Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Rafael Renan Bernardino Carneiro
Roberto Cazalatina De Mattos

A DIFICULDADE NO COMBATE ÀS *FAKE NEWS* NO BRASIL POR FALTA DO LETRAMENTO INFORMACIONAL DOS CIDADÃOS

Americana, SP
2021

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Rafael Renan Bernardino Carneiro

Roberto Cazalatina De Mattos

A DIFICULDADE NO COMBATE ÀS *FAKE NEWS* NO BRASIL POR FALTA DO LETRAMENTO INFORMACIONAL DOS CIDADÃOS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação da Prof.ª Dr.ª Maria Cristina Aranda.

Área de concentração: Segurança da Informação.

Americana, SP

2021

Rafael Renan Bernardino Carneiro
Roberto Cazalatina De Mattos

A DIFICULDADE NO COMBATE ÀS *FAKE NEWS* NO BRASIL POR FALTA DO LETRAMENTO INFORMACIONAL DOS CIDADÃOS

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 06 de dezembro de 2021.

Banca Examinadora:

Maria Cristina Aranda (Presidente)
Doutora
Fatec Americana

Daives Araken Bergamasco (Membro)
Doutor
Fatec Americana

Cleberson Eugênio Forte (Membro)
Doutor
Fatec Americana

AGRADECIMENTOS

O desenvolvimento deste Trabalho de Conclusão de Curso só foi possível graças à ajuda e apoio de algumas pessoas, dentre as quais agradecemos:

Aos professores do curso, que nos proveram todo o conhecimento necessário para que pudéssemos desenvolver este trabalho da melhor forma possível.

Aos nossos amigos, que nos apoiaram em todos os momentos, desde o primeiro dia de aula até a conclusão deste trabalho.

Aos nossos pais, que sempre nos apoiaram e incentivaram que continuássemos, pois nos ensinaram que sempre vale a pena lutar por aquilo que almejamos.

Aos professores orientadores, o Professor Doutor Daives Arakem Bergamasco, que sempre esteve presente para nos ajudar e nos auxiliar, principalmente, a Professora Doutora Maria Cristina Aranda, que nos orientou durante todo o processo e nos deu o suporte necessário para chegar até o fim; sempre nos incentivando a continuar e fazendo valer a pena cada dia de desenvolvimento deste trabalho.

DEDICATÓRIA

Dedicamos este trabalho aos nossos pais, pilares da nossa formação como seres humanos, responsáveis por nos ensinar, desde muito jovens, que a educação é realmente a arma mais poderosa que podemos usar para mudar o mundo.

“Se a educação sozinha não transforma a sociedade, sem ela tampouco a sociedade muda”.

(Paulo Freire)

RESUMO

A informação sempre fez parte da vida das pessoas como forma de comunicação e entretenimento. Como todo período histórico da sociedade as mentiras e notícias falsas também fazem parte da vida das pessoas. O objetivo deste trabalho é apresentar algumas reflexões e análises a respeito do letramento informacional principalmente nas últimas décadas em que a sociedade da informação vem provocando mudanças significativas no processo de ensino na educação brasileira. A metodologia utilizada para a realização deste trabalho foi à revisão de literatura sobre temas como o letramento informacional, engenharia social e *fake news*. Descreve os principais pontos de evolução na comunicação de cada momento histórico da humanidade, partindo desde os primórdios da comunicação humana até os dias atuais. Aborda os instrumentos de aprendizagem do ensino informacional brasileiro, as principais técnicas de engenharia social e o respaldo científico para a identificação e solução da disseminação de *fake news* no Brasil. Concluem-se as habilidades do letramento informacional para impedir que as *fake news* continuem a se disseminar por todo território nacional.

Palavras-chave: Letramento, Informação, Fake News.

ABSTRACT

Information has always been part of people's lives as a form of communication and entertainment. Like every historical period of society, lies and fake news are also part of people's lives. The objective of this work is to present some reflections and analyzes about information literacy, mainly in the last decades, when the information society has been causing significant changes in the teaching process in Brazilian education. The methodology used to carry out this work was a literature review on topics such as information literacy, social engineering and fake news. It describes the main points of evolution in communication in each historical moment of humanity, starting from the beginnings of human communication to the present day. It covers the learning instruments of Brazilian informational education, the main techniques of social engineering and the scientific support for identifying and solving the dissemination of fake news in Brazil. Information literacy skills are completed to prevent fake news from continuing to spread throughout the national territory.

