

**Vulnerabilidade de Dados e a Percepção de Privacidade dos Usuários de Redes Sociais****Data Vulnerability and The Perception Privacy of Social Networks Users**

Recebimento dos originais: 28/08/2019

Aceitação para publicação: 17/09/2019

**Bruna Cardoso Dos Santos**

Graduada em Administração no Centro Universitário FECAP  
Instituição: Fundação Escola de Comércio Álvares Penteado - FECAP  
Endereço: Av. da Liberdade, 532 - Liberdade, São Paulo - SP, Brasil  
E-mail: cardoso.bruna41@gmail.com

**Leticia Cristina Ferraz Santos**

Graduada em Administração no Centro Universitário FECAP  
Instituição: Fundação Escola de Comércio Álvares Penteado - FECAP  
Endereço: Av. da Liberdade, 532 - Liberdade, São Paulo - SP, Brasil  
E-mail: leticiaferraz@hotmail.com

**Mayer Schuman Guerra**

Graduado em Administração no Centro Universitário FECAP  
Instituição: Fundação Escola de Comércio Álvares Penteado - FECAP  
Endereço: Av. da Liberdade, 532 - Liberdade, São Paulo - SP, Brasil  
E-mail: schumanmayer@gmail.com

**Fabricio Stocker**

Doutorando em Administração na Faculdade de Economia, Administração e Contabilidade da  
Universidade de São Paulo  
Instituição: Universidade de São Paulo (USP)  
Endereço: Av. Prof. Luciano Gualberto, 908 - Butantã, São Paulo - SP, Brasil  
E-mail: fabriciostocker@usp.br

**RESUMO**

O fluxo elevado de informações, tal como as redes sociais têm dado acesso a um nível de informação detalhada, organizada uniformemente e agregados em um só lugar, trazendo a atenção para uma série de riscos à privacidade e vulnerabilidade destes dados. Derivado disto, definiu-se como objetivo desta pesquisa: analisar a percepção dos usuários sobre a vulnerabilidade das informações nas redes sociais. A pesquisa foi aplicada empiricamente por meio de uma survey realizada com uma amostra de 454 usuários. Com base nos resultados foi possível destacar que em sua maioria, os usuários das redes sociais reconhecem o que representa a privacidade de dados, a política de privacidade e as ferramentas para alterar as configurações de privacidade para garantir a segurança nos dados. No entanto, notou-se um comportamento diverso com relação a garantia de segurança, uso e compartilhamento de informações, bem como percepção sobre os vazamentos dos dados. A contribuição da pesquisa consiste na ampliação e descrição do fenômeno de vulnerabilidade de dados, no que tange as redes sociais, um campo ainda pouco explorado por pesquisas acadêmicas. Por fim, apresenta-se ainda a proposta de uma agenda de pesquisa futura para o tema.

**Palavras-chave:** Redes Sociais, Privacidade de Dados, Vulnerabilidade, Facebook, Gestão da informação.

### **ABSTRACT**

The high flow of information such as social networks has given access to a detailed, uniformly organized and aggregated level of information in one place, bringing attention to a number of risks to the privacy and vulnerability of this data. Derived from this, it was defined as the objective of this research: to analyze the perception of users about the vulnerability of information in social networks. The research was applied empirically through a survey conducted with a sample of 454 users. Based on the results, it was possible to highlight that most social network users recognize what data privacy, privacy policy, and the tools to change the privacy settings to ensure data security. However, a variety of behavior was noted regarding assurance of security, use and sharing of information, as well as perception of data leaks. The contribution of the research consists in the extension and description of the phenomenon of data vulnerability, regarding social networks, a field not yet explored by academic research. Finally, the proposal for a future research agenda for the theme is presented.

**Keywords:** Social networks, Privacy of Data, Vulnerability, Facebook, Information management.

## **1 INTRODUÇÃO**

O fluxo elevado de informações, tal como as redes sociais têm acesso, segundo Jones e Soltren (2005) com um nível de informação detalhada, organizada uniformemente e agregados em um só lugar, traz a atenção para uma série de riscos à privacidade. A exemplo disto, no ano de 2005 a *Privacy Internacional* cobrou o Facebook sobre as graves falhas de privacidade e colocou-a na segunda categoria mais baixa para “ameaças à privacidade substanciais e abrangentes”.

Os autores identificaram falhas graves no *set-up* do Facebook, no qual isso facilitaria as violações de privacidade e a mineração de dados. Na época desse estudo, quase 2 anos após o lançamento da rede social, as senhas dos usuários ainda estavam sendo enviadas sem criptografia, e, portanto, poderiam ser facilmente interceptados por terceiros (JONES; SOLTREN, 2005).

Em abril de 2018, o jornal New York Times divulgou o maior escândalo de vazamento de dados do Facebook, algo que teve proporções judiciais. Esses dados foram compartilhados com a empresa *Cambridge Analytica*, uma empresa de mineração e análise de dados com comunicação estratégica para processo eleitoral, no qual foram atingidas 87 milhões de usuário.

