Segurança e Privacidade: Proteção e tratamento de dados nos aplicativos de redes sociais

Paulo Teruo Izumi[1], Daiane Mastrangelo Tomazeti[2]

Curso Superior em Tecnologia em Análise e Desenvolvimento de Sistemas - Instituto Federal de São Paulo - Campus Hortolândia (IFSP)

[1]pauloizumi@outlook.com, [2]daianetomazeti@ifsp.edu.br

Abstract. *Due to the increase of users in social networks, the amount of information and data are rising. All websites could be the target of crackers or bad people. Furthermore, websites that contain personal information from your users, due to that, it's been necessary to perform the data's protection, keeping privacy and integrity. This paper proposes to perform a study about data's protection on chat apps and an analysis regarding the today's scenario around the treatment of this kind of information.*

Resumo. Com o aumento do número de usuários utilizando as redes sociais, a quantidade de dados e informações que circulam nelas também cresceu. Qualquer tipo de *site* pode ser alvo de *crackers*[1] e pessoas má intencionadas, ainda mais *sites* onde reúnem inúmeras informações pessoais de seus usuários. Com isso, se faz necessário fazer a proteção, manter a privacidade e a integridade desses dados. Este trabalho tem como objetivo fazer um estudo acerca da proteção dos dados que circulam nos aplicativos de conversa nas redes sociais e fazer um levantamento de qual é o cenário atual em relação ao tratamento desse tipo de informação, ou seja, foi criado um questionário e analisado os dados coletados com o qual teremos dados reais para concluir o nosso estudo.

1. Introdução

Com a popularização da Internet, o número de usuários vem crescendo constantemente. Segundo um levantamento feito pelas empresas *We Are Social* e *Hootsuite*, que são empresas voltadas à questões de redes sociais, revelou-se que cerca de 66% da população brasileira está conectada nas redes sociais, outra pesquisa feita pelas mesmas empresas, levando em conta dados de diversas fontes, mostra que o Brasil fica em segundo lugar na questão de tempo conectado na Internet por qualquer tipo de dispositivo, o que corresponde cerca de nove horas conectados à Internet (TECHTUDO, 2018).

Assim como podemos identificar na Figura 1, dentro dessas nove horas diárias gastas na Internet, cerca de três horas e meia são dedicadas exclusivamente ao acesso das redes sociais. O

[1] Crackers são pessoas aficionadas por informática que utilizam seu grande conhecimento na área para quebrar códigos de segurança, senhas de acesso a redes e códigos de programas com fins criminosos. Em alguns casos, o termo "Pirata Virtual" é usado como sinônimo para cracker (WIKIPEDIA, 2019).

número de pessoas acessando-as vem crescendo a cada ano. Cerca de 1 milhão de pessoas começaram a usar as redes sociais em 2017, o que significa um novo usuário a cada 11 segundos (TECHTUDO, 2018).

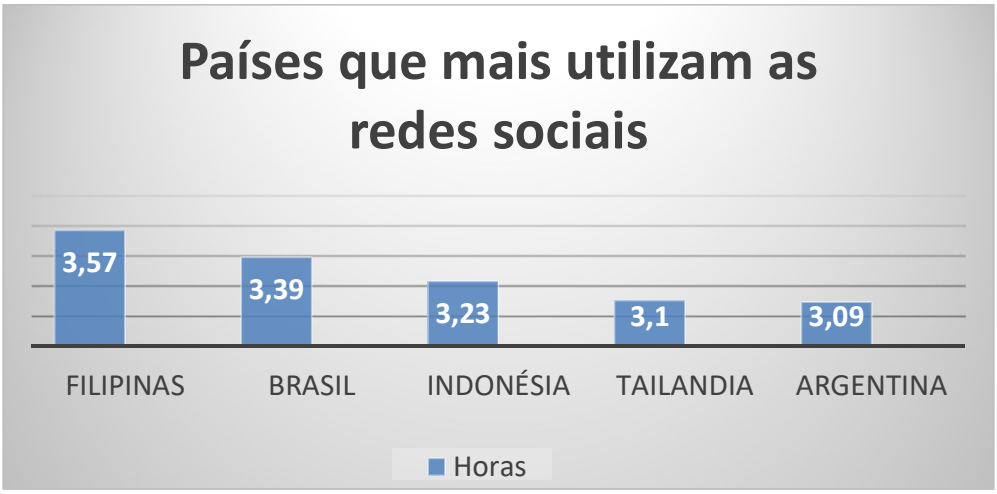


Figura 1 - Brasil se encontra em segundo lugar na questão de tempo dedicadas às redes sociais.

Fonte: Gráfico desenvolvido com referência aos dados divulgados por *We Are Social* e *Hootsuite*.

Com o rápido crescimento de usuários nas redes sociais, a quantidade de dados e informações que circulam nelas aumentou, desde simples nomes inteiros ao número de contas em bancos, ou seja, todo tipo de informação que é compartilhado, sendo em conversas privadas ou até em *posts* públicos que qualquer usuário possa ver, faz com que sejam informações que possam ser usadas contra os seus proprietários.

Em um mundo que há o compartilhamento de grandes quantidades de dados pessoais, se faz necessário a questão de segurança e privacidade dos dados, sendo fundamental entender quem é responsável por manter esses tipos de dados seguros, se as redes sociais possuem permissão de seus usuários para utilizá-los em seus negócios ou até que ponto podem compartilhá-los.

Para abordagem da proposta, este artigo está dividido em sete seções, sendo a introdução, os objetivos do trabalho, a problemática e a justificativa, a metodologia, seguindo os métodos utilizados para fazer este trabalho, o referencial teórico, que tem como objetivo fornecer aos leitores conhecimento sobre alguns conceitos; o levantamento, a coleta e a análise dos dados, por fim as considerações finais e as referências usadas conforme o desenvolvimento.

2. Objetivos

2.1 Objetivos Gerais

Fazer o levantamento e a análise de qual é o cenário atual nas questões de compartilhamento de informações e o que é feito para fazer a proteção desses dados que trafegam nos seus aplicativos de bate-papo.

Com esse estudo poderemos ter uma ideia de como as redes sociais fazem o tratamento e proteção de informações que são inseridas pelos seus usuários nos aplicativos de conversas.

2.2 Objetivos Específicos

- Verificar como as redes sociais como o *Facebook*[2], *Twitter*[3] e o Google+ cuidam dos dados inseridos;
- Identificar quais as redes sociais que já tiveram os dados vazados;
- Quais as possíveis causas dos vazamentos de dados;
- Desenvolvimento de um questionário a respeito do compartilhamento de dados nas redes sociais, bem como a análise e o desenvolvimento de gráficos a partir dos dados obtidos;
- Quais ferramentas estão disponíveis no mercado para auxiliar no processo de segurança quanto ao acesso e manuseio dos aplicativos;
- Sugestões e boas práticas para o uso/navegação nas redes sociais.

3. Problemática e Justificativa

A escolha deste tema deve-se a grande quantidade de informações que são inseridas nas redes sociais. Com o aumento do número de pessoas que as utilizam, as mesmas estão sujeitas a se tornarem vítimas de pessoas má-intencionadas quando compartilham dados pessoais na rede.

Quando ocorre o vazamento de dados nas redes sociais, todos os seus usuários são afetados, mesmo aqueles que são mais cuidadosos, hoje na era digital, o pouco das informações inseridas pode-se acarretar em sérias consequências para seu dono, como por exemplo: assaltos, sequestros relâmpagos e furtos.

Há diversas notícias e reportagens sobre o vazamento de dados privados nas redes sociais, principalmente nas que são mais utilizadas pela população, isto mostra que todos os seus usuários podem se tornar vítimas de ataques de criminosos sem ao menos terem conhecimento do ocorrido. Mesmo que existam brechas no sistema, não podemos colocar toda a culpa nos responsáveis pelo *site*, uma vez que os seus próprios usuários não se portam de maneira adequada dentro delas.

Podemos dizer que ninguém gostaria de ter seus dados vazados, porém há uma lista de boas práticas que mesmo as pessoas mais leigas podem seguir para evitar que esse tipo de incidente aconteça.

