Revista ACB: Biblioteconomia em Santa Catarina,
Florianópolis, v. 24, n. 2, p. 357-372, abr./jun., 2019.

ANÁLISE DA EXPOSIÇÃO DE INFORMAÇÕES PESSOAIS E PROFISSIONAIS NOS PERFIS DE BIBLIOTECÁRIOS(AS) BRASILEIROS(AS) NO FACEBOOK

Danielle Borges Pereira[1]
Elisa Cristina Delfini Correa[2]

Resumo: Pesquisa netnográfica, de caráter descritivo e exploratório, que analisa as publicações pessoais de bibliotecários(as) brasileiros(as) no Facebook, a fim de identificar que tipo de informações pessoais e profissionais estão disponíveis em seus perfis e quais os riscos decorrentes dessa disponibilização. Discute cultura digital, segurança da informação, engenharia social e competência em informação. Foram levantados dados nos perfis dos(as) bibliotecários(as) no Facebook a partir de uma amostra aleatória de 63 bibliotecários(as), selecionando-os por meio de suas atuações nas Universidades Federais, Estaduais e Bibliotecas Públicas de cada estado. Como resultado, foi possível verificar a exposição de informações pessoais que tornam os/as bibliotecários/as vulneráveis a ataques no ambiente virtual. Conclui-se ser necessária a discussão sobre o tema entre os profissionais da área, bem como, envolver bibliotecas e universidades como meio de sensibilizar os(as) usuários(as) da internet de modo geral, a fim de promover uma cidadania mais consciente, crítica e competente no que se refere a criar, desenvolver e disseminar as informações.

Palavras-chave: Exposição de informações. Cultura digital. Competência em informação. Facebook. Bibliotecários(as).

1 INTRODUÇÃO

A cada ano que passa surgem novos modos, aplicativos e dispositivos para realizar essas trocas de informações, cada vez mais interativas e instantâneas, exemplo disso são as mídias sociais que proporcionam uma comunicação cada vez mais interativa e instantânea. No que se refere às mídias sociais a mais utilizada atualmente é o Facebook, com 2.320 bilhões de contas ativas no mundo, conforme pesquisa realizada pela empresa alemã Statista, em abril de 2019[3].

O Facebook é um *website* que liga os perfis de seus usuários, fazendo com que as informações expostas em suas páginas pessoais possam ser vistas por seus amigos ou por todo

[1] Mestranda em Ciência da Informação (PGCIN) pela Universidade Federal de Santa Catarina (UFSC), com graduação em Biblioteconomia e Habilitação em Gestão da Informação pela Universidade do Estado de Santa Catarina (UDESC/2018). E-mail: danielle.borges.pereira@gmail.com

2 Graduada em Biblioteconomia pela Universidade do Estado de Santa Catarina (1995), mestre em Sociologia Política pela Universidade Federal de Santa Catarina (1999) e doutora em Sociologia Política pela Universidade Federal de Santa Catarina (2008). E-mail: elisacorrea61@gmail.com

[3] STATISTA. **Redes sociais mais populares em todo o mundo a partir de abril de 2019, classificadas por número de usuários ativos (em milhões).** 2018. Disponível em: <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>. Acesso em: 10 jun. 2019.

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

o público (CORREIA; MOREIRA, 2014). Possui diversas funcionalidades interativas, entre elas o compartilhamento de informações, publicações de fotos e vídeos, utilização de *tags*, calendários de eventos e aniversários, conversas pessoais ou em grupos, além de permitir uma maior interação, sendo possível curtir, comentar e compartilhar informações já postadas. (CORREIA; MOREIRA, 2014).

Essas novas formas de conexão e a grande quantidade de informações disponíveis fazem com que as pessoas que utilizam essas mídias sociais estejam vulneráveis a perigos em relação ao excesso de informações pessoais e profissionais expostas na internet, tornando-se vulneráveis aos crimes virtuais, por exemplo.

Sendo assim, esta pesquisa tem como intuito estudar as publicações pessoais e profissionais de bibliotecários(as) brasileiros(as) disponibilizadas no item 'Sobre' em seus perfis no Facebook, analisando-as, com o propósito de refletir acerca das consequências que a exposição dessas informações pode acarretar para as suas vidas.

Considerando a crescente tendência de utilização das mídias sociais e, tendo em vista, os perigos que podem estar associados a elas, este trabalho busca responder à seguinte questão: Que tipo de informações pessoais e profissionais estão disponíveis em perfis de bibliotecários(as) brasileiros(as) no Facebook e quais os riscos decorrentes dessa exposição, para os próprios profissionais e seus familiares e amigos?

Com o intuito de responder tal questão, a presente pesquisa buscou: a) Identificar as categorias de informações pessoais e profissionais disponibilizadas pelos(as) bibliotecários(as); b) Categorizar os riscos decorrentes dessa exposição no Facebook; c) Refletir sobre a responsabilidade social do(a) bibliotecário(a) em relação à conscientização quanto aos perigos e direitos dos cidadãos no ambiente digital.