A vulnerabilidade de dados e segurança das redes sociais não é um assunto atual. Segundo Jones e Soltren (2005), até mesmo o mais elogiado recurso de privacidade do Facebook, no qual tem a capacidade de restringir um perfil para ser visto somente por amigos, falhou nos primeiros 3 anos da sua existência: As informações postadas em perfis restritos apareceram em pesquisas, a menos que o usuário tenha escolhido excluir seu perfil de pesquisas. Essa falha foi corrigida somente no final de junho de 2007, mas depois de um blogueiro em tecnologia divulgar essa lacuna e entrar em contato com o

Facebook. No entanto, recentemente, em outubro de 2018, o Facebook afirmou a existência de vulnerabilidade em sua rede que expôs dados pessoais de cerca de 30 milhões de usuários.

Os questionamentos sobre como essas plataformas estão lidando com essas informações estão sendo cada vez mais frequentes, mas ainda é algo obscuro para a sociedade. Acredita-se que poucas pessoas leem e entendem a complexidade acerca das políticas de privacidade das redes sociais, sobre a vulnerabilidade sob os compartilhamentos feitos pelos usuários como preferências, gostos, locais frequentados etc. Outras críticas são baseadas no fato de que terceiros podem usar essas informações divulgadas pelo Facebook ou outras redes, para mineração de dados, *phishing* e outras finalidades maliciosas (HORN; HUGHES; LOVEJOY, 2009).

Além disto, pode-se observar dos consumidores de redes sociais a constante percepção de risco que interferem na sua usabilidade, no qual se reflete em suas características comportamentais, entre as quais, questões concernentes à falta de privacidade (HOARSELY et al. 2010; HUM et al. 2011; WILCOX; STEPHEN, 2013).

Portanto, dadas as informações e estudos sobre este fenômeno, emerge a possibilidade de entender a percepção dos usuários a vulnerabilidade dos dados pessoais na utilização das mídias sociais e a invasão de privacidade, isto posto, este estudo levanta o seguinte problema de pesquisa: Como a vulnerabilidade das informações em redes sociais afeta a percepção de privacidade dos usuários sobre as redes sociais?

## **2 REFERENCIAL TEORICO**

### **2.1 Gestão da Informação**

A gestão da informação (GI) é um conjunto estruturado de atividades que espelha a forma pela qual uma organização captura, distribui, e usa informação e conhecimento (DAVENPORT, 1998).

A informação é infinitamente reutilizável, não se deteriora nem se deprecia e seu valor é determinado exclusivamente pelo seu usuário (MCGEE; PRUSAK, 1994). Há uma distinção entre informação, dados e conhecimento (DAVENPORT, 1998). Segundo McGee e Prusak (1994), informação deve informar, já os dados não tem essa função. Informação não tem limites, os dados podem ser limitados. Já Davenport (1998), insiste em não fazer comparação e acredita que informação é um conjunto dos três.

Quando falamos em gestão da informação, a segurança dessa informação é fator muito importante. A segurança da informação tem como objetivo preservar três princípios básicos que baseiam esta prática: confiabilidade, integridade e disponibilidade (SÊMOLA, 2003).

Segundo Sêmola (2003), a confiabilidade garante que toda informação deve ser protegida e seu acesso é de uso apenas das pessoas para quem são destinadas. O princípio da integridade garante que toda a informação não pode ser alterada e deve ser mantida exatamente como foi disponibilizada pelo indivíduo. Toda informação gerada ou adquirida por indivíduo ou instituição deve estar disponível a qualquer momento para os usuários, caso necessitem para qualquer finalidade.

## **2.2 Redes Sociais**

Apesar de um assunto novo, as redes sociais segundo Martha Gabriel (2010, p. 193) existem há pelo menos três mil anos, quando os homens se sentavam ao redor de uma fogueira para conversar sobre assuntos de interesse comum. Com o tempo, o que mudou foi a abrangência e difusão das redes sociais, conforme as tecnologias de comunicação interativa foram se desenvolvendo. A autora ressalta que os sistemas de redes sociais on-line existiam antes da Web 2.0, como o *Firefly*, por exemplo, em 1996.

Para Marteleto (2010), a Internet tem pelo menos dois aspectos principais. O primeiro deles é que a internet possui uma grande quantidade de dados e informações abertos a múltiplas possibilidades como escritas, consultas, leituras usos e principalmente apropriações, portanto é chamada de “redes das redes”. Em segundo, ela é uma arena ampliada geograficamente e socialmente para interação, comunicação e socialização entre os usuários.

Um dos elementos característicos das mídias sociais é o seu poder de difundir informações através das conexões existentes entre todos os atores. Recuero (2009, p. 116) afirma que essa capacidade alterou de forma significativa os fluxos de informações dentro da própria rede. Com o surgimento da Internet permitiu que as pessoas difundissem as informações de forma mais rápida e interativa, portanto com essa mudança houve a criação de novos canais e, ao mesmo tempo, uma pluralidade de novas informações circulando nos grupos sociais.

Boyd e Ellison (2007) ressaltam que o que torna os sites de redes sociais únicos não é o que eles permitam que os indivíduos encontrem desconhecidos, mas permite aos usuários troquem informações tornando-as visíveis em suas redes sociais. Martha Gabriel (2010) destaca que sem a possibilidade de estarem conectados e interagirem o tempo todo para poderem compartilhar conteúdos de forma natural, os indivíduos não poderiam manter uma rede social.