Para poder oferecer uma camada de proteção a mais, as redes sociais estão buscando ferramentas para poderem implementar em suas plataformas, assim ajudando a evitar esse tipo de problema relacionado aos dados.

Devido aos fatos citados anteriormente justifica-se o presente trabalho de modo que fará uma análise da situação e do cenário atual na questão de compartilhamento de dados que são inseridos nos aplicativos de redes sociais.

4. Metodologia

Para realização deste trabalho, foi realizado um estudo bibliográfico acerca de quais redes sociais são mais utilizadas pelo Brasil, qual o tempo médio a população brasileira gasta nelas, uma

[2] www.facebook.com
[3] www.twitter.com

pesquisa em jornais e periódicos sobre a questão de vazamento de dados de seus usuários na redes sociais, como fazem a proteção dos dados que são compartilhados nos bate-papos privados. Buscou-se possíveis melhoramentos que as redes sociais poderiam aderir aos seus sistemas, futuros planos de implementações de criptografias para obter-se uma camada a mais de proteção para seus usuários.

Em um segundo momento, foi desenvolvido um questionário com a utilização da plataforma de formulário da Google, o *Google Forms*, contendo onze perguntas fechadas, todas baseadas nos principais pontos acerca do compartilhamento e vazamento de dados nas redes sociais. Esse questionário ficou disponível durante os meses de abril até junho de 2019, com a participação de cerca de 39% de homens e 61% de mulheres entre 15 a 50 anos de idade, um total de 170 participantes. O questionário foi divulgado no *Facebook* de maneira quantitativa, que a partir dos dados coletados, foi possível a realização dos gráficos.

5. Referencial Teórico

5.1 *Web* 2.0

Web 2.0 é o termo usado para descrever a segunda geração de comunidades e serviços na Internet. Com ela, ficou mais fácil fazer *upload*[4] de informações na Internet sem ter muito conhecimento de códigos fontes ou linguagens de programação. A *Web* 2.0, no início não oferecia muitas ferramentas para facilitar a vida de seus usuários, porém nos dias atuais, ficou simples, rápido e fácil enviar qualquer tipo de informação ou documentos a qualquer um conectado na rede.

A *Web* 2.0 é a segunda geração de serviços *online* e caracteriza-se por potencializar os modos de publicação, compartilhamento e organização de informações, além de ampliar os espaços para a interação entre os participantes do processo. Suas repercussões sociais facilitam o método de compartilhamento, de troca afetiva, de produção e circulação de informações, de construção social de conhecimento apoiada pela informática. (PRIMO, 2007).

5.2 *Software* Social

Softwares Sociais são ferramentas existentes na *web*, desde o início da *Web* 2.0, ou seja, ela como plataforma. Há diversos tipos de *softwares* sociais, mas todos têm o mesmo objetivo, fazer com que o usuário interaja, compartilhe e troque informações e dados cada vez mais com os outros usuários conectados.

Os elementos sociais formam os *softwares* sociais, onde cada um possui a sua particularidade, através desses elementos, eles tomam sua forma. Segundo Smith (2007, Tradução Nossa), assim como ele definiu em suas pesquisas, a Figura 2 mostra que os *softwares* sociais possuem sete elementos, mas isso não quer dizer que eles tenham que possuir todos, pois na maioria das vezes, eles possuem pelo menos três ou até mais destes elementos.

[4] Upload: Envio de arquivos.

Figura 2. Os sete elementos que compõem o software social.

Fonte: *Business Horizons* (Kietzmann, 2011)

Por meio das redes sociais estudadas neste trabalho, no *Facebook*, o foco principal dos elementos sociais utilizados são os relacionamentos, as presenças, as identidades, as conversas e as reputações. Já no *Twitter*, são as identidades, as presenças e os compartilhamentos.

5.3 Redes Sociais

Redes Sociais, como o próprio nome diz, são computadores, usuários conectados, visando o convívio social, a vida social na internet, através de *sites* que utilizam de *softwares* sociais para a interação de usuários.

Segundo Recuero (2009 *apud* Boyd & Ellison (2007)), redes sociais são *sites* que permitem que:

- O usuário construa, possua um perfil ou página pessoal, ou seja, uma identidade social;
- Aconteça à interatividade entre os usuários cadastrados na rede social através de comentários, mensagens;
- E que cada usuário / ator, tenha suas características na rede, para que assim aconteça uma exposição pública da identidade de cada usuário cadastrado.

Portanto uma rede social possui vários perfis de usuários conectados a um *site*, onde estes perfis possuem certa exposição pública, e os usuários praticam a interatividade com amigos ou até pessoas que nunca viram pessoalmente e também compartilham conteúdo, como imagens, músicas, vídeos e etc. Assim o grande objetivo das redes sociais é a aproximação de usuários, estejam eles aqui no Brasil ou no Japão, bastando apenas poucos cliques para que eles interajam.

5.4 Segurança da Informação

A *Web* 2.0 trouxe junto consigo plataformas colaborativas de troca e criação de conteúdo tais como: redes sociais, *blogs*, etc. Com isso, a Internet se tornou um local onde podemos nos reunir com pessoas ao redor do mundo, conversar e trocar informações a respeito de qualquer tipo de assunto.

Com todos utilizando os *blogs* ou redes sociais e trocando informações dentro delas, se tornou necessário pensar na questão de preservação dos dados que trafegam pela rede, como também manter a sua integridade, fazendo com que a proteção de dados seja uma questão essencial no ambiente virtual.

> Este universo de conteúdos e continentes digitais está sujeito a várias formas de ameaças, físicas ou virtuais, que comprometem seriamente a segurança das pessoas e das informações a elas atinentes, bem como das transações que envolvem o complexo usuário-sistema-informação. (MARCIANO, 2006).

Entende-se por informação como um conjunto de dados sobre determinado tipo de assunto com diferentes níveis de importância para determinados grupos de pessoas ou empresas (WHITMAN, 2013).

A Segurança da Informação mostrou-se necessária para fazer a preservação de todos os tipos de informações que circulam nas redes sociais e na Internet e também manter a sua integridade. Segundo Barbosa *et al.* (2012), como esse tipo de informação é muito visado por grande empresas, é fundamental fazer a sua proteção assim como delimitar quem tem acesso a ela.

Segundo Hintzberg (2018), a Figura 3 representa a base da Segurança da Informação (*Confidentiality, Integrity* and *Availability*) na qual é composta no princípio *CIA*: Confidencialidade, Integridade e Disponibilidade.

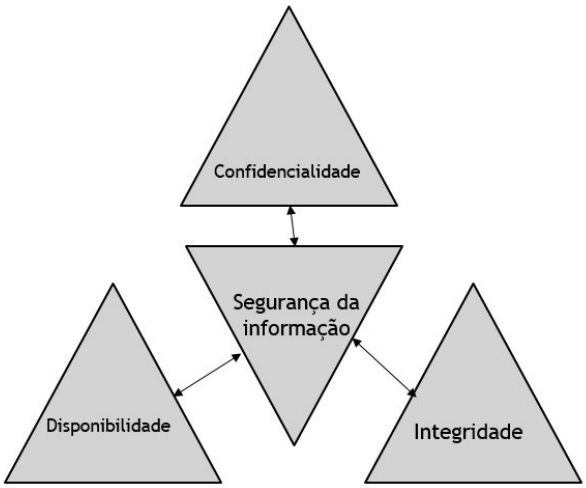


Figura 3. Princípios da Segurança da Informação.

Fonte: Fundamentos da segurança da informação. (Hintzberger, 2018)

Qualquer tipo de ataque abala entre uma, duas ou até mesmo os três princípios da Segurança da Informação.

5.4.1 Confidencialidade

A confidencialidade dos dados significa que apenas as pessoas autorizadas terão acesso aos dados protegidos, mantendo assim as pessoas indesejadas fora do alcance.

Assim como todas as pessoas possuem seus dados privados, manter esse tipo de informação confidencial é uma das características da segurança da informação.