2 REFERENCIAL TEÓRICO

A presente seção discute conceitos e ideias fundamentais para o desenvolvimento do tema proposto, a saber: cultura digital, segurança da informação, engenharia social e competência em informação.

2.1 CULTURA DIGITAL

Desde a era pré-histórica, o ser humano possui e sente a necessidade de registrar suas rotinas e seus conhecimentos, fazendo com que a nossa história passe a ser construída por

meio dessas informações. É através disso que possuímos tantas informações e saberes a respeito do passado. Ao longo da história as tecnologias evoluíram e hoje temos novas maneiras de disseminação de informações como os computadores e o armazenamento em nuvem decorrentes das mudanças por que passaram as sociedades humanas. (GARCIA; SOUSA, 2011).

Sobre essas mudanças na sociedade, Pierre Lévy (1999) afirma que, quando as formas de construção da memória e de sua transmissão aumentam ou são criadas novas interfaces que interferem no sistema cognitivo humano – como a realidade virtual, ou até mesmo trazendo essa questão para os dias atuais, com a chegada das mídias sociais – ou as formas de produzir conteúdo se modificam, ocorre que o digital ganha cada vez mais espaço nos processos realizados pela sociedade, sendo necessário reavaliar essas implicações culturais e sociais. Essa afirmação do autor deve-se ao fato de que é a partir dessas mudanças que se iniciam novas culturas, com novas formas de comunicação, criação, organização, planejamento e disseminação da informação.

O termo ciberespaço foi utilizado pela primeira vez por William Gibson, em 1984, em seu romance *Neuromante*, do qual emprega o termo ciberespaço como uma palavra utilizada para designar um "[...] universo das redes digitais, descrito como campo de batalha entre as multinacionais, palco de conflitos mundiais, nova fronteira econômica e cultural.". Esse termo foi retomado pelos criadores e usuários das redes digitais e atualmente existe uma pluralidade de correntes artísticas e até políticas que se dizem parte da cibercultura. Por fim, Lévy define "[...] o ciberespaço como o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores." (LÉVY, 1999, p. 92).

Como qualquer outra cultura que se constrói em determinado espaço social, a cibercultura é produto socialmente construído pela humanidade nos ambientes virtuais (ciberespaço), sendo o surgimento de uma nova sociedade com costumes e conexão com o ciberespaço. Em seu programa de desenvolvimento da cibercultura, Pierre Lévy (1999) traz os três princípios que conduzem o desenvolvimento inicial do ciberespaço, sendo eles: a interconexão (ligada à origem do ciberespaço, a conexão sempre fará parte do seu processo), a criação de comunidades virtuais (complementam o primeiro, pois a formação de comunidades virtuais está ligada à interconexão) e a inteligência coletiva (perspectiva espiritual da

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

cibercultura da qual participa um grupo de humanos que possuem o interesse pela busca e aproximação do ideal do coletivo inteligente).

A democracia moderna que emergiu da Europa no século XVIII trouxe a liberdade de expressão e a oportunidade de compartilhar a opinião pública, contudo, também trouxe consigo o poder da manipulação e da enganação, encontrado em muitas comunidades virtuais, assim como nas mídias de massa, como televisão, jornal e rádio. (LÉVY, 1999). Por causa disso, participantes das comunidades virtuais devem possuir competência para ler e debater criticamente sobre o que se está lendo em especial por causa da grande quantidade de informação criada e disseminada nesse ambiente e da notória dificuldade de muitos usuários em saber distinguir as informações verdadeiras das falsas.

Conforme Correa e Silva (2017), estar no ambiente digital, utilizando-se das mídias sociais para compartilhamento de informações pessoais ou não, é mostrar quem você é como indivíduo e como profissional. Esses fatores possuem pontos positivos, por exemplo, quando a pessoa que publica diversas informações se torna uma formadora de opinião. Entretanto, o excesso de informações disponíveis sobre tal pessoa pode torná-la vulnerável perante engenheiros sociais, que estão sempre alerta às informações pessoais que estão sendo expostas. Por isso é tão importante desenvolver competências para utilizar conscientemente as mídias sociais.

2.2 ENGENHARIA SOCIAL

De acordo com Mitnick e Simon (2003), a engenharia social utiliza de influência, persuasão e manipulação para enganar e coibir as pessoas e, assim, conseguem com maior facilidade ter acesso às informações e tirar proveito próprio das pessoas ou organizações com ou sem o uso da tecnologia.

Qualquer indivíduo pode ser um engenheiro social sem que seja necessário possuir uma formação específica. Atua em diversas áreas, desde ataques a pessoas físicas e até a empresas de grande porte. Esses profissionais utilizam, na maioria das vezes, da conversa e simpatia para conseguirem as informações que necessitam para utilizá- las de forma negativa. São espertos e estratégicos, estudam as pessoas e o ambiente no qual estão entrando, identificam os pontos fracos e fortes de suas vítimas e a partir de então iniciam seu plano para atacar a pessoa ou organização que desejam. (SILVA; ARAÚJO; AZEVEDO, 2013).