Segundo Recuero (2009), com o advento da Internet houve algumas mudanças significativas para a sociedade. Entre essas mudanças temos algumas fundamentais. A mais significativa é a possibilidade de expressão e sociabilização através das ferramentas de comunicação mediada pelo computador (CMC). Essas ferramentas proporcionaram, assim, que atores pudessem construir-se, interagir e comunicar com outros atores, deixando, na rede de computadores, rastros que permitem o

reconhecimento dos padrões de suas conexões e a visualização de suas redes sociais através desses rastros.

Segundo uma pesquisa realizada pela *We Are Social* em parceria com a Hootsuite e publicada em 2017 pela The Next Web, 3 bilhões de pessoas no mundo utilizam redes sociais ativamente pelo menos uma vez por mês, portanto representando 40% da população mundial. A pesquisa ainda destaca que os telefones celulares são os dispositivos mais importantes para pelo menos dois terços da população.

De acordo com o Slash Gear (2017), empresa de pesquisa e *highlighting* em tecnologia, divulgou uma pesquisa em seu site no qual o Facebook gera aproximadamente 2,7 bilhões de curtir e 300 milhões de novas fotos postadas no serviço diariamente, contabilizando mais de 2,5 milhões de novos conteúdos processados pelo sistema. A empresa ainda afirma que a cada 30 minutos 105TB de dados são escaneados pelos os servidores das redes sociais.

## **2.2 Vulnerabilidade dos Dados**

Segundo Sêmola (2003) circunstâncias podem dificultar a preservação dos três princípios básicos da Segurança das Informações, sendo ameaças e vulnerabilidade. Ameaças são agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade.

Vulnerabilidade é a fragilidade presente ou associada a ativos que manipulam e/ou processam informações que, ao ser explorada por ameaças, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

A Política de Dados do Facebook, Instagram e Messenger são divididas em dois grupos, sendo os tipos de dados coletadas pela plataforma e a forma de utilização. Dados Coletados, como i) Redes e conexões (Páginas, grupos e hashtags no qual o usuário interage); ii) Uso geral (Conteúdo que o usuário visualiza ou no qual se envolve); iii) Transações realizadas (Quando se utiliza aplicativos para realizar transações financeiras); iv) Informações do dispositivo (Atributos do dispositivo, operações, identificadores, sinais dos dispositivos, dados de configuração). Outro tipo de utilização dos dados, refere-se a: i) Aprimorar os produtos (Melhorar o Feed, Sugestão de Eventos); e ii) Anúncios e outros conteúdos patrocinados (Selecionar e personalizar).

Apesar de várias partes dentro do Termo de Serviço citarem a quantidade de dados que são adquiridos por causa dos usuários e quais formas eles podem se proteger de ataques externos em suas contas. Em nenhuma parte do Termo de Uso ou Segurança deixam claro como o Facebook, Instagram ou Messenger se defendem dos ataques externos a sua rede.

Na política de segurança do Facebook, existem políticas, ferramentas e recursos com o intuito de manter a segurança. O site oferece controle sobre o conteúdo compartilhado, com quem compartilham essa informação e também manuais de como se proteger, proteger sua conta e proteger suas informações estão disponíveis para ajudar os usuários. Na política de dados do Facebook, são informados todos os dados e informações que são acessados e utilizados pela empresa. Também é dito como essas informações são trabalhadas em conjunto com todas as redes sociais da empresa.

Vários estudos descobriram que há pouca relação entre a divulgação de informações privadas pelos usuários de sites de redes sociais e suas preocupações declaradas de privacidade (Dwyer; Hiltz; Passerini, 2007; Livingstone; 2008; Tufekci; 2008)

### **3 PROCEDIMENTOS METODOLÓGICOS**

O objetivo desta pesquisa é analisar a percepção dos usuários sobre a vulnerabilidade das informações nas redes sociais. Para tanto, alguns passos metodológicos serão adotados. Para Vergara (1990), devemos classificar a pesquisa em dois aspectos: quanto aos fins e quanto aos meios.

Quanto aos fins, esta pesquisa será exploratória e descritiva. Exploratória porque a área, no qual estamos estudando, não se verificou a existência de estudos recentes, ou seja, pesquisas atuais que abordam a privacidade e vulnerabilidade dos usuários nas redes sociais. Descritiva porque visamos descrever as percepções dos usuários acerca da privacidade de dados nas suas redes sociais e qual seu nível de conhecimento e preocupação sobre o assunto. Quanto aos meios, esta pesquisa figura-se como uma pesquisa de campo, em razão da aplicação de um questionário aos indivíduos que desejam expor sua perspectiva e percepção sobre o uso e privacidade dos dados nas redes sociais.

Foram seguidas as seguintes etapas para a pesquisa, de acordo com Vianna (2001), tais como: i) definição e delimitação do problema de pesquisa; ii) formulação da hipótese/objetivo de estudo; iii) coleta de dados; iv) análise e interpretação dos resultados; e por fim, iv) inferências e considerações sobre o fenômeno estudado.