Keywords: *Literacy, Information, Fake News.*

SUMÁRIO

1 INTRODUÇÃO 13

2 DA COMUNICAÇÃO À ENGENHARIA SOCIAL E SEUS RISCOS 14

2.1 A HISTÓRIA DA COMUNICAÇÃO HUMANA 14

2.2 TEORIA DA COMUNICAÇÃO 23

2.3 O LETRAMENTO INFORMACIONAL NA ATUALIDADE 24

2.4 A ENGENHARIA SOCIAL 27

2.5 OS TIPOS DE GOLPES MAIS CONHECIDOS 29

2.5.1 Phishing 29

2.5.2 Baiting 32

2.5.3 Pretexting 33

2.5.4 Quid pro quo 33

2.5.5 Tailgating e Piggybacking 34

2.6 OUTROS CASOS CONHECIDOS 34

2.6.1 O Caso da jornalista que permitiu ser hackeada 35

2.6.2 O Massacre de Christchurch 37

2.7 POLÍTICA E O ESCÂNDALO DA CAMBRIDGE ANALYTICA 38

2.7.1 O ex-funcionário que delatou a Cambridge Analytica 40

2.8 COMO SE DEFENDER DA ENGENHARIA SOCIAL 42

2.8.1 Como funciona o ataque 42

2.8.2 Sinais de um ataque de engenharia social 42

2.8.3 Como se defender 44

2.9 A GDPR EUROPEIA E A LGPD BRASILEIRA 45

3 *FAKE NEWS* 49

3.1 NOTÍCIAS FALSAS E AS MÍDIAS SOCIAIS 51

3.2 CASOS NAS REDES 52

3.3 COMO DETECTAR *FAKE NEWS* 65

3.3.1 Quem 65

3.3.2 O que 65

3.3.3 Quando 66

3.3.4 Onde 66

3.3.5 Exemplos 69

3.4 COMO COMBATER *FAKE NEWS*.....76
3.4.1 Agências verificadoras.....*76*
3.4.2 Projeto de Lei das Fake News.....*77*
3.4.3 O papel do profissional de Segurança da Informação.....*78*
4 CONCLUSÕES.....**80**
5 REFERÊNCIAS.....**82**

LISTA DA FIGURAS

Figura 1 - Escrita cuneiforme, de origem Suméria, encontrada no Iraque. 16
Figura 2 - Página do primeiro livro impresso, O Sutra do Diamante, em 868 d.C. 18
Figura 3 - A Bíblia de Gutenberg com 42 linhas, impressa em Mainz, Alemanha, em 1455. 19
Figura 4 - Computador típico do final dos anos 90 e início dos anos 2000 20
Figura 5 - Celular Motorola DynaTAC 8000X 21
Figura 6 - O modelo de Lasswell 23
Figura 7 - Exemplo de *Smishing* com *link* malicioso tentando se passar por *link* de banco 32
Figura 8 - Promoção com contador regressivo no *site* da loja Kabum! 35
Figura 9 - O número de pessoas que Facebook estima terem sido afetadas pelo escândalo, e o país de origem. 40
Figura 10 - Aviso de coleta de cookies no *site* g1.globo.com 47
Figura 11 - Aviso de coleta de cookies no *site* nytimes.com 47
Figura 12 - Usuária do Facebook em postagem contendo *fake news*.....52
Figura 13 - Quadro mostrado após clicar no botão "Entenda" na postagem sinalizada como *fake news*. 53
Figura 14 - Usuária do Facebook em postagem contendo *fake news*, em postagem mais antiga. 54
Figura 15 - Quadro mostrado após clicar no botão "Entenda" na postagem sinalizada como *fake news*. 55
Figura 16 - Postagem original da deputada Bia Kicis em sua página no Facebook. .56
Figura 17 - Publicação de Regina Duarte marcada como parcialmente falsa pelo Instagram. 57
Figura 18 - *Link* enviado por Whatsapp se passando por promoção de passagens aéreas da companhia Gol 60
Figura 19 - *Site* falso se passando pela Gol, acessado de um smartphone. 61
Figura 20 – *Site* falso solicitando o compartilhamento da promoção com mais 10 amigos.....62
Figura 21 - Resultado da busca *Whois* sobre o *site* voegolbr.com.....63
Figura 22 - *Sites* relacionados com o IP do *site* voegolbr.com.....64