O engenheiro social, após identificar as características do ambiente e do(s) indivíduo(s)

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

que irá atacar, processa o reconhecimento de informações percorrendo quatro etapas, sendo estas, 1) coletar o máximo de informações possíveis; 2) desenvolver um relacionamento com a vítima, se tornando uma pessoa de confiança; 3) exploração, quando a vítima começa a ser manipulada para passar informações secretas; e 4) execução, quando o engenheiro consegue o que estava procurando. (ALLEN, 2006, p. 5, tradução nossa).

A engenharia social pode começar com a estratégia individual e passar para corporativa, o engenheiro social pode recolher informações pessoais e/ou mercadológicas por meio das mídias sociais quando se tornam 'amigos' de um indivíduo ou quando utilizam perfis *fakes*. Podem, inclusive, criar um personagem específico, como um funcionário de determinada empresa, e ganhar a confiança de reais funcionários para recolher informações pessoais/profissionais com o fim de prejudicar indivíduos e empresas que possuem informações sigilosas. (SILVA; ARAÚJO; AZEVEDO, 2013).

Seguindo a perspectiva desse assunto voltado a mídia social Facebook, quando um perfil é criado, os usuários podem adicionar seus colegas e amigos para se conectarem e formar grupos por parentesco, por colegas de serviço, colegas de escola, de melhores amigos, entre outros, dependendo do círculo de amizade que deseja enquadrar o grupo, sendo assim "Uma opção que talvez seja diferente dos outros sites é se tornar assinante de seus amigos para receber o *feed* de notícias. Essa opção também pode ser escolhida para pessoas não amigas.". Com essa função, o usuário irá possuir acesso à todas as informações postadas na *timeline* (conhecida também como linha do tempo) da pessoa ou organização em que está seguindo, podendo recebê-las via *e-mail* e SMS. (SILVA; ARAÚJO; AZEVEDO, 2013, p. 43).

A comunicação no Facebook ocorre principalmente por meio de publicações de fotos, vídeos e textos na sua própria linha do tempo, em álbuns separados por temas ou na linha do tempo de seus amigos, essas postagens podem ser curtidas e/ou compartilhadas, os usuários também podem criar eventos e utilizar a mídia social em qualquer ferramenta (computador, notebook, tablet e celular). A rede social possui ainda ligação com outros aplicativos, essas conexões fazem com que essa mídia se transforme em um terreno fértil para os ataques de engenharia social. (SILVA; ARAÚJO; AZEVEDO, 2013).

2.3 SEGURANÇA DA INFORMAÇÃO

Considerando o grande crescimento de informações ofertadas e recebidas e o

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

desenvolvimento de tecnologias da informação para facilitar o seu acesso a sociedade fez com que a sua utilização no dia-a-dia aumentasse cada vez mais, desde tarefas simples como assistir receitas no Youtube a tarefas mais complexas realizadas no trabalho, favorece a visualização de como ocorre as atividades sociais na década em que vivemos, tornando-se necessário ampliar os estudos a respeito da segurança da informação. (SOUZA, 2015).

Para compreender a segurança da informação, é necessário estabelecer um conceito de informação nesse contexto: "Entende-se por informação qualquer conteúdo ou conjunto de dados com valor para determinada organização ou pessoa, sendo esta, um recurso de extremo valor na sociedade atual." (ABREU, 2011, p. 11).

A segurança da informação se torna cada dia mais relevante a fim de evitar que ocorram inconsistências na proteção dos dados, garantindo segurança aos indivíduos e organizações que utilizam as tecnologias da informação, reduzindo "[...] riscos de fraudes, erros, vazamento, roubo e uso indevido e uso indevido de informações.". (ABREU, 2011, p. 12).

A segurança da informação está preocupada com alguns princípios, sendo estes, a confidencialidade (propriedade da informação, que esteja exposta somente para os indíviduos e entidades autorizados), integridade (manter a integridade e originalidade da informação) e a disponibilidade (acessivel, disponivel e utilizavel para todos que estão autorizados), outras propriedades podem estar envolvidas, "[...] tais como autenticidade, responsabilidade, não repúdio e confiabilidade[...]." (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2006, p. 2).

Mitnick e Simon (2003) falam a respeito do perigo do fator humano para a eficácia da segurança da informação, pois os seres humanos muitas vezes possuem a ilusão de estarem sendo protegidos, como se uma política de segurança da informação em alguma empresa ou website da internet, já fosse por si só um mecanismo único e suficiente para assegurar que nada de ruim irá lhe acontecer com as informações dispostas. Porém para os autores, não é necessário treinar apenas um sistema, mas as pessoas também, conscientizá-las dos perigos e mostrar que não estão completamente protegidas somente porque possuem algum sistema de segurança.