Com relação a técnica de coleta e análise dos dados, a abordagem da coleta de dados é quantitativa com uma amostragem não probabilística utilizando como base questionários de pesquisa auto administrados e aplicados via formulário eletrônico. O questionário da pesquisa foi realizado em março de 2019 com o objetivo de classificar as características dos usuários de redes sociais e avaliar sua percepção sobre a confiabilidade e privacidade de seus dados. Utilizamos uma abordagem quantitativa para a pesquisa, usando a ferramenta *Google Forms*®. O foco foram os usuários de redes sociais em geral, esperando atingir uma grande diversidade de pessoas.

Na pesquisa aplicada, obtivemos 470 respostas. Foram descartados 16 questionários que tiveram suas respostas incompletas, ou seja, apenas 3,40% da amostra coletada, assim este estudo tem como base a percepção de 454 usuários.

#### **4 ANÁLISE E DISCUSSÃO DOS RESULTADOS**

Os resultados apresentados nesta sessão, representam um universo de 454 indivíduos, questionados sobre o uso e percepção da privacidade dos dados quando no uso de redes sociais. Dos 454 (n=100%) respondentes, 77,09% dos respondentes são do sexo feminino e 22,91% do sexo masculino. A escolaridade de 59,03% do público é de ensino superior completo/incompleto, 22,47% com ensino médio, 15,64% pós-graduação e o restante, representando 2,86%, com ensino fundamental e mestrado/doutorado. Aproximadamente 40% das pessoas que responderam o questionário possuía idade na faixa de 18 a 24 anos, 23,13% tem idade de 25 a 35 anos, 23,79% estão entre a faixa etária de 36 a 50 anos, somente 5,95% tem idade de até 17 anos e 6,61% estão acima de 50 anos.

Identificou-se que a grande maioria, aproximadamente 60%, utilizam mais o WhatsApp, ficando à frente do Instagram com 28,85%, Facebook com 9,03% e Twitter 2,20%, e outras redes sociais LinkedIn, Reddit e YouTube com 0,22% cada uma.

Foi perguntado aos usuários com qual frequência utilizam e acessam as redes sociais. Ao analisar as respostas, constatou-se que 11,67% declararam gastar mais tempo nas redes sociais do que as pessoas a sua volta e o restante, com 4,63%, responderam que raramente utilizam as redes sociais somente quando estão em um intervalo entre atividades. Percebeu-se que a maioria, representando 50,22%, estão sempre compartilhando, postando e vendo assuntos do seu interesse, o que já foi evidenciado por Jones e Soltren (2005), que dizem em seu artigo “*Facebook: Threats to Privacy*” que os usuários compartilham uma variedade de informações sobre si mesmos em seus arquivos no Facebook, incluindo fotos, informações de contato e gostos em filmes e livros e que embora a quantidade necessária de informações para uma conta do Facebook seja mínima, quantidade total de informações que um usuário pode postar é grande.

Uma das questões tinha como objetivo indagar os entrevistados se eles tinham costume de ler as políticas de privacidade, geralmente na criação de uma nova rede social, e 67,84% dos entrevistados disse nunca ter lido, 12,78% disseram que leram, entenderam e concordaram, 10,79% alegaram terem lido, mas não entendido e apenas 8,59% responderam ter lido, entendido e não concordado. Segundo a pesquisa realizada, 46,48% declararam já terem alterado algumas opções de configurações de privacidade, 35,90% disseram ter alterado a maior parte das configurações, 8,37% disseram não se

recordar, 5,73% não alterou nada e 3,52% das pessoas alegaram que não sabem fazer essa mudança e acham confuso/difícil.

Tabela 1 – Síntese Das Questões de Escala

PERGUNTA	1	2	3	4	5
Com que frequência você compartilha sua localização?	9,55%	34,47%	8,56%	39,61%	9,81%
Qual é seu grau de confiança na segurança dos seus dados pessoais nas redes sociais?	11,40%	22,43%	35,02%	24,26%	6,89%
Nos diga de 1 a 5, quanto a notícia sobre o vazamento de dados, te influenciou na utilização das redes sociais?	18,97%	13,55%	28,75%	17,42%	21,30%
Você sente que as redes sociais invadem a privacidade das pessoas? Como, por exemplo, a possível venda de seus dados pessoais, vulnerabilidade das redes sociais e etc.	1,96%	3,70%	11,60%	24,44%	58,30%

Foi decidido colocar as perguntas em uma tabela, usando a escala de 1 a 5, sendo menos seguro o número 1 e 5 para mais seguro. Já o número 3 é para aqueles casos em que os questionados sentem indiferença ou estão com dúvida.

Em uma das perguntas, questionou-se os entrevistados se eles haviam sido notificados sobre o vazamento de dados do Facebook em 2018. Identificou-se que 56,17% acharam que os dados não foram vazados e 23,35% declararam não ter tido conhecimento sobre esse vazamento de dados. 13,88% dos entrevistados alegaram não terem sido notificados, mas acreditam que são uns dos 443 mil brasileiros atingidos pelo vazamento. 6,61% afirmaram que foram notificados, sendo que 6,39% não fez nada e 0,22% não gostou de saber que seus dados foram vazados e entrou na justiça.