Figura 23 - *Site* oficial da companhia aérea Gol avisando sobre possível golpe acontecendo em seu nome. 64
Figura 24 - Infográfico de como identificar notícias falsas 68
Figura 25 - Publicações do tipo caça-*likes* no grupo sobre animais. 70
Figura 26 - Pesquisa de imagem no Google mostrando a origem da imagem utilizada como caça-*likes*. 71
Figura 27 - Publicação do tipo caça-*likes* com imagem de idosa em situação de saúde. 72
Figura 28 - Pesquisa de imagem no Google mostrando a origem da imagem utilizada como caça-*likes.* 72
Figura 29 - Postagens de *fake news* no grupo sobre animais. 73
Figura 30 - Certificado HTTPS válido para o *site* brasilacontece.net.br 74
Figura 31 - Resultado da ferramenta Whois sobre o domínio do *site* de *fake news*. 75

1 INTRODUÇÃO

Notícias sempre fizeram parte do cotidiano, sendo tradicionalmente transmitidas há décadas via mídias como canais de televisão, estações de rádio, jornais e revistas. Levando em consideração que mentiras e verdades se tornaram possíveis desde que as primeiras formas interpessoais de comunicação foram estabelecidas, qualquer cidadão ou instituição pode publicar alegações nulas, parcial ou totalmente fundadas, sejam elas verdadeiras ou falsas, com o intuito de beneficiar ou prejudicar grupos ou indivíduos. A partir do século XXI foi criado o termo *fake news* para caracterizar as notícias do tipo não completamente verídicas.

Este trabalho pretende esclarecer informações acerca da transmissão de *fake news* e sugerir o letramento informacional como combate a elas, pois esse tipo de notícia falsa tornou-se mais comum nos últimos anos, prejudicando entidades e inferindo desconfiança da população em relação à circulação de informações transmitidas tanto por meios oficiais quanto por pequenos grupos de pessoas.

2 DA COMUNICAÇÃO À ENGENHARIA SOCIAL E SEUS RISCOS

As palavras ditas e as ações executadas transmitem mensagens, emoções e informações. Praticamente todos os seres vivos se comunicam de alguma forma. Para um melhor entendimento, precisamos definir e aprender sobre o seu funcionamento.

> [...] é somente através da comunicação, e com a finalidade de transmitir e submetê-la a outros, que se apresenta aqui para nós a tarefa de definir a comunicação.
> De outra parte, a resposta que espontaneamente vem a nosso espírito é a situação de diálogo onde duas pessoas (emissor-receptor) conversam, isto é, trocam ideias, informações ou mensagens. É isto que, sem dúvida, mais prontamente entendemos como comunicação. Entretanto, se solicitados, estaríamos prontos a admitir que o fenômeno não se restringe exclusivamente ao envolvimento entre duas pessoas. Sem maiores problemas, aceitamos a ideia de que os animais se comunicam, bem como a comunicação realizada entre aparelhos técnicos (dois computadores ligados por modem, por exemplo). (MARTINO, 2010, p.12)

A etimologia do termo “comunicação” tem a sua origem no Latim *communicatio*, e pode ser traduzido, de forma literal, em algo como “tornar comum”, porém também foi atribuído o significado de “ato de repartir, dividir, distribuir”. Este termo é derivado de outra palavra do Latim, *communis*, que significava “algo compartilhado por vários, público, geral”.

Sem a comunicação humana, não haveria a possibilidade de projetar pesquisas e formular teorias nos diferentes campos do comportamento humano. A ciência estaria comprometida e nossa evolução nunca teria chegado no ponto em que chegou hoje.

2.1 A HISTÓRIA DA COMUNICAÇÃO HUMANA

É muito difícil afirmar com exatidão quando a comunicação *proto-humana*[1] se iniciou. Apesar do árduo trabalho de arqueólogos, a pré-história foi um período em que fatos e acontecimentos não eram registrados com a finalidade de deixá-los para o futuro. Não existia uma linguagem desenvolvida. Ao escrever sobre os primórdios da comunicação proto-humana é preciso trabalhar muito mais com hipóteses e probabilidades do que com registros em si. Porém é de consenso entre os linguistas

[1] Na Antropologia, diz-se de ou hominídeo que já apresenta algumas das características do Homo sapiens. (MICHAELIS, 2021)

do mundo todo que a comunicação entre os proto-humanos possa ter começado há cerca de 500 mil anos.