5.4.2 Integridade

A integridade dos dados garante que a informação não tenha sido alterada ou comprometida durante a sua fase de processamento ou de envio.

Assim como na brincadeira do telefone sem fio, durante a fila em que a informação é repassada, pode se ocorrer falhas, mal entendimentos e substituição dos dados, assim a última pessoa da fila pode receber a informação inicial totalmente comprometida, perdendo a sua integridade.

5.4.3 Disponibilidade

Disponibilidade significa assegurar que todas as pessoas autorizadas tenham acesso à informação desejada em um curto período de tempo.

Muitas empresas estão ligadas diretamente à esse pilar, pois empresas que trabalham com dados, se não tiverem acesso as informações necessárias, pode-se acarretar em processos travados, causando assim lentidão e perda em seus lucros.

Segundo Ticiano Benetti (2015), “sem confidencialidade perde-se vantagem competitiva, sem integridade perde-se lucratividade e sem disponibilidade perde-se a capacidade de operar. Isso equivale a dizer que sem segurança da informação, uma empresa tem muito mais dificuldade em crescer, em lucrar e em sobreviver.”

Mais tarde, outros dois princípios foram agregados à base da Segurança da Informação, são eles:

- O não-repudio, garante que caso haja algum tipo de movimentação ou acesso as informações, tenha-se uma prova de que o autor as realizou, tendo assim uma “garantia” que determinada pessoa fez o uso das informações. (TechEnter, 2019).
- Autencidade garante a veracidade do autor da informação, ela não verifica se a informação passada é verdadeira ou falsa, mas sim confirmando quem é o autor das informações que estão sendo processadas (TechEnter, 2019).

5.5 Ameaças, Vulnerabilidades e Ataques

Nas redes sociais, dentre todas as informações que podemos encontrar, os dados pessoais são o principal alvo de ataques dos *crackers*. Dados que para nós podem parecer sem importância, como

datas de nascimento, nomes completos, fotografias, nomes de escolas, etc, nas mãos dos invasores podem-se tornar uma ferramenta contra seus usuários (SANTOS, 2016).

Os dados pessoais também podem ajudar os invasores a acessar contas de e-mail. Hoje os *sites* que utilizam de um sistema de *login* e senha para acessar determinadas contas, possuem um sistema de recuperação de senha, que é composto muita vezes em responder perguntas a respeito da vida pessoal do usuário (MARTELETO, 2018). Se de alguma maneira a informação é divulgada por algum outro meio, o invasor tiver acesso às respostas das perguntas, outros serviços utilizados pelo usuário podem ser comprometidos. O invasor apenas precisa fornecer a resposta correta a respeito da vítima para "comprovar" que é realmente o dono da conta, assim o sistema libera a troca da senha para ter acesso a conta (HAMADA; NASSIF, 2019).

Se os dados que a vítima digitou estiverem corretos, por exemplo, "nome da escola em que estudou" ou "nome de solteiro da mãe", o invasor pode ter acesso à conta do usuário sem precisar conhecê-lo (COSTA *et al*, 2018).

5.6 Redes Sociais que tiveram dados de usuários vazados

5.6.1 Facebook

Segundo investigações que foram feitas pelo jornal americano *The New York Times*, que cerca de 30 milhões de contas de usuários do *Facebook* tiveram seus dados como nome, conversas privadas e preferências vazadas à empresas privadas. (GAUCHAZH,2018).

5.6.2 Google+

Devido a dois incidentes ocorridos em 2018 e 2019, cerca de 50 milhões de usuários da rede social Google+, uma rede social da Google que entrou no mercado para competir com outras redes sociais, devido a um erro em suas *APIs*, tiveram seus dados como profissões, nomes, emails, idade vazados para 38 aplicativos conectados a rede social, ocasionando o seu encerramento para agosto de 2019 (TECHTUDO, 2019).

5.6.3 Twitter

Desenvolvedores do aplicativo do *Twitter* tiveram acesso à conversas privadas e *posts* protegidos onde o seu autor delimita quem pode ter acesso a elas, devido a um bug encontrado na *API* da plataforma. O *site* afirma que o problema pode ter ocorrido devido aos desenvolvedores possuirem as suas assinaturas digitais configuradas para domínios que foram resolvidos para o mesmo *IP*[7] público. Segundo o *Twitter* apenas 1% dos seus 335 milhões de usuários foram afetados (TIINSIDE, 2017).

5.7 Criptografia e Segurança

A criptografia se refere ao processo matemático de tornar uma mensagem impossível de ser lida, é um conjunto de regras que visa fazer a codificação da informação onde apenas o emissor e o receptor consiga ter acesso a elas (Surveillance Self-Defense, 2018).

Quando uma mensagem é enviada a partir de um aplicativo de troca de mensagens, quer dizer que estamos enviando informações de um lugar para outro, isso é chamado de "dados em movimento", significa que a informação sai do dispositivo, passa pelos servidores da empresa

prestadora do serviço até chegar no outro lado que seria o destinatário. Hoje, temos métodos de criptografia que nos auxiliam a fazer a proteção desses dados em movimento: *TLS* (*Transport Layer Security*) que em português seria a segurança na camada de transporte e o ponta-a-ponta.

5.8 Encriptação *Transport Layer Security*

A encriptação *TLS*, faz a proteção das mensagens durante seu trajeto, o remetente faz o envio da mensagem, que é encriptada e transmitida para uma torre de comunicação, que passa pela empresa provedora do serviço, que faz a desencriptação, mantem uma cópia da mensagem e reencripta para que chegue até o destino da mensagem, onde é feito novamente a desencriptação para que possa ter acesso ao conteúdo.

Hoje, é assim que o *Facebook* faz o tratamento das nossas conversas nos aplicativos de bate-papo, sempre mantendo um "histórico" das mensagens com o pretexto de usabilidade, caso precisemos de alguma informação, vai estar lá pois já a enviamos previamente.

Com isso elas conseguem manter uma cópia desse conteúdo caso alguma autoridade faça a requisição ou até mesmo se tornem vulneráveis a vazamentos caso os servidores sejam alvo de ataques de *crackers* ou brechas nos sistemas. A Figura 4 representa o funcionamento da encriptação *TLS* que é utilizada pelas redes sociais em seus aplicativos de bate-papo.

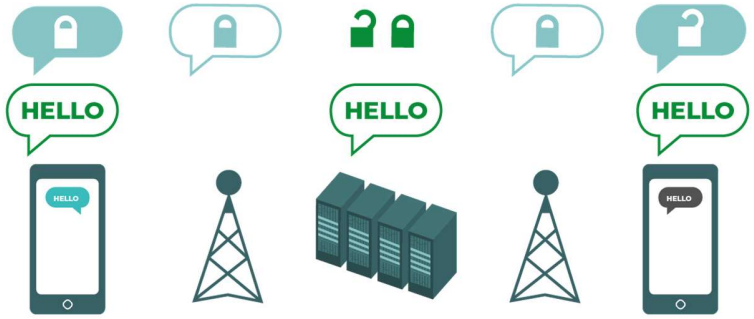


Figura 4. Funcionamento da criptografia TLS.

Fonte: *Surveillance Self-Defense, 2018*

5.9 Encriptação Ponta-a-Ponta

Com a grande quantidade de incidentes de vazamento de informações que são compartilhados apenas em conversas privativas, o *Facebook*, a rede social que lidera o quadro de redes sociais mais utilizadas, está com o projeto de implementar o *end-to-end* [5] (ponta a ponta) como principal método de criptografia nos seus aplicativos de conversas e troca de mensagens entre usuários, sem que seja um recurso extra e sim um recurso que é ativado automaticamente (*Newsroom Facebook*, 2019).

A criptografia de ponta-a-ponta faz a proteção da mensagem durante todo o percurso percorrido. Ela faz com que as informações nela contidas sejam transformadas em uma mensagem secreta, como por exemplo, ela envia a mensagem como uma carta fechada, garantindo que

[5] End-to-end: Método de encriptação.

ninguém, nem mesmo o aplicativo por onde a mensagem está sendo enviada tenha acesso ao conteúdo da mensagem. Para abrir a carta e ler a mensagem, é necessário usar uma frase secreta que apenas o autor e os destinatários possuem. Dessa forma apenas os participantes da conversa possuem acesso a mensagem. A Figura 5 a seguir, faz a representação de como a encriptação ponta-a-ponta trabalha (*Newsroom Facebook*, 2019).