Após o questionamento sobre se as pessoas tinham conhecimento sobre o vazamento de dados de 2018 declarado pela empresa Facebook, foi perguntado se alguma empresa já tinha utilizado algum dado do respondente, obtido através das redes sociais para oferecer algum produto ou serviço e 41,41% declarou que não gostaria que isso acontecesse, 39,21% disseram que já foram abordados algumas vezes. 8,37% alegaram não terem sido abordados, mas se caso acontecesse, não se importariam. 11,02% declararam terem sido abordados, 5,95% contaram que só aconteceu uma vez e 5,07% contaram que não se importariam com essa abordagem. Analisou-se que 50,23% dos entrevistados já foram abordados por

terceiros, corroborando com os argumentos apresentador por Jones e Soltren (2005), de que as críticas em seu artigo são baseadas no fato de que terceiros podem usar o Facebook para mineração de dados, *phishing* e outras finalidades maliciosas.

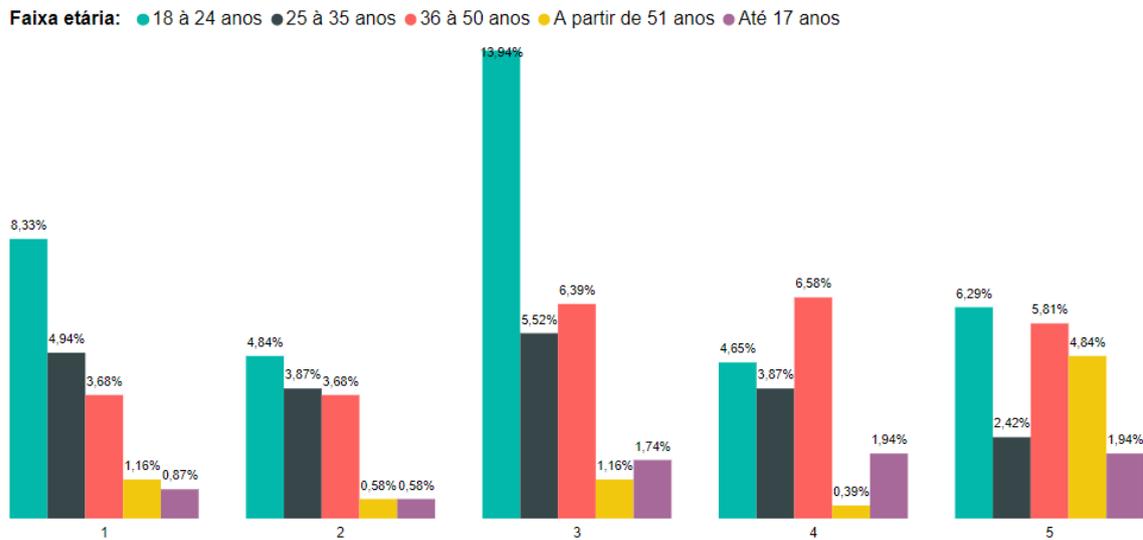
A coleta de dados tinha como objetivo saber se as pessoas perceberam alterações nas configurações e política de privacidade, sendo assim, 39,65% disseram não prestar atenção nessas mudanças e 31,06% assinalaram que não perceberam essas mudanças e que as detentoras das redes sociais deveriam comunicar de uma forma clara. 12,11% declararam que perceberam as mudanças, mas não puderam fazer nada a respeito. 10,57% contaram terem sido notificados pela rede social, mas não entenderam nada. E o restante, representando 6,61%, declararam terem percebido as mudanças, mas não se importaram com elas.

A fim de entender se os usuários sentiam que os seus dados estavam seguros quando alguma alteração na política de privacidade era feita, foi feita tal pergunta, e 34,36% disseram que não, porque as redes sociais serão sempre vulneráveis a hackers, 25,33% declararam sentir que os seus dados estão seguros, pois as redes sociais passam uma sensação de cuidado. 14,54% relataram que se sentem seguros, mas não veem qualquer diferença. 13,66% mencionaram sentir que as redes sociais não se importam com vazamentos ou possíveis vazamentos de dados e 13,66% contaram que para eles são indiferentes.

Encerrando o questionário, questionou-se os usuários o que os levaria a deixar de utilizar as redes sociais e 36,34% disseram que deixariam de utilizar as redes sociais se soubessem que os seus dados estão sendo vendidos, sem a sua permissão, para empresas. 36,43% relataram que deixariam de utilizar as redes sociais atuais se surgisse uma rede social mais “legal” e mais segura, 25,33% exprimiram deixar de utilizar caso houvesse um excesso de informação, notícias fúteis e irrelevantes, 7,27% caso houvesse um grande escândalo sobre vazamentos de dados e, por fim, 4,63% nunca deixariam de utilizar as redes sociais por confiar na privacidade de dados.