O que parece mais plausível é que as primeiras formas humanas se comunicavam através de um número limitado de sons que eram fisicamente capazes de produzir, tais como, rosnados e grunhidos além de linguagem corporal, como gestos com as mãos ou braços e outros movimentos maiores utilizando o corpo. Isso acontecia porque a capacidade de aprendizagem das espécies proto-humanas era insuficiente para criar códigos complexos. Mas isso se modificou com o tempo, conforme ia se alterando a relação entre o corpo e o cérebro.

O homo sapiens (espécie humana) surgiu entre 30 mil e 10 mil anos atrás. Entre 10 mil e 6.500 anos atrás os seres humanos começaram a se estabelecer em determinadas regiões do Oriente Médio. No período em que os grupos de humanos começaram a habitar um mesmo território de forma mais fixa, iniciou-se o seu processo de enraizamento à terra habitada onde se trabalhava coletivamente para o seu cultivo. E daí surgiram as condições para o surgimento da escrita.

Foi por motivos primariamente econômicos, nas sociedades mais antigas, que se deu o surgimento da escrita.

> [...] Fortes indícios existem de que a motivação principal que levou os seres humanos ao registro da informação em suportes materiais (como pedra e argila, inicialmente) foram fatores econômicos. A partir do momento em que o ser humano passou a habitar locais determinados, iniciando uma vida sedentária, adquiriu, gradualmente, a necessidade de estabelecer limites para este território. Além disso, os limites de propriedade entre os indivíduos que cultivavam a terra adquiriram extrema importância para o funcionamento do grupamento social. (LAIGNIER, 2009, p. 15)

Visto que não é de se surpreender que a escrita tenha surgido na Mesopotâmia, região onde a agricultura foi criada e berço da civilização. A estreita faixa de terra que se localiza entre os rios Tigre e Eufrates, no Oriente Médio, onde atualmente é o Iraque, foi chamada de Mesopotâmia na Antiguidade. Mesopotâmia significa “entre rios” (do grego *meso* = no meio e *potamos* = rio). Essa região foi ocupada entre 4.000 a.C. e 539 a.C., por diversos povos diferentes, formando o que são denominados como povos mesopotâmicos, sendo, entre eles, Sumérios, Babilônios, Hititas, Assírios e Caldeus.

Os primeiros registros de um sistema de linguagem escrita são datados de 3.300 a.C., na cidade-Estado de Uruk, na antiga Suméria. Foi chamada de escrita

cuneiforme (Figura 1). Eram feitos registros cotidianos, econômicos e políticos da época, na argila, com símbolos formados por cones. Nesse mesmo momento, surgem os hieróglifos no Egito. Essa era uma escrita dominada apenas por pessoas poderosas da sociedade, como escribas e sacerdotes.

Figura 1 - Escrita cuneiforme, de origem Suméria, encontrada no Iraque.

Fonte: Fedor Selivanov / Shutterstock.com, [s.d.]

Por volta do século XII a.C. os Fenícios, exímios comerciantes, desenvolveram um sistema escrito que se aproximava muito de um alfabeto. Composto por 22 sinais, porém apenas com consoantes.

No século VIII a.C., o primeiro código alfabético completo foi inventado pelos gregos. O Alfabeto Grego, uma adaptação do alfabeto fenício (devido ao comércio entre os dois povos), é um sistema de escrita fonética composto por 24 letras que podem representar vogais e consoantes.

O alfabeto grego é usado apenas no idioma grego, mas como foi a base da maioria dos alfabetos existentes no ocidente é bastante comum o mesmo ser utilizado no dia a dia. Como na Astronomia, em que as letras são utilizadas na nomenclatura das estrelas; no registro arqueológico, as primeiras ocorrências do alfabeto grego aparecem em gravações feitas em cerâmicas, sendo as mais conhecidas encontrados em Atenas na metade do século VIII a.C.