Atualmente, as formas de obter segurança são por meio das novas tecnologias desenvolvidas com esse intuito e também com o objetivo de vigilância, visando a proteção e controle dos perigos que nos cercam, pois, os cenários mudaram tanto da parte da vigilância quanto dos vigiados, indicando o cenário contemporâneo de desigualdade mundial.

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

(BAUMAN; LYON, 2012).

Bauman traz o termo "vigilância líquida" para compreender a insegurança e a necessidade de vigilância por parte dos indivíduos para que se sintam cada vez mais seguros, seguindo seu discurso sobre a 'liquidez' da modernidade. O termo "vigilância líquida" é utilizado reforçando a liquidez contemporânea que nos faz tentar com todas as forças sobreviver ao medo no mundo atual, tornando a convivência humana a mais suportável possível, apesar de que cada ampliação desse novo sentimento produz outros riscos e novos medos. (BAUMAN; LYON, 2012).

Esse tipo de vigilância, segundo os autores, se dá por dois fatores: o primeiro é a facilidade de desconstruir em alta velocidade as formas sociais criadas e o surgimento de novas formas que não se solidificam e que não mantém um molde por longos períodos. O segundo fator trata do poder e da política como itens da sociedade que estão se separando: o poder está se expandindo e existindo de forma global, já a política ocorre o contrário, por mais que ainda esteja ligada ao público, ainda está ligada a um território específico e impossibilitada de interagir globalmente. (BAUMAN; LYON, 2012).

Como visto, os indivíduos podem ser considerados a fraqueza dos sistemas de segurança da informação, tanto em recursos físicos como nos digitais, mostrando a ligação entre a engenharia social e a segurança da informação e o fato de que a ação dos engenheiros sociais pode prejudicar alguns sistemas de segurança da informação. Por isso torna-se importante além da formulação de políticas de segurança da informação, investir em capacitação para construir competências e habilidades em ambientes digitais. (SILVA; ARAÚJO; AZEVEDO, 2013).

2.4 COMPETÊNCIA EM INFORMAÇÃO

A informação e o conhecimento são pontos fundamentais para o desenvolvimento humano e a formação de uma sociedade e de sua cultura, são fatores de sobrevivência humana e do desenvolvimento sustentável. A criação de novos conhecimentos, o acesso a informação e o desenvolvimento da comunicação foram e ainda são fatores que contribuem para o desenvolvimento social e econômico da população, sendo o bem mais precioso dos seres humanos. (MOELLER et al., 2011, tradução nossa).

Com a chegada e concretização das Tecnologias de Informação e Comunicação (TIC), verifica-se o aumento e a promoção do crescimento das redes sociais e sites de

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

entretenimento, fazendo com que estivesse ao alcance de muitas pessoas o acesso à criação, distribuição e disseminação de informações em diversos formatos. (MOELLER et al., 2011, tradução nossa). Por esse motivo, as habilidades para o uso eficaz dos recursos da internet, inclusive das mídias sociais, fazem parte da chamada competência digital.

Antes de discutir esse conceito, no entanto, será feita uma breve introdução à competência em informação (CoInfo), cujos primeiros estudos realizados se deram em 1974, nos Estados Unidos da América, sendo introduzida no Brasil no início dos anos 2000. (ANGELO, 2016). A CoInfo, conforme Angelo (2016), significa a competência de um indivíduo em aprender e ensinar a realizar buscas e avaliações de informações, assim como possuir competência para utilizá-las e criar novas informações atingindo seus objetivos pessoais, acadêmicos, sociais e profissionais.

Pensar, criar e fomentar competências para a utilização dos ambientes digitais, faz-se extremamente necessário nos dias atuais, principalmente para os profissionais da informação como os(as) bibliotecários(as). “O processo de avaliar as informações, embora complexo, é essencial para a tomada de decisão efetiva, seja na votação, na seleção da melhor medicação ou na identificação do melhor curso de ação.” (MOELLER et al., 2011, p. 5, tradução nossa).

Coelho e Silva (2016) afirmam que as redes sociais, por mais que estejam sendo utilizadas de forma superficial, estão se mostrando um importante canal de comunicação entre leitores(as) e bibliotecários(as), por meio das quais podem ensinar o uso eficiente destas ferramentas, criar conteúdo por meio de pesquisas e formar cidadãos críticos nos ambientes digitais.

Em vista disso, é correto considerar que é preciso expandir a utilização dessas tecnologias e de torná-las aliadas dos profissionais da informação, para que eles possam ensinar o uso eficiente dessas ferramentas, criar conteúdo por meio de pesquisas e formar cidadãos críticos nos ambientes digitais.