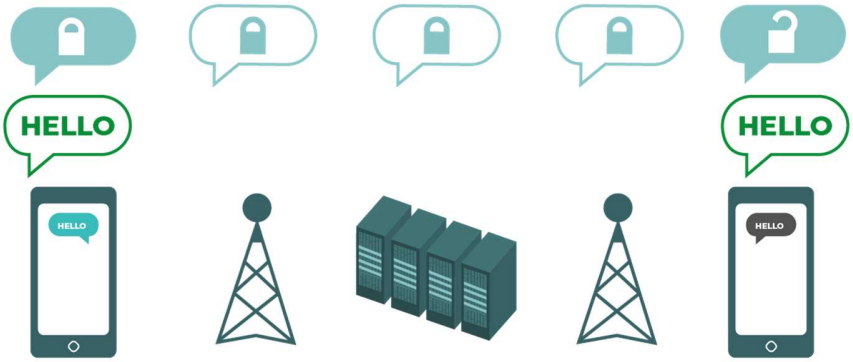


Figura 5. Funcionamento da criptografia ponta a ponta.

Fonte*: Surveillance Self-Defense, 2018*

Segundo o *CEO*[6] do *Facebook*, Mark Zuckerberg, "A criptografia de ponta-a-ponta é uma importante ferramenta no desenvolvimento de uma rede social centrada na privacidade. A criptografia ajuda a descentralizar – ela limita serviços como os nossos de ver o conteúdo que está fluindo através deles e dificulta muito o acesso de qualquer um às suas informações".

5.10 Exemplo de Aplicação de Criptografia Ponta-a-Ponta

Assim como sugerido por Mark Zuckerberg em 2018, uma das possíveis soluções a se implementar nos seus aplicativos de bate-papo é a criptografia ponta-a-ponta que já foi mencionada, esse recurso já está disponível para utilização no aplicativo do *Facebook*, porém é necessário fazer a sua ativação manualmente. Empresas de segurança e entusiastas na questão de proteção de dados, assim como mostrado nas figuras 6, 7 e 8, a *Rogue Wave Company*, uma empresa que trabalha com aplicações de segurança, que trabalham junto da *Google* e da *Microsoft*, desenvolveu um exemplo na linguagem *PHP* de como seria a implementação da criptografia *end-to-end*.

[6] *Chief Executive Officer*, que significa Diretor Executivo.

```php
use Zend\Crypt\PublicKey\RsaOptions;
use Zend\Crypt\BlockCipher;

$username = 'alice';
$password = 'test'; // user's password

// Generate public and private key
$rsaOptions = new RsaOptions();
$rsaOptions->generateKeys([
    'private_key_bits' => 2048
]);
$publicKey  = $rsaOptions->getPublicKey()->toString();
$privateKey = $rsaOptions->getPrivateKey()->toString();

// store the public key in a .pub file
file_put_contents($username . '.pub', $publicKey);

// encrypt and store the private key in a file
$blockCipher = BlockCipher::factory('openssl', array('algo' => 'aes'));
$blockCipher->setKey($password);
file_put_contents($username, $blockCipher->encrypt($privateKey));
```

Figura 6. Geração e armazenamento das chaves públicas e privadas.

Fonte: *Zend Framework*.

Em um primeiro momento, é gerado uma chave privada de 2048 bits, existem chaves de 4096 *bits*, porém as de 2048 *bits* são mais comuns em serem utilizadas em aplicativos. No exemplo, as chaves públicas e privadas são armazenadas em dois diferentes arquivos *$username.pub* e *$username*, respectivamente. Uma vez que foi utilizado uma encriptação nos arquivos, apenas seus "donos" podem acessá-los (2016, Tradução Nossa).

Uma vez que foi criado as chaves públicas e privadas para os usuários, pode-se iniciar um sistema híbrido de criptografia[7] desenvolvido pelo autor do *framework* acima. Supomos que Alice gostaria de enviar uma mensagem encriptada para Bob (2016, Tradução Nossa).

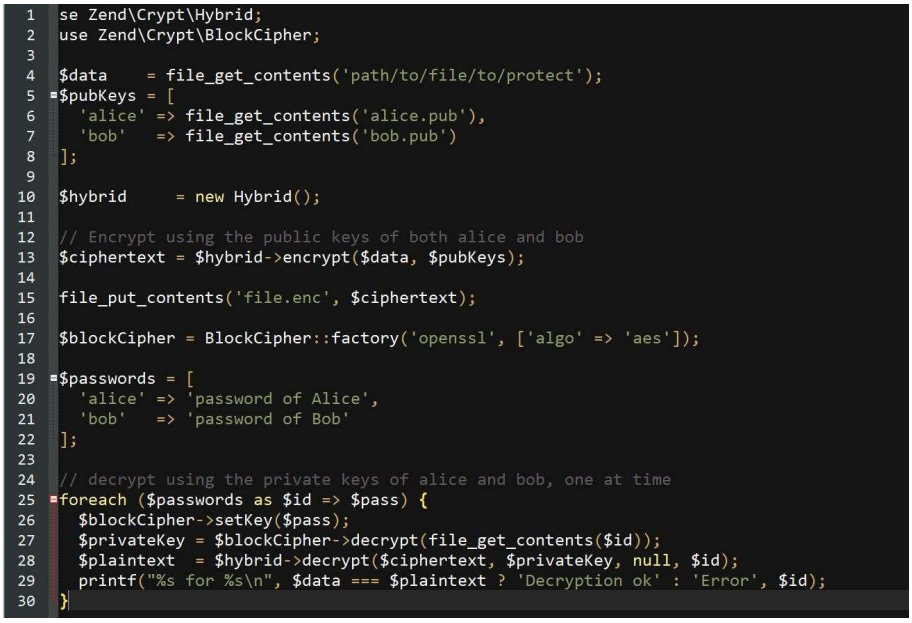
```php
use Zend\Crypt\Hybrid;
use Zend\Crypt\BlockCipher;

$sender   = 'alice';
$receiver = 'bob';
$password = 'test'; // bob's password

$msg = sprintf('A secret message from %s!', $sender);

// encrypt the message using the public key of the receiver
$publicKey  = file_get_contents($receiver . '.pub');
$hybrid     = new Hybrid();
$ciphertext = $hybrid->encrypt($msg, $publicKey);

// send the ciphertext to the receiver

// decrypt the private key of bob
$blockCipher = BlockCipher::factory('openssl', ['algo' => 'aes']);
$blockCipher->setKey($password);
$privateKey = $blockCipher->decrypt(file_get_contents($receiver));

$plaintext = $hybrid->decrypt($ciphertext, $privateKey);

printf("%s\n", $msg === $plaintext ? "The message is: $msg" : 'Error!');
```

Figura 7. Seleção de destinatário e encriptação da mensagem a ser enviada.

Fonte: *Zend Framework*.

[7] Sistema híbrido de criptografia é um método de sistema de criptografia que utiliza tanto uma criptografia simétrica como assimétrica. Use criptografia de chave pública para compartilhar uma chave para criptografia simétrica. A mensagem que está sendo enviada no momento é criptografada usando sua própria chave privada e, em seguida, a mensagem criptografada é enviada ao destinatário. Como o compartilhamento de uma chave simétrica não é seguro, é diferente para cada sessão (WIKIPEDIA, 2019).