Na Grécia também foi inventado o pergaminho, que são suportes feitos de pele de animais, geralmente de cabra, carneiro, cordeiro ou ovelha para a escrita ou desenho. Acredita-se que os pergaminhos tenham origem na cidade Pérgamo, na Antiga Grécia, e por isso o nome pergaminho.

Paralelamente aos gregos, os chineses desenvolveram um padrão escrito ideográfico, com mais de 4 mil caracteres, usando como suporte a madeira. A busca por materiais mais leves e portáteis, que pudessem servir de suporte para a informação escrita, levou os chineses à invenção da seda e do papel, por volta do século II a.C.

Posteriormente, por volta dos séculos VIII e VII a.C., na região da Toscana na Itália, a escrita alfabética chegou através de uma adaptação do alfabeto grego. Também conhecido na época como alfabeto etrusco. Os Etruscos (povo que viveu na Toscana no século X a. C.), ao entrarem em contato com a cultura local, adotaram o seu alfabeto e alteraram-no de acordo com as suas necessidades. Os Romanos, herdeiros dos Etruscos, utilizaram o alfabeto destes e fixaram-no em 21 letras. Este alfabeto permaneceu sendo utilizado até o século I a.C., e depois deu lugar ao alfabeto Latino (por vezes chamado alfabeto Romano), que depois passou por algumas reformulações e novas adaptações e é o qual são utilizadas hoje no Brasil e em grande parte do mundo.

A comunicação escrita deixou de restringir a mensagem à instantaneidade da oralidade. Graças também aos suportes materiais da informação cada vez mais portáteis que o ser humano passou a dominar tanto o tempo quanto o espaço.

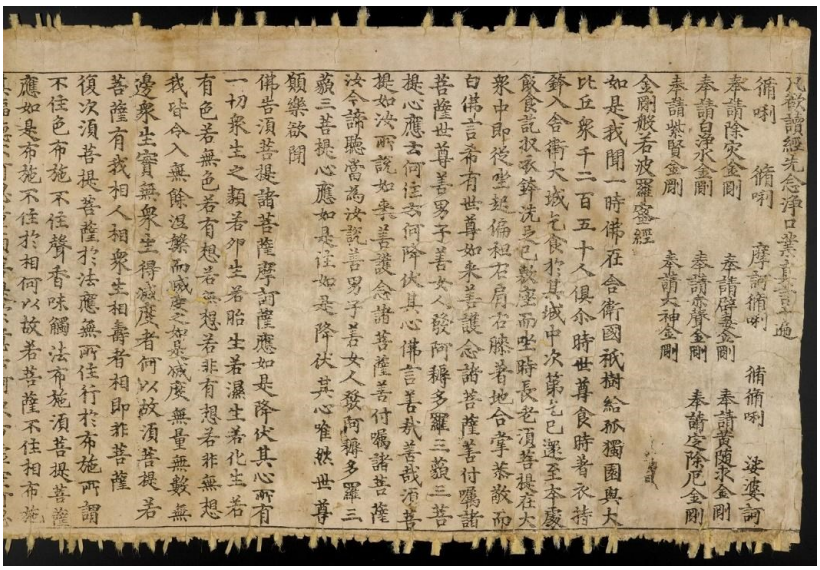
> A escrita abriu um espaço de comunicação desconhecido pelas sociedades orais, no qual se tornava possível tomar conhecimento das mensagens produzidas por pessoas que se encontravam a milhares de quilômetros, ou mortas há séculos, ou então que se expressavam apesar de grandes diferenças culturais ou sociais. A partir daí, os atores da comunicação não dividiam mais necessariamente a mesma situação, não estavam mais em interação direta. (LÉVY, 1999. *apud* LAIGNIER, 2009)

O surgimento da escrita possibilitou que cada mensagem pudesse ser relida, pensada e analisada, adquirindo durabilidade, clareza e profundidade. Foram então criados livros manuscritos que preservavam a informação e permitiam uma disseminação maior de ensinamentos e conhecimentos.

Séculos depois, foram criadas as primeiras invenções de prensas[2] tipográficas, que são um tipo de dispositivo que permite a produção em massa de impressos uniformes, principalmente textos na forma de livros, panfletos e jornais. Criada na China, a imprensa[3] revolucionou a sociedade local antes de ser desenvolvida na Europa no século XV por Johannes Gutenberg e sua invenção da Prensa de Gutenberg.