Como exemplo, a publicação de informações pessoais e eventualmente profissionais dos(as) bibliotecários(as) em seus perfis no Facebook, atenta às questões éticas da disponibilização e uso da informação, reflete questões de segurança da informação e protege de possíveis ataques de engenharia social. Da mesma forma que a segurança da informação dá competência, por outro lado, permite não se deixar levar pela sensação de segurança ofertada pela mídia social e assim, não ser alvo fácil de pessoas mal-intencionadas.

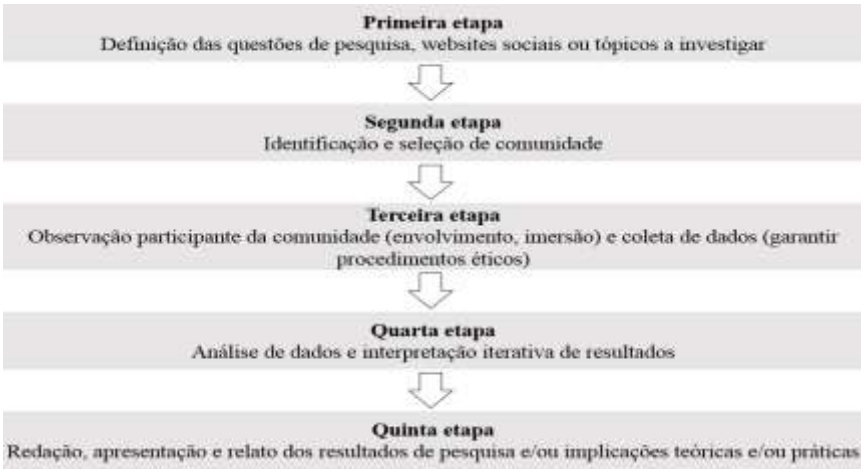
Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

3 PROCEDIMENTOS METODOLÓGICOS

A pesquisa segue a abordagem descritiva e exploratória de caráter qualitativo, bibliográfica e documental, utilizando o método netnográfico para elencar os parâmetros de observação utilizados na coleta e análise de dados.

Conforme Vicente (2015) a netnográfica surgiu das questões culturais e estudos antropológicos e etnográficos, com o diferencial de como se realiza a análise, da qual ocorre a partir das redes sociais na internet, sendo utilizada para o levantamento de informações referentes a informações disponibilizadas dos(as) bibliotecários(as) no Facebook, seguido seis passos exemplificados na figura abaixo:

Figura 1 - Fases pesquisa netnográfica



Fonte: Kozinets, 2014.

A seleção dos perfis analisados nessa pesquisa foi realizada a partir de uma amostra aleatória de bibliotecários(as) atuantes nas regiões brasileiras em Universidades Federais, Universidades Estaduais e Bibliotecas Públicas de cada estado brasileiro, constatando de um profissional por instituição, ou seja, três bibliotecários(as) por estado, totalizando 81 bibliotecários(as). Os critérios de seleção foram: a) possuir perfil pessoal no Facebook; b) estar atuando na área da Biblioteconomia no período de realização da pesquisa (2018) e c) a biblioteca em que o profissional está atuando, possuir website para sua identificação no quadro de funcionários em atividade.

Após a realização de etapas de triagem que envolveram a localização de páginas institucionais de universidades e instituições públicas de cada estado brasileiro e identificação de bibliotecários atuantes em suas bibliotecas (em páginas web das instituições e currículo Lattes), totalizou uma amostra de 63 bibliotecários(as) a serem analisados(as).

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

As informações pessoais coletadas dos perfis desses profissionais, assim como sua identificação, não serão reveladas na pesquisa. O levantamento de dados nos perfis do Facebook dos(as) bibliotecários(as) foi realizado por meio de observação descritiva e, após a coleta, os dados foram transportados para a ferramenta Excel para uma melhor visualização e análise, transformando-os em informações visíveis por meio de gráficos.

4 RESULTADOS

A amostra de 63 profissionais foi dividida em regiões: nove bibliotecários(as) da região Sul, 11 bibliotecários(as) da região Sudeste, nove bibliotecários(as) da região Centro-Oeste, 12 bibliotecários(as) da região Norte e 22 bibliotecários(as) da região Nordeste. A análise foi realizada por meio das informações pessoais e profissionais disponíveis no item 'Sobre' (onde trabalha/trabalhou, onde estuda/estudou, onde mora, localização/visitas, nascimento, gênero, telefone, família, outras informações e acontecimentos importantes) e o modo de publicação (público, privado ou amigos e conexões) do Facebook.

Dos 63 bibliotecários(as) pesquisados(as), a maioria foi do gênero feminino, tendo como participantes 39 bibliotecárias (72% feminino) e 15 bibliotecários (28% masculino), sendo que nove profissionais não informaram o gênero em seu perfil.