Realizando assimilações, na pergunta que visava saber o quanto a notícia sobre o vazamento de dados influenciou na utilização das redes sociais, constatou-se que para a faixa etária de 18 a 24 anos essa notícia era indiferente, sendo assim não houve influência no seu modo de utilização nas redes sociais. Além disso, para as pessoas maiores de 36 anos, notou-se o quanto essas notícias sobre o vazamento de dados influenciaram na utilização das redes sociais. As pessoas a partir de 51 anos declararam que influenciou muito, representando 4,84%.

Gráfico 3 – Assimilação Entre Faixa Etária E Vazamento De Dados

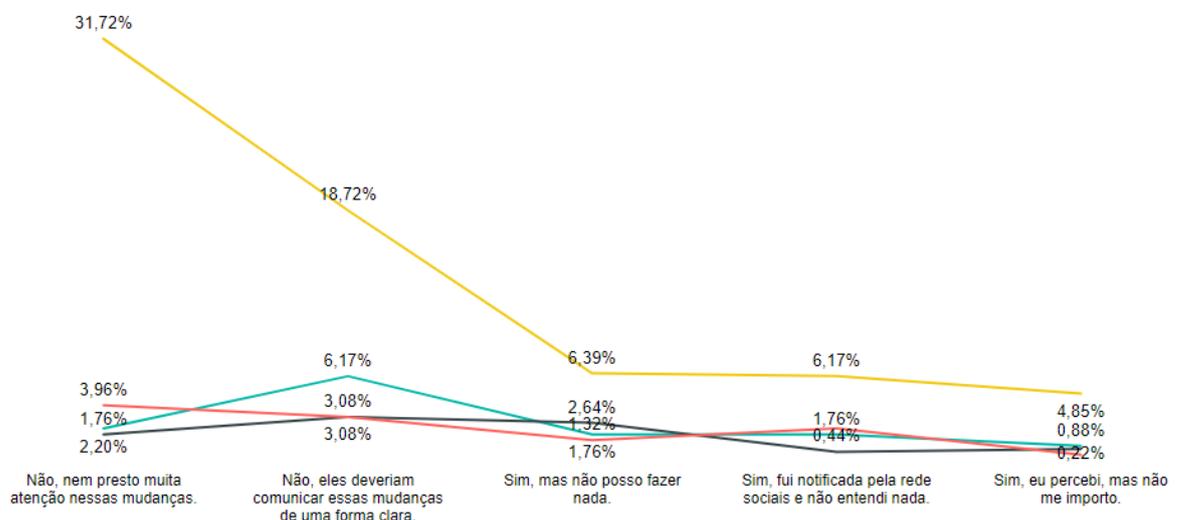


\*Escala de 1 a 5 (sendo 1 pouca influência e 5 muita influência)

Em um outro ponto, percebeu-se que 67,84% dos respondentes não leem a política de privacidade das redes sociais, equiparando as pessoas que não costumam ler a política com a percepção dos usuários sobre as alterações nas configurações e política de privacidade após o vazamento, observou-se que 31,72% daqueles que nunca leram, não sabem das mudanças. Além disso, os usuários que costumam ler a política, representando 6,17%, não souberam das mudanças e acreditam que as redes sociais deveriam comunicar de uma forma mais clara.

Gráfico 4 – Percepção sobre as alterações de configuração VS. leitura da política de privacidade

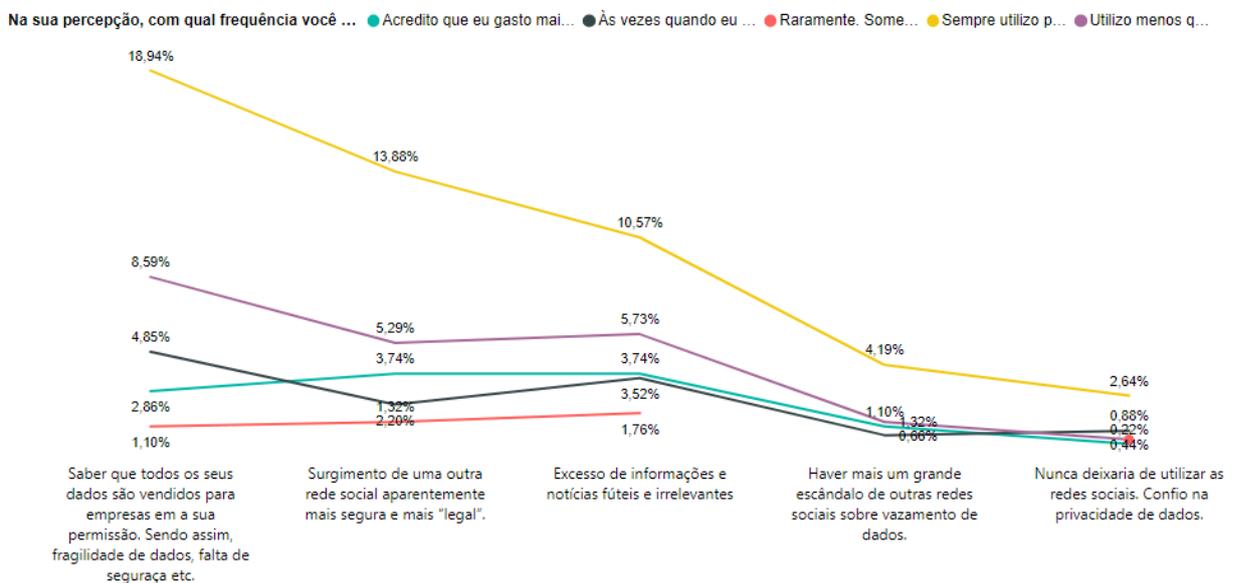
Você tem costume de ler a polític... ● Li, entendi e concordo. ● Li, entendi e não concordo. ● Li, mas não entendi. ● Nunca li.