O exemplo acima, demonstra como seria a encriptação da mensagem entre seus usuários. Nesse modelo, o remetente (Alice) tem conhecimento da mensagem pois foi ela que a redigiu, porém se fosse necessário enviar para múltiplos destinatários, seria necessário especificar as chaves públicas para serem utilizadas na encriptação (2016, Tradução Nossa).



```php
se Zend\Crypt\Hybrid;
use Zend\Crypt\BlockCipher;

$data    = file_get_contents('path/to/file/to/protect');
$pubKeys = [
  'alice' => file_get_contents('alice.pub'),
  'bob'   => file_get_contents('bob.pub')
];

$hybrid     = new Hybrid();

// Encrypt using the public keys of both alice and bob
$ciphertext = $hybrid->encrypt($data, $pubKeys);

file_put_contents('file.enc', $ciphertext);

$blockCipher = BlockCipher::factory('openssl', ['algo' => 'aes']);

$passwords = [
  'alice' => 'password of Alice',
  'bob'   => 'password of Bob'
];

// decrypt using the private keys of alice and bob, one at time
foreach ($passwords as $id => $pass) {
  $blockCipher->setKey($pass);
  $privateKey = $blockCipher->decrypt(file_get_contents($id));
  $plaintext  = $hybrid->decrypt($ciphertext, $privateKey, null, $id);
  printf("%s for %s\n", $data === $plaintext ? 'Decryption ok' : 'Error', $id);
}
```

Figura 8. Processo de desencriptação da mensagem recebida pelo destinatário.

Fonte: *Zend Framework*.

Para se fazer a desencriptação, é utilizado um código que é validado durante o processo de *login* dos usuários, que por motivos de segurança não deve ficar muito tempo armazenado. Essa senha pode ser salva temporariamente usando a variável session() que o *PHP* disponibiliza (2016, Tradução Nossa).

Na decriptação é utilizada a função *Zend\Crypt\Hybrid::decrypt()*, onde é especificado a chave privada, a frase secreta nula e por último, a identificação da chave privada. Eles são necessários para encontrar a chave correta no cabeçalho da mensagem encriptada (2016, Tradução Nossa).

5.11 Vantagens e Desvantagens da Criptografia Ponta-a-ponta

A grande vantagem da aplicação desse tipo de criptografia, é se assegurar que apenas as pessoas inseridas na conversa vão ter acesso às mensagens enviadas, dando mais privacidade e confiança aos seus usuários, sabendo-se que nem mesmo o provedor do serviço de mensagens vai poder ter acesso ao conteúdo da conversa (Surveillance Self-Defense, 2018).

As mensagens enviadas estarão mais seguras pois cada uma delas terá um cadeado que somente as pessoas envolvidas terão acesso a chave secreta para desbloqueá-las e terem acesso ao seu conteúdo (Surveillance Self-Defense, 2018).

Sua principal desvantagem é que esse tipo de serviço pode ser utilizado por terroristas e pessoas de má índole, para planejarem e executarem ações que possam prejudicar a sociedade. Em maio de 2018, o vice presidente do *Whatsapp*, um aplicativo de troca de mensagens que já

implementou esse tipo de criptografia, foi preso pois ele não compartilhou as mensagens de supostos criminosos que utilizavam seu aplicativo para fazer o planejamento de ataques terroristas, sendo que nem mesmo ele possuia acesso a esse tipo informação devido ao tipo de encriptação usada pelo aplicativo (G1 Globo, 2016).

5.12 Recomendações e Dicas de Segurança para o uso de Redes Sociais

Nas redes sociais, é normal compartilharmos todo os tipos de informações, porém devemos manter as informações sensíveis o mais longe de estranhos. Antes de se registrar nas redes sociais, devemos considerar que tipo de conteúdo vamos compartilhar dentro delas e relevar se elas não vão conter dados importantes do usuário (HAMADA; NASSIF, 2019).

Portanto, o senso comum deve ser a regra mais importante a ser levada em conta ao usar uma rede social. Evitar fazer *uploads* de fotografias sem primeiro considerar sua verdadeira utilidade ou oferecer informações que possam ser comprometidas no futuro (COSTA *et al*, 2018).

5.12.1 Verificar se esta é a página correta

Esta é uma medida de segurança que se deve verificar em qualquer *site* na Internet onde é necessário fazer *login*. A ação se faz necessário devido a muitos *crackers* criarem páginas idênticas às originais para fazer o roubo de informações como emails e senhas de seus donos. Assim podendo acessar contas e se passando por seus usuários (Olhar Digital, 2017).

Hoje em dia podemos fazer a verificação de modo simples, em seu navegador, do lado onde é inserido o *link* do *site*, podemos ver um cadeado fechado na cor verde, que identifica que é um *site* seguro que permite que os dados inseridos pelos usuários estejam trafegando criptografados entre o computador e o servidor (Mozila Firefox, 2018).

5.12.2 Controlar quem tem acesso a informações pessoais

Dentro das redes sociais podemos adicionar outros usuários para que possamos nos tornar “colegas”, muitas vezes adicionamos pessoas com o mesmo tipo de interesse ou até mesmo conhecidos de outros colegas para que possamos nos relacionar com novas pessoas, dando a elas acesso à informações privadas disponíveis no nosso perfil (FREIRE, 2015).

Apenas pessoas que estão conectadas podem tem acesso às informações que compartilhamos no perfil, porém, a rede social permite separar em grupos tais como: família e colegas de trabalho e delimitar o acesso a determinado tipo de informação para cada um deles, dando mais controle ao dono do perfil (MARTELETO, 2018).

5.12.3 Privacidade do perfil

As rede sociais possuem “configurações de privacidade”, onde podemos definir quem pode acessar determinado tipo de conteúdo tais como: fotos, *posts,* vídeos e etc. Assim podemos evitar que pessoas indesejadas tenham acesso a esse conteúdo (HAMADA; NASSIF, 2019).

5.12.4 Evite compartilhar dados sigilosos nos *chats* de bate-papo

Devemos a todos custo evitar de compartilhar dados pessoais tais como: endereços, contas bancárias, senhas, etc. Mesmo que enviemos essas informações para pessoas que confiamos através dos chats de bate-papo, *crackers* podem ter acesso a eles caso alguma brecha de segurança seja detectadas por eles.

5.12.5 Não siga links suspeitos

Prevenir de clicar em *links* suspeitos que levem para fora das redes sociais, pois pode acontecer de contas de usuários estarem infectados por vírus ou até mesmo terem sido invadidas por outras pessoas e, claro, evitar a execução de arquivos que foram enviados (SANTOS, 2016).

5.12.6 Removendo o perfil

Por fim, lembrar-se de que, se não for usar uma rede social temporariamente, é aconselhável desativar o perfil. E se definitivamente não for mais usado, o perfil do usuário deve ser excluído (DE SOUZA *et al*, 2018).

5.13 Questões de Segurança

Com a grande quantidade de ataques as redes sociais, o seu uso pode parecer perigoso. Porém se algumas dicas e boas práticas forem empregadas, é possível se proteger e evitar esse tipo de incidente ocorra durante o usos dessas plataformas (MARTELETO, 2018).

Manter o sistema sempre atualizado, utilização de um segundo fator de acesso as contas, delimitação de conteúdo nas redes sociais e uso do protocolo HTTPS são alguns cuidados que podemos ter ao navegar. No entanto, podemos diminuir os riscos durante a navegação se utilizarmos as redes sociais com precaução e ao mesmo tempo nos manter atentos às questões atuais de segurança (SANTOS, 2016).

5.13.1 Soluções de Segurança

Como os vírus são ainda uma grande ameaça, o uso de *softwares* de antivírus se fazem necessários para ajudar a impedir que código maliciosos se espalhem pelo computador do usuário e pelas redes sociais (FREIRE, 2015).

As ferramentas como o *antispam* e *firewall* também auxiliam na questão da segurança do sistema contra esses riscos. Outra dica importante é utilizar perfis sem as permissões de administrador durante a navegação, assim evita a instalação de códigos maliciosos sem ter o conhecimento do mesmo (MOREIRA *et al*, 2017).