Sobre a disponibilização de informações no Facebook dos(as) profissionais analisados(as), de modo geral verificou-se uma grande exposição de informações a respeito da formação, gênero, local de trabalho, acontecimentos importantes (como exemplo início de relacionamentos) e a localização ou locais em que visitou, como demonstrado no Gráfico 1:

Gráfico 1 - Exposição de informações no Facebook dos profissionais analisados

Fonte: Dados da pesquisa, 2018.

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

A quantidade de informações postadas pelos usuários faz com que estejam mais suscetíveis aos ataques de engenharia social, visto que facilitam o conhecimento dos lugares onde moram, onde trabalham, indicam instituições em que se formaram, apresentam seus familiares, etc. O engenheiro social sabendo de tais informações pode aplicar golpes, como por exemplo, furto de identidade, *phishing (*manipulação do indivíduo para obter dados e informações pessoais e financeiros*)*, golpes por meio de sites fraudulento e/ou golpes por meio da modificação da navegação do usuário para sites falsos (*pharming*).

Em relação às informações disponibilizadas com maior ocorrência (números indicados entre parênteses), as que oferecem maior perigo são: a) Formação Profissional (52); b) Gênero (51); c) Local onde trabalha (50); d) Onde mora (47); e) Acontecimentos importantes (46); f) Localização e visitas (45); g) Família (28); h) Nascimento (29).

Com menor grau de ocorrências e susceptibilidade média de exposição a perigos estão locais onde já morou (34) e trabalhou (24). Em último lugar de ocorrência, contudo, com alto grau de periculosidade, está o fornecimento do número de telefone para contato.

Considera-se alto o número de profissionais que informa seu local de trabalho, principalmente por ter em vista o perigo que esta informação pode causar ao usuário em mãos maliciosas, como planejamento de assaltos e sequestros.

Mais arriscado ainda é fornecer local de residência, tanto atual quanto anteriores, uma vez que permite aos criminosos virtuais traçar um histórico de vida que, somado às demais informações fornecidas, pode construir um quadro de relacionamentos e preferências que torna ainda mais vulnerável a pessoa cujas informações são expostas.

As informações a respeito da formação (grau de escolaridade e local de formação) e família (parentes classificados como, por exemplo: mãe, pai, tio/a, irmão/irmã, primo/prima, entre outros) também tiveram altos índices de disponibilidade pelos usuários, porém, apesar de não constituir perigo imediato, indicar a formação pode ser utilizado por criminosos digitais como um ponto de partida para uma aproximação dos engenheiros sociais, que podem iniciar conversas indicando falsos pontos em comum com as vítimas e, a partir daí, chegar a informações de caráter mais privado e confidencial

A indicação de familiares, principalmente os mais próximos como pais, filhos(as) e irmãos(ãs) pode acarretar em riscos não somente para o indivíduo que publica a respeito, mas também para o seu círculo de amizade e confiança.

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

As informações a respeito da data de nascimento foram encontradas em 29 perfis, um número relativamente alto. Muitas pessoas não compreendem os perigos da exposição dessa informação, porém, para um engenheiro social, esses dados podem facilitar seu processo de invadir sistemas de segurança da informação, como por exemplo, o uso da data de nascimento como senha de bancos, cartões e celulares.

Em relação ao gênero, a maior parte dos pesquisados informou esse dado: 51 usuários. Apesar de que essa exposição não representa grandes riscos, existe a possibilidade de ser utilizado em crimes de ódio relativos ao gênero.

'Acontecimentos importantes' (46 ocorrências) dão informações a respeito de algum acontecimento em sua vida, como por exemplo, início ou término de um relacionamento sério ou casamento, formação acadêmica, início em algum serviço, início em conselhos de sua profissão, informações sobre adoções de animais, entre outros. Uma vez que esse item pode englobar diferentes aspectos da vida social ou profissional, podem oscilar entre alta, média, ou baixa periculosidade de acordo com sua natureza.

Dos usuários analisados, 45 disponibilizam sua localização na página do Facebook, muitas vezes só pelo desejo de publicar sobre onde estão, informando sua localização e visitas no serviço, passeios e saídas para lanchonetes, bares e baladas, e outras vezes para ter acesso ao *Wi-Fi* em determinado local. O maior problema dessa exposição é que qualquer pessoa mal-intencionada saberá todos os seus passos, gostos, assim como os momentos que não estará em casa, inclusive em viagens. Informações desse tipo facilitam o acesso criminoso às residências, além de outros riscos como sequestros e sequestros relâmpagos.

Sobre o item 'Outras informações', trata de um mecanismo do Facebook em que a pessoa coloca informações a respeito de si que não se encaixam nas demais seções do item 'Sobre'. Foram encontrados 24 perfis que disponibilizam informações neste subitem, com conteúdos variados a respeito de sua crença religiosa, frases que gostam, sites e blogs pessoais, apelidos, links para outras contas de mídias sociais, idiomas que são fluentes, interesses sexuais, ideologias políticas entre outras informações pessoais como suas características físicas e emocionais. Essas informações podem trazer riscos aos usuários, como por exemplo, sendo uma forma do engenheiro social se aproximar das pessoas a partir de gostos 'em comum' para conseguir as informações que deseja, ganhando sua confiança e amizade para depois manipulá-lo em benefício próprio.