Ninguém sabe quando a primeira prensa tipográfica foi inventada ou quem a inventou, mas o texto impresso mais antigo conhecido se originou na China durante o primeiro milênio d.C. O Sutra do Diamante, apresentado na Figura 2, um livro budista de Dunhuang, China, de cerca de 868 d.C. durante a Dinastia Tang, é considerado o livro impresso mais antigo conhecido. O Sutra do Diamante foi criado com um método conhecido como impressão em bloco, que utilizava painéis de blocos de madeira entalhados à mão ao contrário.

Figura 2 - Página do primeiro livro impresso, O Sutra do Diamante, em 868 d.C.



Fonte: British Library[4], [s.d.]

A Prensa de Gutenberg era feita com letras e símbolos em relevo esculpidos em metal. A invenção de Johannes Gutenberg permitiu a impressão em massa de

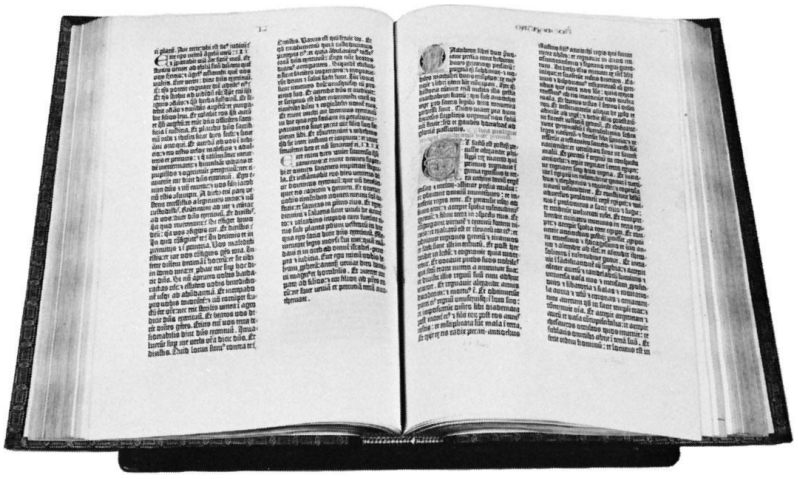
[2] Máquina de impressão; prelo. (MICHAELIS, 2021)

[3] Conjunto de publicações de periodicidade regular, de determinado lugar, gênero ou assunto; conjunto dos meios de difusão de informações jornalísticas; aquilo que é expresso pelos veículos de difusão coletiva (jornal, rádio, televisão etc.). (MICHAELIS, 2021)

[4] Disponível em: https://www.bl.uk/collection-items/%20the-diamond-sutra

livros, antes escritos a mão, começando uma revolução na Europa, em meados de 1455, na Alemanha.

Figura 3 - A Bíblia de Gutenberg com 42 linhas, impressa em Mainz, Alemanha, em 1455.



Fonte: Enciclopédia Britannica[5].

A Figura 3 apresenta a Bíblia de Gutenberg que é considerada a obra prima do inventor Alemão e foi o primeiro livro a ser produzido, lançado e vendido com a tecnologia da prensa mecânica de papel e que foi produzido em larga escala (escala industrial).

A imprensa foi se disseminando no lado Ocidental do globo a partir do século XV e sua invenção foi um dos marcos da passagem da Época Medieval para a Época Moderna. Além disso, a imprensa trouxe uma série de consequências importantes e muito positivas para a época, como a possibilidade de imprimir muitas cópias idênticas de um mesmo livro; o aumento da variedade e quantidade de títulos de livros disponíveis; tornou comum a tradução de obras para diferentes idiomas de edições que antes estavam disponíveis apenas em latim e grego; possibilitou a redução do preço dos livros.

Não é possível precisar a data de circulação do primeiro jornal. Mas sabe-se que informativos e gazetas com diversos temas circularam no século XVI e XVII. Nessa época, os jornais não tinham tanto impacto social. A partir do século XVIII Isso

[5] Disponível em: https://www.britannica.com/biography/Johannes-Gutenberg

muda e assuntos como política, ideias e publicidade começam a ser abordados em jornais.