5.13.2 Senhas

As senhas são chaves digitais pessoais para podermos acessar diferentes plataformas, assim é necessário mantê-las segura. Pode-se utilizar as seguintes recomendações para elaboração de senhas fortes para proteger as contas de mídia social (SOUZA *et al*, 2018):

I. Não utilizar a mesma senha das redes sociais em outro *sites*, assim como também não compartilhar;

II. Evitar incluir nomes comuns ou datas comemorativas. As senhas devem ser difícil de

adivinhar;

III. Evitar usar computadores públicos para acessar redes sociais. Lembrar-se de efetuar *logout*, especialmente quando usa um computador compartilhado com outras pessoas;

IV. Pensar duas vezes antes de clicar ou baixar qualquer conteúdo, lembrar-se de que pode ser um chamariz de engenharia social.

6. Coleta e Análise dos Dados

Com o auxílio do Google Forms, uma plataforma que permite a criação de pesquisas e enquetes, foi elaborado um questionário com perguntas fechadas, onde foi divulgado e publicado no *Facebook*, com o intuito de conhecer quais os hábitos que os usuários possuem dentro das redes sociais e como se portam na questão de compartilhamento de dados pessoais nos *chats* de bate-papo das redes sociais.

Com os resultados obtidos, podemos entender um pouco mais a respeito de como as redes sociais são usadas, qual é o maior público que as utiliza, como seus usuários se portam dentro delas e se possuem conhecimento que elas são um grande banco de dados com diversas informações com que devemos nos preocupar caso haja alguma brecha na proteção desses dados.

Na Figura 9, temos os resultados das enquetes gerado pelo *Google Forms* apresentados a partir de gráficos:

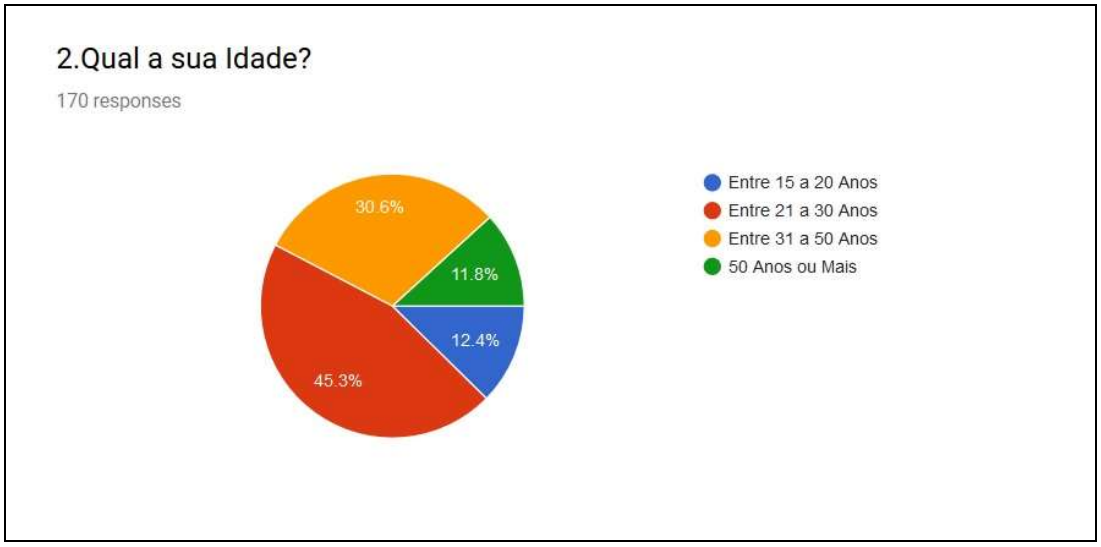


Figura 9. Faixa etária das pessoas que responderam ao questionário.

A Figura 9, das 170 pessoas que responderam, podemos observar que 45% são jovens entre 21 a 30 anos, que são a faixa etária mais predominante dentro das redes sociais.

Na Figura 10 mostra-se a representação de quais redes sociais são mais utilizadas.

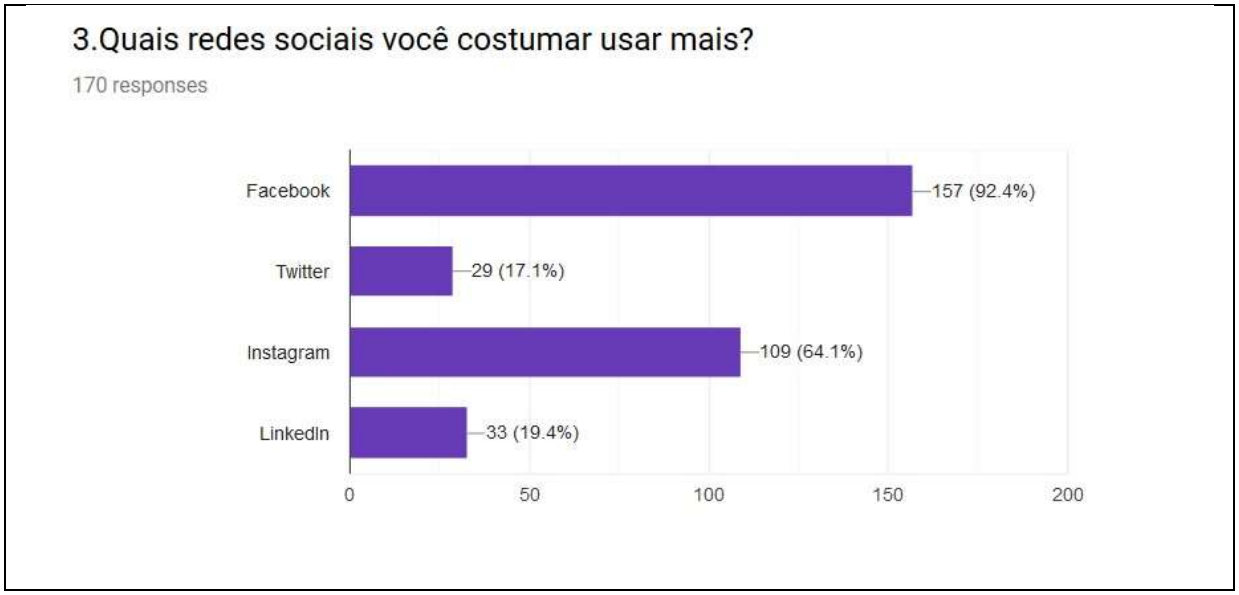


Figura 10. Redes sociais onde as pessoas mais são cadastradas.

De acordo com os dados da Figura 10, nota-se que o *Facebook* é a rede social mais utilizadas por aqueles que responderam a pesquisa. Dentro de 170 pessoas, 157 possuem ou utilizam o *Facebook* como a principal rede social.

Na Figura 11, trata-se de comportamento nos *chats* de bate-papo. Aborda o comportamento do usuário.

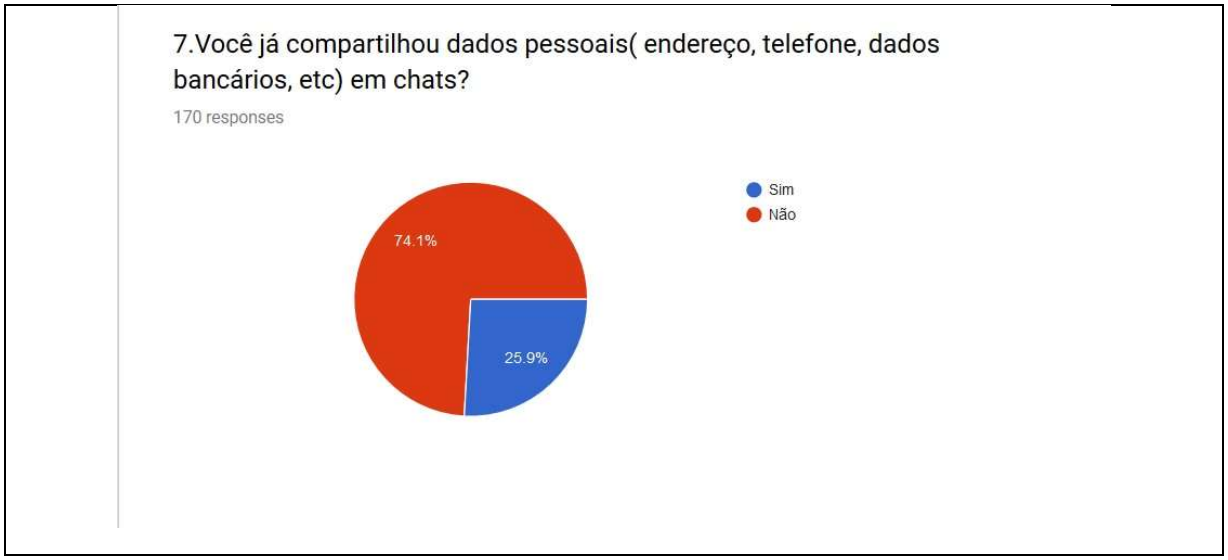


Figura 11. Informações pessoais via bate-papo.

