação por estranhos: devido a falhas no design do serviço provido ou falta de conhecimento ou atenção do usuário sobre o controle a ele fornecido. Relaciona-se a perfis, conexões, mensagens, multimídia, tags, dentre outros fatores na fronteira da divulgação.
- Incapacidade de esconder informação de usuários específicos: associado à fronteira da identidade ao não haver o controle de certas ações.
- Compartilhamento de informações próprias por outros usuários: divulgando mensagens trocadas anteriormente ou informações que não pretende que sejam de conhecimento público, porém sem o usuário ter controle sobre as atividades alheias.

← Privacy concerns	Data types →	Profiles	Connections	Messages	Multi-media	Tags	Preferences/ratings	Groups	Behavioral information	Login credentials
User related	Stranger views private info	●	●	●	●	•	●	●	•	·
	Unable to hide info from specific friend / group	●	●	●	●	•	·	·	·	·
	Other users posting information about you	·	·	●	●	●	·	·	·	·
Provider related	Data retention issues	●	●	●	●	●	●	●	●	·
	OSN employee browsing private info	●	●	●	●	●	●	●	●	•
	Selling of data	●	●	●	●	·	●	·	●	·
	Targeted marketing	●	·	·	·	·	●	·	●	·

Figura 3. Questões de privacidade em redes sociais para o usuário e os fornecedores comparando com os tipos de dados associados [6], sendo que quão maior for o círculo indicado, maior será a correlação entre os campos mencionados.

Conforme visto, existem distintas necessidades de proteção [7]. Em primeira instância, há a questão de proteção contra usuários, podendo ser:

- Diretamente conectados: possuindo alguma associação no grafo de conexões com o usuário alvo.
- Indiretamente conectados ou sem conexão.
- Público geral.

Ainda é capaz de ser em relação ao próprio provedor ou a propagandas e aplicações, com terceiros desenvolvendo códigos que acessem um conjunto de funções da rede e disponham de informações determinadas por estes, relativo a venda de dados. Essa diferenciação precisa ser feita para desenvolver respostas apropriadas e associar corretamente com os méritos de privacidade previamente mencionados.

Em suma, conforme as redes sociais contem uma quantidade considerável de informações úteis a cerca de seus usuários, estas tornam-se alvo de interesse por terceiros, tanto em questões privadas quanto comerciais. Sendo que isso relaciona os distintos interesses dos integrantes de uma rede com o provedor desta e coloca em foco o balanço entre o que é eficiente e o que fornece a proteção requisitada pelo usuário.

Ameaças

As ameaças iniciam no âmbito da privacidade, com a anonimidade e a identidade do usuário e o vazamento de informações do perfil, conforme visto anteriormente. Em complemento, os ataques podem vir na forma de “desanonimização” e por vizinhança [17], com o primeiro focando inicialmente em um grupo, para então atingir usuários específicos através do histórico de buscas e as atividades relacionadas por este em redes sociais, e o segundo sendo feito a partir das conexões de um usuário.

Ainda sobre ameaças à privacidade, a dispersão de dados pode partir de configurações de privacidade mal administradas e por invasão de terceiros, arquivos multimídia podem ser associadas por tags a um perfil, sem que o usuário tenha essa pretensão, e dados podem ser difíceis de serem totalmente removidos, com o usuário perdendo controle sobre eles. Outra questão preocupante é a de novas tecnologias [18] que fazem comparações para determinar a localidade a partir de uma imagem, por exemplo. Ou seja, mesmo que o usuário tenha o cuidado de não revelar onde se encontra (algo que muitos tendem a fazer), já existem métodos de dedução como a Recuperação de Imagem Baseada no Conteúdo (CBIR), podendo levar a casos de perseguição.

Na questão do roubo de identidade, pode ocorrer o “pishing”, revelando informações sensíveis como senhas e contas bancárias ao se aproveitar de limiares baixos de confiança em redes e ataques que permitam a injeção automática de links para tal propósito. O alastramento é uma das maiores preocupações, desde computadores que são invadidos a informações vazadas que possibilitem formar links que enganem o usuário. Assim, o vazamento se mostra como outro fator intrínseco, pois, além do que foi mencionado, possibilita gerar constrangimento, chantagem e até ferir a imagem de alguém, inclusive com o uso das informações (especialmente de imagens nas quais haja reconhecimento facial) para personificação entre redes sociais distintas ou em uma mesma, com usuários clonados.