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

De maneira geral, portanto, os principais riscos na utilização das mídias sociais e na exposição específica destas informações, são: a) Invasão de privacidade e/ou de perfil; b) Uso indevido de informações ou furto de identidade; c) Vazamento de informações e danos à imagem e à reputação; d) Recebimento de mensagens contendo códigos maliciosos e/ou *phishing*; e) Instalação de programas maliciosos; f) Contato e disponibilização de informações para criminosos ou pessoas mal- intencionadas, que as podem usar em tentativas de sequestro ou para furto de bens.

A análise dos perfis revela que os(as) bibliotecários(as) analisados(as) disponibilizam voluntariamente informações que podem colocá-los(as) em risco. Essa constatação revela a necessidade de trabalhar essa conscientização entre os(as) profissionais da informação presentes no Facebook, não apenas como meio de garantir sua segurança no ambiente digital, mas, inclusive, para que possam ser formadores dessa mesma consciência nas comunidades das bibliotecas onde atuam.

Dos cuidados a serem tomados pelos usuários, além da preservação da própria privacidade, deve-se ter em mente os seguintes pensamentos, questionamentos e ações: a) Considere que você está em um local público, que tudo que você divulga pode ser lido ou acessado por qualquer pessoa; b) Pense bem antes de divulgar algo, pois não é possível voltar atrás; c) Use as opções de privacidade oferecidas pelos sites e seja o mais restritivo possível; d) Mantenha seu perfil e seus dados privados; e) Restrinja o acesso ao seu endereço de *e-mail*; f) Seja seletivo ao aceitar seus contatos; g) Não acredite em tudo que você lê; h) Seja cuidadoso ao se associar a grupos e comunidades; i) Seja cuidadoso ao fornecer a sua localização; j) Cuide da sua imagem profissional; k) Antes de divulgar uma informação, avalie-se, de alguma forma, ela pode atrapalhar a sua carreira e lembre-se que pessoas do ambiente profissional podem ter acesso aquilo; l) Verifique se sua empresa possui um código de conduta e evite divulgar detalhes sobre seu trabalho. (DIRETORIA DE GESTÃO E TECNOLOGIA DA INFORMAÇÃO, 2012).

A respeito da legislação atualmente no Brasil como forma de proteção e conhecimento dos direitos aos cidadãos existem poucas legislações sobre crimes cibernéticos ou até mesmo crimes de ódio que ocorrem nos ambientes digitais, geralmente são utilizadas legislações vigentes criadas durante a formulação e desenvolvimento da Constituição de 1988, além de algumas leis e decretos posteriores.

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

Contudo, com a grande quantidade de usuários da internet e seu crescimento contínuo, além do vasto desenvolvimento de mídias sociais, torna-se necessária a criação de legislações que deem cobertura aos usuários de redes digitais, bem como de ações que os protejam para além das políticas de privacidade e segurança que esses sites ofereçam.

Com simples cuidados é possível criar um ambiente mais seguro no Facebook e, com este trabalho, espera-se facilitar o conhecimento desses mecanismos de defesa entre os profissionais da informação.

5 CONSIDERAÇÕES FINAIS

A presente pesquisa permitiu observar a ampla aplicabilidade deste tema para futuras pesquisas, trabalhos e debates, em especial na área de Biblioteconomia e Ciência da Informação, tendo em vista a ausência de trabalhos publicados sobre o assunto. Com o intuito de mostrar os riscos das mídias sociais, os cuidados a serem tomados, o porquê e como proteger as informações pessoais e profissionais, além de conscientizar os cidadãos de seus direitos.

Esses resultados levam a uma reflexão sobre a necessidade de esses profissionais aprofundarem seu conhecimento sobre os riscos existentes no ambiente digital, e buscando mecanismos de defesa para sua proteção contra crimes virtuais. Portanto, espera-se que essa pesquisa sirva de inspiração para novos trabalhos, ampliando esta temática e buscando estudar outros aspectos desses assuntos e envolver as bibliotecas e universidades como meio de sensibilizar os(as) usuários(as) da internet de modo geral, tornando cidadãos conscientes, críticos e competentes no que se refere a criar, desenvolver e disseminar as informações.

REFERÊNCIAS

ABREU, L. F. dos S. **A segurança da informação nas redes sociais**. 2011. 56 f. Trabalho de Conclusão de Curso (Tecnólogo em Processamento de Dados) - Faculdade de Tecnologia de São Paulo, São Paulo, 2011. Disponível em: http://www.fatecsp.br/dti/tcc/tcc0023.pdf. Acesso em: 24 mar. 2018.