Por semelhança, foi constatado, ao fazer o cruzamento das pessoas sobre o que as levariam a deixar de utilizar as redes sociais e a frequência delas no Facebook, Instagram, WhatsApp e Twitter etc, que 18,94% das que sempre utilizam as redes sociais deixariam de utilizar caso soubessem que todos os seus dados são vendidos para as empresas sem sua permissão. As pessoas que utilizam sempre, representando 13,88% e 10,57% respectivamente, estão entre surgimento de uma rede social aparentemente mais segura e mais “legal” e excesso de informações e notícias fúteis e irrelevantes.

Para aqueles usuários que responderam que raramente utilizam, eles não deixariam caso houvesse mais um grande escândalo de outras redes sociais sobre o vazamento de dados, essas pessoas só deixaram de usar por outros motivos e o principal seria o surgimento de uma rede sociais aparentemente mais segura e mais “legal”. Sendo assim, quando olhamos todas as pessoas que responderam essa pesquisa, 36,34% só deixariam as redes sociais caso soubessem que todos os seus dados estão sendo vendidos para empresas sem a sua permissão.

Gráfico 5 – Frequência de utilização das redes sociais VS. Porque os usuários deixariam de usar redes sociais



Portanto, corroborando com os argumentos apresentados por Jones e Soltean (2005) de que, embora as falhas de privacidade do Facebook estivessem bem documentadas e tenham entrado na mídia, relativamente pouca pesquisa está disponível sobre como exatamente esses problemas afetam os usuários do Facebook e o quanto os usuários sabem e se preocupam com estas questões. Os argumentos

apresentados pelos autores vão de encontro com a quantidade de pessoas que se importaram com o vazamento de dados, os motivos do qual fariam elas deixarem de utilizar as redes sociais e entre outras perguntas expostas nesse artigo.

## **5 CONSIDERAÇÕES FINAIS**

O objetivo desta pesquisa foi de analisar a percepção dos usuários sobre a vulnerabilidade das informações nas redes sociais. Por meio da coleta dos dados e análise dos resultados podemos destacar que em sua maioria, os usuários das redes sociais reconhecem o que representa a privacidade de dados, a política de privacidade e as ferramentas para alterar as configurações de privacidade para garantir a segurança nos dados. No entanto, notou-se um comportamento diverso com relação a garantia de segurança, uso e compartilhamento de informações, bem como percepção sobre os vazamentos dos dados.

De acordo com os resultados, no público mais jovem, entre os 17 e 24 anos, mesmo sabendo sobre o vazamento de dados e a possível exposição deste conteúdo, o mesmo grupo afirmou que não deixaria de utilizar as redes sociais por esse motivo. Já para os grupos com idade superior, há uma maior preocupação sobre o quanto os dados pessoais podem estar expostos e sendo utilizados para fins desconhecidos.

Este estudo corrobora, de uma maneira mais enfática, com os resultados já apresentados por Jones e Soltren (2005), que mostraram que 74% dos usuários das redes sociais estão cientes das opções de privacidade, no entanto, apenas 62% realmente fazem o uso desta ferramenta. Ao mesmo tempo que os usuários demonstram preocupação com a privacidade dos dados, os usuários postam grandes quantidades de informações pessoais, dados demográficos, como idade, sexo, localização e seus interesses, demonstrando assim um certo grau de confiança pelas configurações de privacidade e política de privacidade e termos de serviço das redes sociais.

Essas descobertas mostram que o Facebook bem como outras redes sociais apresentam riscos à privacidade de seus usuários. Ao mesmo tempo, eles são extremamente populares e parecem fornecer um alto nível de gratificação aos seus usuários, e por essa razão, pode-se supor que a gratificação esperada motiva os usuários a fornecer e atualizar frequentemente dados pessoais muito específicos que a maioria deles imediatamente se recusam a revelar em outros contextos, como uma pesquisa por telefone. Assim, as redes sociais fornecem um ambiente ideal, rico em dados, para o marketing de microssegmentação e publicidade, especialmente quando os perfis de usuário são combinados com funções que acompanhem o comportamento do usuário, conforme já destacado por Beacon. (HORN et al., 2009).

A contribuição da pesquisa consiste na ampliação e descrição do fenômeno de vulnerabilidade de dados, no que tange as redes sociais, um campo ainda pouco explorado por pesquisas acadêmicas. Acredita-se que para além deste trabalho, estudos futuros sejam realizados com um aprofundamento sobre o comportamento destes usuários, com relação ao perfil de uso da internet e costumes sociais, buscando entender o comportamento durante o uso das redes e uma maior ênfase para a vulnerabilidade das informações pessoais, informações bancárias/econômicas e a possível relação com crimes cibernéticos, assim como faz se necessário também o estudo do viés das empresas sobre a vulnerabilidade dos dados e o impacto da privacidade das informações para a gestão das organizações.