Com relevância maior ao sistema desenvolvido pelo provedor, existem vulnerabilidades como o “spam”, as quais trazem riscos como sobrecarga de tráfico, perda de confiança ou dificuldade de uso da aplicação, até mesmo divergindo para sites indesejados. Ainda há ataques de “cross-site scripting” (XXS – que explora fraquezas e pode trespassar políticas de controle de acesso), vírus (softwares maliciosos) e “worms” (programas autorreplicantes, sem precisar de um programa hospedeiro para se alastrar), podendo advir de ferramentas pouco verificadas de terceiros. Os riscos referentes a esses ataques são diversos, como o comprometimento de contas, abrir caminho para o “pishing”, espalhar conteúdo não solicitado e causar a negação de serviços.

Por fim, existem as ameaças sociais, assim como a espionagem corporativa, com o perigo da perda de propriedade intelectual e que algum “hacker” cause danos ou faça chantagem aos funcionários para revelar informações ou para acessar propriedades. Ademais, usuários podem ser perseguidos ao revelar informações de localidade, cronograma, endereço, dentre outros. Com isso, sua integridade, até mesmo física e psicológica, pode ser comprometida.

Conflitos de design

Acabam por ser inerentes às redes sociais alguns conflitos de design [2] existentes entre os objetivos de proteção e privacidade em contraponto a usabilidade e sociabilidade previstas.

Em primeiro ponto há o suporte para busca de conexões (exploração do espaço virtual) e a divulgação de informações dos perfis dos usuários e correspondentes listas de contato. No caso, para haver pesquisas eficientes e precisas é necessária a disponibilidade de dados pessoais, ainda que isso aumente a possibilidade de violações de privacidade.

Sobre a privacidade, ainda há o fator de dispor certas informações para conexões de específicos âmbitos. Isso faz com que um dado, que tenha como alvo apenas um grupo de amigos, possa ser acessado indiretamente por alguém desconhecido pelo usuário, mas que tenha alguma conexão em comum. Por exemplo, interesses pessoais, locais frequentados e atividades praticadas podem ser deduzidas a partir de outros perfis ao atribuir similaridades do usuário alvo com suas conexões. Ainda assim, esse fator pode ser usado para auxiliar o sistema da rede, sinalizando ou fornecendo maior nível de confiança para usuários que tenham proximidade em um grafo social, baseado nas conexões estabelecidas.

As interações sociais, mesmo que o cerne das redes sociais, também trazem outro fator: um usuário pode inadvertidamente divulgar informações que outro pretende manter como privada ou relacionar um conteúdo já compartilhado, mas não identificado, ao seu autor. No caso, não se pode ter controle sobre a ação de todos os outros membros de uma rede, então esses podem ter ações que prejudiquem outros, pretensiosamente ou não.

Desconsiderando os fatores de sociabilização, existem outros que podem violar a privacidade, como a mineração de dados. Ou seja, os dados armazenados pela rede podem prover um material para análises de marketing ou até da evolução de colaborações e da comunicação. Como também permitem uma melhora no serviço, otimizando e customizando de acordo com preferências e interesses. De qualquer forma, há a possibilidade de associação desses dados a sua origem, aumentando a importância de procedimentos para tornar um usuário anônimo e causando uma ruptura entre a qualidade dos resultados da mineração e os requisitos de privacidade.

Por um lado mais técnico, um último conflito é o comparativo entre as distintas arquiteturas, cliente-servidor e P2P. A primeira tem vantagens para alcançar os objetivos das redes sociais, como os usuários não estarem restringidos a interações com amigos já existentes e serem capazes de restabelecer conexões perdidas por meio de uma mineração mais eficiente. Assim, pelos grafos de conexões, um repositório central pode facilitar a exposição de um determinado usuário procurado por interesses, localidades ou grupos em comum. Entretanto, o armazenamento dos dados fornecidos, de modo direto ou indireto, é permanente nos bancos de dados do provedor, abarcando uma potencial exploração que pode violar a privacidade.

Capacitar o controle dos dados ao usuário e não ter uma única entidade com acesso a todos os dados pessoais pode ser benéfica [14]. Em uma arquitetura P2P, a privacidade é fortalecida ao retirar o repositório central e possibilitar que o usuário se responsabilize pelo cumprimento do controle de acesso e encripte seus próprios dados. Sendo que com o modelo cliente-servidor, o provedor poderia proibir que o usuário encriptasse seus dados ao recusar certos serviços, especialmente considerando que os termos são mutáveis, e seria capaz de inferir relações entre os usuários através de dados correlacionados ou endereços IP.