O auge do prestígio e popularidade do jornalismo se deu no século XX. O período entre 1890 e 1920 é conhecido como a era de ouro dos jornais. Por volta de 1920, com a chegada do rádio, a atividade do jornalismo tradicional começa a decair. Aproximadamente em 1928 a televisão foi inventada. A partir de 1950 a TV se tornou o principal canal de mídia do mundo, posição que ocupa até hoje.

No final da década de 80 a Internet começou a se popularizar de forma comercial. Já no final dos anos 90 e início dos anos 2000, surgiu o boom da Internet. Com a popularização da Internet doméstica e dos computadores domésticos, como o modelo mostrado na Figura 4, a comunicação entre pessoas ao redor do mundo todo se tornou muito mais fácil e rápida, senão instantânea. Não era mais necessário aguardar dias para se ter acesso a determinada informação, pois com a Internet era possível ter acesso a um livro de qualquer língua em qualquer lugar do mundo que também possuísse acesso a esta rede. Também se tornou possível ter acesso a notícias em tempo real em que aconteciam, bastando acessar algum portal dedicado às notícias.

Figura 4 - Computador típico do final dos anos 90 e início dos anos 2000

Fonte: Retrogame Museum[6].

[6] Disponível em https://www.retrogamingmuseum.com/the-collection/pc-gaming-in-the-year-2000

A partir dos anos 2000, também surgiram as redes sociais (como Orkut, Facebook, MySpace) e comunicadores instantâneos (como ICQ, MIRC, MSN).

Hoje, 21 anos depois, houve um grande salto e modernização de tecnologias, seja dos dispositivos que acessam a Internet como os computadores; seja a Internet em si que hoje é banda larga e milhares de vezes mais rápida do que nos anos 90, atingindo taxas de conexão de *gigabits* por segundo e tempos de resposta que beiram a instantaneidade; ou seja ainda pelas redes sociais e comunicadores, que também se modernizaram com o tempo, e hoje não fazem mais apenas seu papel principal que antes era criar a comunicação e trazer a sensação de proximidade entre pessoas, mas também tem o papel de vender produtos e publicidade.

Outra ferramenta importantíssima que foi inventada na década de 70 e se modernizou muito, foi o celular. O celular se popularizou aproximadamente em 1984 com o lançamento pela Motorola do modelo Motorola DynaTAC (Figura 5). Era um modelo bastante grande e pesado e servia apenas para fazer ligações, pois para a época este era o único propósito de um celular.

Figura 5 - Celular Motorola DynaTAC 8000X

Fonte: Techtudo. [7]

[7] Disponível em: https://www.techtudo.com.br/artigos/noticia/2012/06/historia-dos-telefones-celulares.html

Hoje esses dispositivos são conhecidos como *dumb phones*, ou telefones burros, pois tinham a única função de fazer ligação. A partir dos anos 2000 começaram a surgir os *smartphones*, que eram celulares com sistemas operacionais próprios e que transformavam os dispositivos em dispositivos inteligentes, mas ainda eram muito simples e sem muitos recursos.

Em 2007 a Apple lançou o primeiro iPhone e este revolucionou o mercado de dispositivos móveis. Apple substituiu o teclado convencional, que era de botões físicos, por um teclado de toque diretamente na tela, o *touchscreen*, que permitia aos usuários manipular o dispositivo e sentir como se estivessem fisicamente manipulando as ferramentas do celular com os dedos. Era muito simples clicar em *links*, alongar e encolher fotos e folhear álbuns de fotografias. Além disso, ele trouxe diversos novos recursos. Tinha seu próprio sistema operacional como o de um computador, mas em um minúsculo telefone. A partir disso o mercado seguiu a tendência de sempre lançar diversos *smartphones* de diversas marcas, com cada vez mais recursos e cada vez mais potentes, superando hoje alguns computadores. e tudo isso na palma da mão.

Hoje os *smartphones* possuem sistema de localização GPS, *player* integrado de música e vídeo, diversas lentes ópticas para fotografia com grande capacidade de *megapixel*, armazenamento interno superior ao de alguns computadores mais antigos, bastante memória RAM para suportar os sistemas operacionais cheios de recursos, e tecnologia celular 5G, que se assemelha a uma banda larga por cabo de fibra óptica, porém sem fio. São verdadeiros computadores que cabem no bolso. São práticos e excelentes ferramentas de comunicação nos tempos atuais.