### REFERÊNCIAS

- BOYD, D. M.; ELLISON, N. B. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, v. 13, n. 1, 1 out. p. 210 - 230 2007.
- DAQUINO, Fernando. A História das redes sociais: como tudo começou. nov. 2012. Disponível em: <<https://www.tecmundo.com.br/redes-sociais/33036-a-historia-das-redes-sociais-como-tudo-comecou.htm>>. Acesso em: 20 set. 2018.
- DAVENPORT, T. H. *Ecologia da informação: Porque só a tecnologia não basta para o sucesso na era da informação*. São Paulo: Futura, 1998.
- DEBATIN, B. et al. Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, v. 15, n.1, 1 out. 2009, p. 83 - 108. Disponível em:<<https://doi.org/10.1111/j.1083-6101.2009.01494.x>>. Acesso em: 13 out. 2018.
- DWYER, C. ET AL. Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *Proceedings of AMCIS 2007, Keystone*, dez. 2007. Disponível em: <<https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1849&context=amcis2007>>. Acesso em: 13 out. 2018.
- FACEBOOK. Política de Dados. Disponível em: <<https://pt-br.facebook.com/privacy/explanation>>. Acesso em: 27 out. 2018.
- FACEBOOK. Segurança no Facebook. Disponível em: <<https://www.facebook.com/safety>>. Acesso em: 28 nov. 2018.
- FERREIRA, N.S.; ARRUDA FILHO, E. J. M. Usabilidade e preferência de uso na rede social Facebook: uma análise netnográfica dos usuários tecnológicos. *JISTEM - Journal of Information Systems and Technology Management*, São Paulo, SP, v. 12, n. 2, p. 415-434, mai/ago., 2015.

- GABRIEL, M. Marketing na era digital: conceitos, plataformas e estratégias. São Paulo: Novatec, 2010. 424 p. ISBN 9788575222577.
- HOOTSUITE. The global state of digital in 2018 – from Argentina to Zambia. Disponível em <<https://hootsuite.com/pt/pages/digital-in-2018>>. Acesso em: 26 mar. 2019.
- JONES, H.; SOLTREN, J. H. Facebook: Threats to privacy. dez. 2005. Disponível em: <<http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf>> Acesso em: 13 out. 2018.
- KAPLAN, A.; HAENLEIN, M. Social media: back to the roots and back to the future. ESCP Europe. 4f. Disponível em: <<http://www.michaelhaenlein.eu/Publications/Kaplan,%20Andreas%20-%20Back%20to%20the%20roots%20and%20back%20to%20the%20future.pdf>> Acesso em: 20 out. 2018.
- KEMP, Simon. Digital in 2018: world`s internet users pass the 4 billion mark. Disponível em <<https://wearesocial.com/blog/2018/01/global-digital-report-2018>>. Acesso em: 26 mar. 2019.
- KEMP, Simon. Number of social media users passes 3 billion with no signs of slowing. Disponível em: <[https://thenextweb.com/contributors/2017/08/07/number-social-media-users-passes-3-billion-no-signs-slowing/#.tnw\\_CzcMScMP](https://thenextweb.com/contributors/2017/08/07/number-social-media-users-passes-3-billion-no-signs-slowing/#.tnw_CzcMScMP)>. Acesso em: 11 nov. 2018.
- MARTELETO, R.M. 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. Brasília, 2010.
- MCGEE, J.; PRUSAK, L. Gerenciamento estratégico da informação: Aumente a competitividade e a eficiência de sua empresa utilizando a informação como uma ferramenta estratégica. 24. ed. Rio de Janeiro: Campus, 1994.
- MILLER, M. D.; BRUNNER, C. C. Social impact in technologically-mediated communication: An examination of online influence. Computers in Human Behavior. v. 24, n. 6, p. 2972–2991, 30 jun. 2008. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S0747563208001015>> Acesso em: 13 out. 2018.
- RECUERO, R. Redes Sociais na Internet. Porto Alegre: Editora Meridional, 2009.
- SÊMOLA, M. Gestão da segurança da informação: Uma visão executiva. 1. ed. Rio de Janeiro: Campus, 2003.
- TORRES, C. A bíblia do marketing digital: tudo que você queria saber sobre marketing e publicidade na internet e não tinha a quem perguntar. São Paulo: Novatec, 399 p. 2009.

VI SECIN Seminário em Ciência da Informação - Fenômenos Emergentes na Ciência da Informação. 2016, Londrina. Análise de Redes Sociais: Uma Década de Publicações. Londrina: 2016. Disponível em: <<http://www.uel.br/eventos/cinf/index.php/secin2016/secin2016/paper/view/342/168>>. Acesso em: 23 out. 2018.

VERGARA, S. Projetos e relatórios de pesquisa em administração. 5. ed. São Paulo: Atlas, 2004.