Dessa forma, uma arquitetura P2P combinada com um esquema apropriado de encriptação pode fornecer uma melhor proteção na questão da privacidade em redes sociais [19]. Ainda assim, há a dificuldade de recriar eficientemente todas as funcionalidades das redes sociais em um modelo descentralizado e de como encorajar a cooperação entre usuários para coletar grafos de interação social, mantendo a privacidade esperada.

Caminhos de pesquisa

Eliminar conflitos entre os distintos objetivos das redes sociais abre caminho para exploração, em vista das dificuldades encontradas. Além dos já citados conflitos de design, existem outros âmbitos para desenvolver pesquisas, um exemplo disso é a capacidade que essas redes têm para formular um grafo das conexões estabelecidas, já que tendem a simplificar usuários como sendo ou não amigos [5], o que de fato não traz todas as complexidades de amizades humanas e contrapõe com o princípio da consistência entre a vida real e a virtual de um usuário.

Para contornar o problema citado, a modelagem do grafo pode ser feita a partir de tipos de relações (tanto bidirecionais – como colegas – quanto unidirecionais – como seguidores), da quantificação da confiança entre as partes (em contexto geral ou em tópicos específicos) e da intensidade das interações. Esse detalhamento também pode melhorar a determinação da privacidade, articulando de forma clara e tratando decisões a cerca do assunto com precisão, especialmente ao diferenciar usuários de uma forma não binária. Todavia, precisa de cuidado com a acurácia em vista da complexidade em descrever relações sociais e deve-se analisar o custo-benefício entre a praticidade do desenvolvimento e possíveis ambiguidades do resultado.

A proteção desses grafos, assim, deve ser de primordial importância e eles podem ser usados para esse propósito. Por exemplo, uma conexão é capaz de ser forjada por um usuário malicioso ao fazer um outro confiar nele, porém introduzir a confiança e a intensidade de interação pode limitar os efeitos desse forjamento. Além disso, se um usuário malicioso falsificar sua identidade, há a possibilidade das próprias conexões o identificarem como falso. No caso, conforme as redes sociais tendem a ser uma extensão dar relações fora do âmbito virtual, sua posição nesse contexto que determina sua identidade [15]. Pode ser simples se cadastrar com um nome falso, mas é difícil formar e mudar contatos, verificando assim o nível de confiança para distintos usuários a partir de fatores qualitativos.

Conforme o tipo de acesso difere entre usuários e provedores, o desenvolvimento de mecanismo de defesa específicos também se torna necessário, com pesquisas que procuram mitigar os problemas supracitados. Para proteger os dados de um usuário de outros, ferramentas apropriadas e divulgação para maior consciência do assunto e reforçar políticas de acesso se tornam centrais [6]. Sendo que isso não considera provedores com os quais não se tem confiança, mas formas de esconder dados sensíveis as empresas responsáveis ou retirá-los totalmente do quadro, como visto com a descentralização proposta pela arquitetura P2P.

Ademais, outros campos que precisam ser explorados pelas desenvolvedoras das redes sociais são: a encriptação (envolvendo a gestão das chaves, o custo de operação e o obstáculo da escalabilidade) e a "anonimização", separando a informação divulgada do indivíduo (tornando incapaz de identificá-lo e preservando a estrutura dos dados) e, assim como visto anteriormente, proteger contra a identificação. Isso é possível ao misturar atributos ou modificar a estrutura do grafo para dificultar o caminho inverso, sendo a maior dificuldade determinar como podem associar os dados para alcançar objetivos escusos.

Conclusão

Com o uso expansivo das redes sociais e a variedade de propósitos propostos por elas, cresce a necessidade de classificação e determinação do que é suposto como requisito entre os usuários e os provedores. A partir disso, torna-se praticável distinguir quais são as necessidades específicas, especialmente no comparativo entre a privacidade dos conteúdos compartilhados e os objetivos de socialização pretendidos, associando com isso os dados que podem ser comprometidos e as medidas cabíveis.

As redes sociais trazem novos artifícios para interação e comunicação, porém aumentam preocupações no quesito da privacidade. Sendo uma das tecnologias que teve maior fama recentemente, torna-se um alvo para um marketing inescrupuloso, ataques no âmbito privado, dispersão de softwares maliciosos e uso indevido de dados pessoais.