Conforme dados da Figura 11, é apresentado o resultado do questionamento sobre compartilhamento de dados pessoais nos aplicativos de bate-papo, cerca de 25,9% afirmaram que já divulgaram. A grande maioria, entretanto nunca passou esse tipo de informação pelo bate-papo.

Muitos participantes, assim como mostra na Figura 12, já ouviram em jornais, reportagens ou até possuem conhecidos que já tiveram dados vazados por algum tipo de incidente.

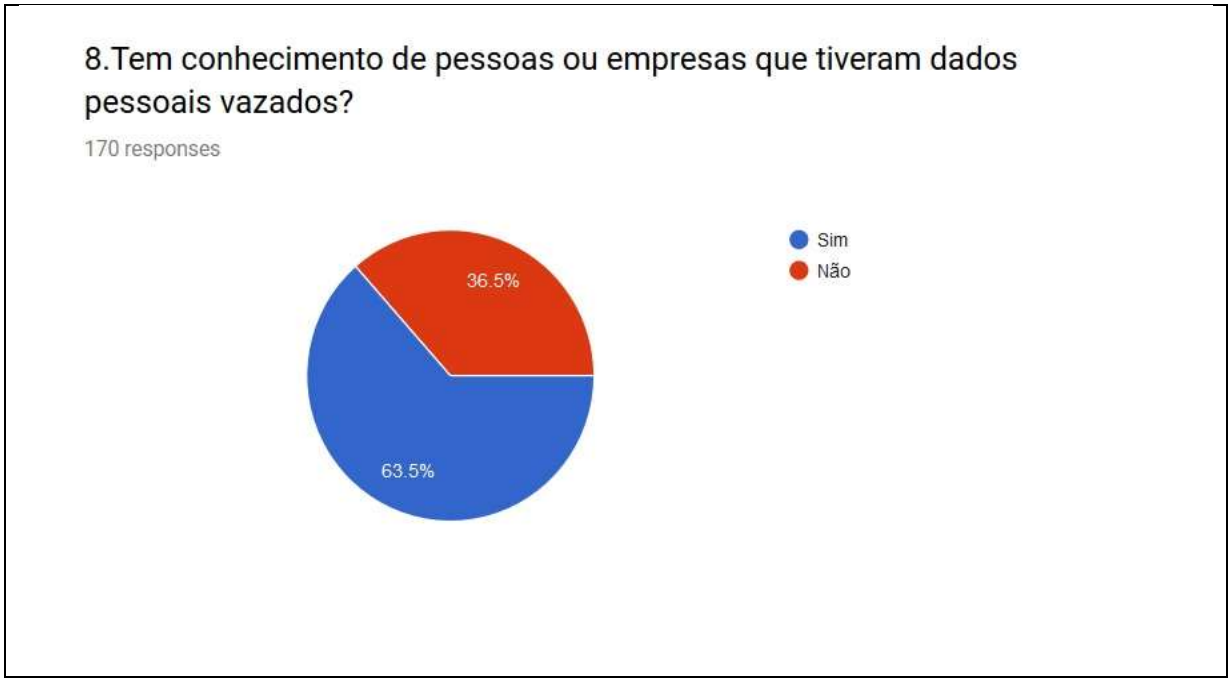


Figura 12. Conhecimento sobre pessoas ou empresas que tiveram seus dados vazados.

A Figura 12 revela que muitos dos que participaram da enquete possuem conhecimento que pessoas no círculo de amizade ou até empresas, já tiveram de alguma maneira, dados pessoais ou de seus usuários vazados.

Assim como revelado na Figura 13, poucos lêem corretamente os termos durante o cadastro nas redes sociais.

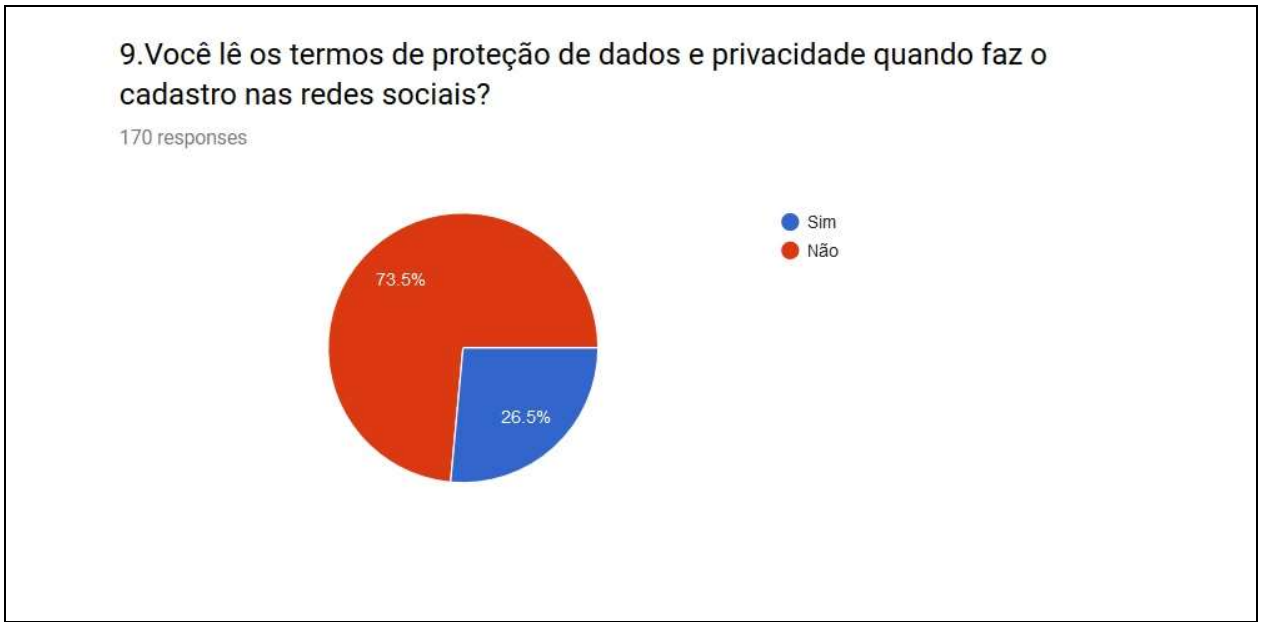


Figura 13. Termos de proteção e privacidade de dados.

A Figura 13 nos mostra que mais da metade dos usuários nunca lêem os termos de privacidade e proteção de dados das redes sociais onde estão ingressando.

A Figura 14, trata-se de uma notícia onde mostra que o *Facebook* já teve vazamento de dados de usuários.

Figura 14. Opinião dos entrevistados sobre o vazamento de dados do Facebook no ano de 2018.

Assim como grande parte dos participantes já tinham conhecimento dos escândalos do *Facebook*, assim como mostra na Figura 14, podemos ver qual é o opinião deles, podemos ver que a grande maioria (40,6%) se sentem indignados com uma rede social dessa magnitude ter problemas em relação ao vazamento de seus dados.

7. Considerações Finais

Neste trabalho, com o auxílio do conteúdo aprendido na matéria de Segurança da Informação, exploramos as questões de compartilhamento, privacidade e segurança de dados nos aplicativos de conversas nas redes sociais. A partir de um estudo quantitativo, buscamos entender como as redes sociais cuidam das informações que enviamos para nossos contatos nos aplicativos de bate-papo, quais são os futuros planos de implementação de tecnologias de proteção de dados, quais suas mudanças e principalmente entender como o usuário se porta e se tem conhecimento na questão de dados compartilhado dentro delas.