ALLEN, M. Social engineering: a means to violate a computer system. **SANS Institute InfoSec Reading Room,** [S.l.], p. 1-13, jun./dez. 2006. Disponível em: https://www.sans.org/reading-room/whitepapers/engineering/paper/529. Acesso em: 2 nov. 2018.

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

ANGELO, E. Redes sociais virtuais na sociedade da informação e do conhecimento: economia, poder e competência informacional. **Encontros Bibli**, Florianópolis, v. 21, n. 46, p. 71-80, maio/ago. 2016. Disponível em: https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2016v21n46p71. Acesso em: 22 abr. 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR/ISO/IEC 27001:** Tecnologia da informação – Técnicas de segurança – Sistema de gestão de segurança da informação. Rio de Janeiro: ABNT, 2006.

BAUMAN, Z.; LYON, D. **Vigilância liquida**. Rio de Janeiro: Zahar, 2012.

COELHO, V. L.; SILVA, M. R. da. Acesso competente à informação na web. **Biblionline**, Pernambuco, v. 12, n. 3, p. 3-15, jul./set. 2016. Disponível em: http://www.periodicos.ufpb.br/ojs2/index.php/biblio/article/view/29027. Acesso em: 22 abr. 2018.

CORREA, E. C. D.; SILVA, F. C. G. da. Presença digital dos Conselhos Regionais de Biblioteconomia do Brasil no Facebook. **Perspectivas em ciência da informação**, Minas Gerais, v. 22, n. 3, p. 16-32, jul./set. 2017. Disponível em: http://www.scielo.br/scielo.php?script=sci_abstract&pid=S1413-99362017000300016&lng=en&nrm=iso&tlng=pt. Acesso em: 15 ago. 2018.

CORREIA, P. M. A. R.; MOREIRA, M. F. R. Novas formas de comunicação: história do Facebook: uma história necessariamente breve. **Revista Alceu**, Rio de Janeiro, v. 14, n. 28, p. 168-187, jan./jun. 2014. Disponível em: http://revistaalceu.com.puc-rio.br/media/alceu%2028%20-%20168-187.pdf. Acesso em: 4 maio 2018.

DIRETORIA DE GESTÃO E TECNOLOGIA DA INFORMAÇÃO. **Segurança em redes sociais**. Universidade Federal de Lavras. 11 dez. 2012. Disponível em: https://www.dgti.ufla.br/site/seguranca-em-redes-sociais/. Acesso em: 2 nov. 2018.

GARCIA, J. C. R.; SOUSA, M. R. F. de. Cultura digital: odisseia da tecnologia e da ciência. **Em Questão**, Porto Alegre, v. 17, n. 2, p. 77-90, jul./dez. 2011. Disponível em: https://seer.ufrgs.br/index.php/EmQuestao/article/view/22252. Acesso em: 11 abr. 2018.

KOZINETS, R. V. **Netnografia**: realizando pesquisa etnográfica online. Porto Alegre: Penso, 2014.

LÉVY, P. **Cibercultura**. São Paulo: Editora 34, 1999.

SOUZA, R. C. de. **Prevenção para ataques de engenharia social:** um estudo sobre a confiança em segurança da informação em uma ótica objetiva, social, estrutural e interdisciplinar utilizando fontes de dados abertos. 2015. 189 f. Dissertação (Mestrado em Ciência da Informação) – Faculdade de Ciência da Informação, Universidade de Brasília, Brasília, 2015. Disponível em:

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594

http://repositorio.unb.br/bitstream/10482/18863/1/2015_RaulCarvalhodeSouza.pdf. Acesso em: 20 abr. 2018.

MITNICK, K. D.; SIMON, W. L. **A arte de enganar.** São Paulo: Makron Books, 2003.

MOELLER, S. *et al*. **Tomwards media and information literacy indicators**. 2011. Paris: UNESCO, 2011. 53 p. Disponível em: https://www.ifla.org/files/assets/information-literacy/publications/towards-media-and-Information-literacy-indicators.pdf. Acesso em: 10 set. 2018.

SILVA, N. B. X.; ARAÚJO, W. J. de; AZEVEDO, P. M. Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. **RICI**, Brasília, v. 6, n. 2, p. 37-55, ago./dez. 2013. Disponível em: http://periodicos.unb.br/index.php/RICI/article/view/9222. Acesso em: 11 abr. 2018.

VICENTE, N. I. **O uso do Twitter e Facebook para divulgação científica**: um estudo netnográfico em perfis de bibliotecas universitárias federais do sul do Brasil. 2015. 184 f. Dissertação (Mestrado Profissional em Gestão de Unidades de Informação)– Universidade do Estado de Santa Catarina, Florianópolis, 2015. Disponível em: http://www.fatecsp.br/dti/tcc/tcc0023.pdf. Acesso em: 20 abr. 2018.

Revista ACB: Biblioteconomia em Santa Catarina, Florianópolis (Brasil) - ISSN 1414-0594