Considerando a complexidade desses sistemas, os problemas de privacidade são inúmeros. O simples fato da confiança que se deve ter com o provedor não ser algo justificável já mostra a complicação referente as expectativas do usuário em proteger seu perfil com as ferramentas que lhe são fornecidas em contraponto ao projeto destas ser desenvolvido por partes que não tem as mesmas metas de privacidade. Por conseguinte, mesmo que estejam protegidos de outros usuários, o fornecedor pode utilizar indevidamente os dados armazenados por ele.

Diversas áreas de pesquisa podem ajudar, desde questões mais técnicas, como o design de sistemas e a criptografia, a fatores sociológicos e do direito. Ainda assim devem focalizar em proteger a privacidade de forma incorporada ao sistema, sem prejudicar demais operações e propósitos ou sobrecarregar tarefas para os usuários e até mesmo os provedores. Por fim, a questão principal não é tratar o problema como um único fator, mas desenvolver soluções em áreas separadas que sejam, então, reunidas.

Bibliografia

[1] Wüest, Candid. “The Risks of Social Networking” Symantec Security Response, 2010.

[2] Zhang, Chi. Sun, Jinyuan. Zhu, Xiaoyan. Fang, Yuguang. **“**Privacy and Security for Online Social Networks: Challenges and Opportunities” IEEE Network, 2010.

[3] Kancheti, Vamshi. “Security Analysis of Social Networks” Master Graduate Project Report for the Faculty of the Department of Computing Sciences Texas A&M University-Corpus Christi, 2010.

[4] Cutillo, Leucio. “Security and privacy in online social networks” TelecomParisTech, 2014.

[5] Boyd, Danah. Ellison, Nicole. “Social Network Sites: Definition, History, and Scholarship” Journal of Computer-Mediated Communication, 2008.

[6] Beye, Michael. Jeckmans, Arjan. Erkin, Zekeriya. Hartel, Pieter. Lagendijk, Reginal. Tang, Qiang. “Privacy in Online Social Networks”. 2010.

[7] Novak, Ed. Li, Qun. “A Survey of Security and Privacy in Online Social Networks” Department of Computer Science The College of William and Mary, 2012.

[8] Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information. Acesso em: 19/06/2016 às 15:30. Disponível em: https://aspe.hhs.gov/legacy-page/niiprivacy-principles-june-6-1995-142711

[9] UK Parliament. Data protection act 1998, 1998. Acesso em: 23/06/2016 à 19:20. Disponível em: http://www.legislation.gov.uk/ukpga/1998/29/contents.

[10] Weiss, Stefan. "The need for a paradigm shift in addressing privacy risks in social networking applications". In The Future of Identity in the Information Society, volume 262, 161–171. IFIP International Federation for Information Processing, 2008.

[11] Gross, Ralph. Acquisti, Alessandro. "Information revelation and privacy in online social networks". In WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society, 71–80, 2005.

[12] Facebook.com. Statement of rights and responsibilities. Acesso em: 24/06/2016 à 16:00. Disponível em: http://www.facebook.com/terms.php.

[13] Paul MacNamara. Facebook blocks web 2.0 suicide machine'. Acesso em: 24/06/2016 às 19:20. Disponível em: http://www.networkworld.com/news/2010/010410-buzzblog-facebook-blocks-suicide-machine.html.

[14] Anderson, Jonathan. Daz, Claudia. Bonneau, Joseph. Stajano, Frank. "Privacy-enabling social networking over untrusted networks". Jon Crowcroft and Balachander Krishnamurthy, editors, WOSN, 1–6, 2009.

[15] G. Mezzour, "Privacy-Preserving Relationship Path Discovery in Social Networks" Proc. CANS '09, Ishikawa, Japan, 2009.

[16] S. Buchegger, "A Case for P2P Infrastructure for Social Networks — Opportunities and Challenges" Proc. WONS '09, Snowbird, UT, 2009.

[17] Gunatilaka, Dolvara. "A Survey of Privacy and Security Issues in Social Networks". 2011.

[18] Al Hasib, Abdullah. "Threats of Online Social Networks". Helsinki univesity of Technology, 2008.

[19] Bodriagov, Oleksandr. "Social Networks and Privacy". Licentiate Thesis. Sotckholm, Sweden, 2015.