Entendemos que as redes sociais são responsáveis por manter seguro os dados que compartilhamos dentro delas, são cuidados que qualquer *site* que trabalha com informações pessoais precisam tomar, mas nem sempre podemos confiar totalmente nelas, por isso, devemos ser prudentes na hora de usá-las.

Mesmo com a implementação de novas tecnologias de segurança, devemos seguir as boas práticas e tomar muito cuidado com o que escrevemos e enviamos.

Segundo os dados obtidos por meio do questionário aplicado no estudo, vimos que as redes sociais são formadas pela maioria de jovens. Podemos ver também que eles estão atentos na questão de vazamento de dados sendo que apenas uma parcela faz o envio de dados privados nos

chats de bate-papo e estão cientes que colegas ou empresas famosas já tiveram participações em incidentes relacionados a exposição de informações.

Referências

BARBOSA, J. G. P. et al. **Obtenção de Conhecimento para Inovação: Benefícios e Malefícios de Processos de Gestão da Segurança da Informação**. Sociedade, Contabilidade e Gestão, Rio de Janeiro, v. 7, n. 1, jan. 2012.

COSTA, JEISON ESTEVAM. **Engenharia social e segurança da informação no ambiente corporativo: um estudo de caso em uma cooperativa de crédito localizada no sul de Santa Catarina.** Repositório Institucional, Santa Catarina, jun. 2018. Disponível em:<https://repositorio.ufsc.br/handle/123456789/187348>. Acesso em: 17 abr. 2019.

FERNANDES, Jorge Henrique Cabral; , Raul Carvalho De Souza. **UM ESTUDO SOBRE A CONFIANÇA EM SEGURANÇA DA INFORMAÇÃO FOCADO NA PREVENÇÃO A ATAQUES DE ENGENHARIA SOCIAL NAS COMUNICAÇÕES DIGITAIS.** Brazilian Journal of Information Studies: Research Trend, Brasília, v. 10, n. 1, jan./dez. 2016. Disponível em: <http://www2.marilia.unesp.br/revistas/index.php/bjis/article/view/5088/3976>. Acesso em: 01 mai. 2019.

FIREFOX. **Como saber se a minha conexão com um site é segura?**. Disponível em: https://support.mozilla.org/pt-BR/kb/como-saber-se-minha-conexao-e-segura. Acesso em: 24 jun. 2019.

G1. **Twitter alerta usuários sobre vazamento de dados após 'atividade anormal'**. Disponível em: <https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2018/12/18/twitter-alerta-usuarios-sobre-vazamento-de-dados-apos-atividade-anormal.ghtml>. Acesso em: 22 abr. 2019.

GAUCHAZH CIÊNCIA E TECNOLOGIA. **Saiba como o vazamento de dados pelo facebook pode ter afetado você e como se proteger**. Disponível em:

<https://gauchazh.clicrbs.com.br/tecnologia/noticia/2018/12/saiba-como-o- vazamento-de-dados-pelo-facebook-pode-ter-afetado-voce-e-como-se-proteger-cjpvpvhku0mgl01pi0i05ip1a.html>. Acesso em: 17 abr. 2019.

KIETZMANN, J. *et al*. **Business Horizons**. 54. ed. Vancouver: j.bushor, 2011. p. 241-251.

HAMADA, Hélio Hiroshi; , Lilian Noronha Nassif. **PERSPECTIVAS DA SEGURANÇA PÚBLICA NO CONTEXTO DE SMART CITIES: desafios e oportunidades para as organizações policiais**. Perspectiva em Políticas Públicas, Belo Horizonte, v. 11, n. 22, p. 189-213, jul./dez. 2018. Disponível em:

<http://revista.uemg.br/index.php/revistappp/article/view/3467>. Acesso em: 25 abr. 2019.

HINTZBERGEN, J. *et al*. **Fundamentos de Segurança da Informação:** : com base na ISO 27001 e na ISO 27002. 1. ed. [S.l.]: BrasPort, 2018.

MARCIANO, J. L. P. **Segurança da Informação - uma abordagem social**. Brasília, out./2009. Disponível em: <http://repositorio.unb.br/handle/10482/1943>. Acesso em: 15 mai. 2019.

MARTELETO, Regina Maria**. REDES SOCIAIS, MEDIAÇÃO E APROPRIAÇÃO DE**

INFORMAÇÕES: situando campos, objetos e conceitos na pesquisa em Ciência da Informação. BRAPCI - Base de Dados em Ciência da Informação, Rio de Janeiro, v. 3, n. 1, p. 27-46, jan./dez. 2010. Disponível em: <http://www.brapci.inf.br/index.php/article/view/0000009339/e02c06fa980a47881 18f8ef357e2d5c0/>. Acesso em: 22 abr. 2019.

MOREIRA, Artur Carlos Da Silva. **As redes sociais em segurança e saúde do trabalhador: proposta de uma estrutura de avaliação**. Repositório Nacional, Florianópolis, jan. 2017. Disponível em: <https://repositorio.ufsc.br/handle/123456789/185461?show=full>. Acesso em: 30 abr. 2019.

NEWSROOM. **Uma visão centrada em privacidade para redes sociais**. Disponível em: <https://br.newsroom.fb.com/news/2019/03/uma-visao-centrada-em- privacidade-para-redes-sociais/>. Acesso em: 26 mar. 2019.

PRIMO, Alex. **O aspecto relacional das interações na Web 2.0**. E- Compós, Rio Grande do Sul, v. 9, n. 1, p. 1-21, mai./2007. Disponível em: <http://www.ufrgs.br/limc/PDFs/web2.pdf>. Acesso em: 13 jun. 2019.

RECUERO, RAQUEL. **Redes sociais na internet**. 1 ed. Porto Alegre: Meridional, 2009. p. 191.

SANTOS, Marco Antonio Fernandes Dos. **Segurança na cultura digital**. Repositório Institucional, Santa Catarina, set. 2016. Disponível em: <https://repositorio.ufsc.br/handle/123456789/168731?show=full>. Acesso em: 22 abr. 2019.

SOUZA, I. T. D. **ANÁLISE DO CONHECIMENTO DE SEGURANÇA E PRIVACIDADE DA INFORMAÇÃO** . REVISTA INTERDISCIPLINAR ENCONTRO DAS CIÊNCIAS , Ceará, v. 1, n. 2, p. 196-206, abr./2018. Disponível em: <www.fvs.edu.br/riec/index.php/riec/article/download/29/23>. Acesso em: 14 mai. 2019.

SURVEILLANCE SELF-DEFENSE. **O que eu deveria saber sobre criptografia?**. Disponível em: https://ssd.eff.org/pt-br/module/o-que-%C3%A9-criptografia. Acesso em: 15 mai. 2019.

TECH ENTER. **Princípios Básicos da Segurança da Informação**. Disponível em: https://techenter.com.br/principios-basicos-da-seguranca-da-informacao/. Acesso em: 18 jun. 2019.

TECHTUDO. **10 fatos sobre o uso de redes sociais no brasil que você precisa saber**. Disponível em: <https://www.techtudo.com.br/noticias/2018/02/10-fatos- sobre-o-uso-de-redes-sociais-no-brasil-que-voce-precisa-saber.ghtml>. Acesso em: 01 abr. 2019.

TECHTUDO. **Google chega ao fim após vazamentos de dados e baixa popularidade**. Disponível em:

<https://www.techtudo.com.br/noticias/2019/04/google-chega-ao-fim-apos-vazamentos-de-dados-e-baixa-popularidade.ghtml>. Acesso em: 25 abr. 2019.

TIINSIDE. **twitter confirma vazamento de dados ocorrida em maio de 2017**.

Disponível em: <http://tiinside.com.br/tiinside/seguranca/mercado-seguranca/21/09/2018/twitter-confirma-vazamento-de-dados-ocorrida-em-maio- de-2017/>. Acesso em: 01 mai. 2019.