A exemplo, existe hoje um *smartphone* da marca Samsung, modelo Galaxy Note 20 Ultra, cujas especificações são semelhantes a um computador, como: tela de 6,9 polegadas, com resolução de 1440 x 3200px, armazenamento rápido de 256GB, 12GB de memória RAM, conexão 5G, câmera com resolução de 108 m*egapixels* e CPU de 8 núcleos.

Vale lembrar que os *smartphones* de hoje também fazem ligação como os celulares de antigamente, porém com o advento da Internet móvel cada vez mais rápida, se tornou comum fazer ligações utilizando também a Internet, fazendo com que a ligação através da rede móvel entre cada vez mais em desuso.

A história da comunicação humana não termina quando alcança o auge da modernidade atual, com a tecnologia se superando cada vez mais rápido e trazendo mais e mais facilidades ao dia a dia. Apesar de parecer um ato simples do cotidiano,

a comunicação se torna um pouco mais complexa quando aprofunda-se um pouco mais no assunto. Essa, é estudada desde muitos séculos atrás, possuindo diversas teorias científico-filosóficas a respeito.

2.2 TEORIA DA COMUNICAÇÃO

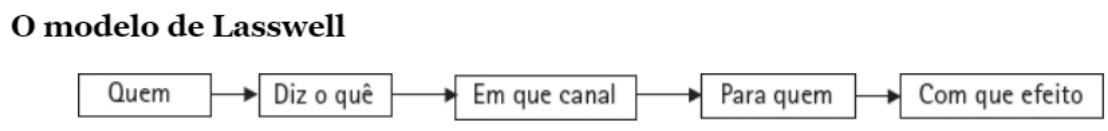
A teoria da comunicação estuda o processo científico de envio e recebimento de informações. Existem muitos princípios, métodos e componentes que podem afetar uma mensagem, e a teoria da comunicação tenta explicar isso. Existem ainda muitas características da teoria da comunicação que podem afetar o processo: emissor, receptor, ruído, diferenças culturais e assim por diante.

Para tornar as coisas um pouco menos complicadas, os criadores das diferentes teorias da comunicação as emparelharam com modelos de comunicação. Os modelos atuam como uma representação visual de uma teoria.

Como a comunicação se tornou complexa com o tempo, existem diferentes modelos de comunicação para diferentes tipos de comunicação. Um desses modelos é o modelo (Figura 6) criado pelo cientista político Harold Lasswell, em 1948.

> Lasswell desenvolve sua concepção a partir de uma ampliação do modelo de comunicação de Aristóteles (Emissor - Mensagem - Receptor) exposto na Arte retórica. A partir daí, Lasswell formula sua hipótese: 'Uma maneira de estudar o processo de comunicação é perguntar 'Quem'; 'Diz o que', 'Em que canal', 'para quem', 'Com que efeito'. Lasswell desmonta a comunicação em partes simples, relacionando o estudo de cada uma delas com uma proposta específica de comunicação: ao 'quem' corresponde um estudo de produção; 'diz o que' volta-se para a análise de conteúdo; 'em que canal', focaliza o estudo na mídia; 'para quem' pesquisa de audiência e 'com que efeitos' o que acontece com a audiência diante da mensagem (MARTINO, 2009, p.23).

Figura 6 - O modelo de Lasswell



Fonte: MARTINO, 2009.

Embora o modelo de Lasswell tenha sido desenvolvido para analisar a comunicação de massa, este modelo é usado para comunicação interpessoal ou

comunicação de grupo para serem disseminadas mensagens a vários grupos em várias situações.

2.3 O LETRAMENTO INFORMACIONAL NA ATUALIDADE

Embora não existam leis que definam uma idade ideal para começar a usar a Internet ou para deixar de usar, é de senso comum que existam grupos de idade em que o uso precoce da Internet poderia acarretar maiores riscos, como crianças. Também válido para pessoas idosas com pouco conhecimento informacional, cujo discernimento sobre o que é verdadeiro e seguro no mundo virtual pode se tornar confuso devido a grande quantidade de informações. Estes grupos podem ser considerados grupos vulneráveis e mais sensíveis à golpes e crimes cibernéticos, bem como às *fake news*[8]. Para Estabel (2020), os idosos são mais vulneráveis a acreditarem em *fake news* pois não foram preparados para atuar em ambientes virtuais e os chama de “não nativos da era digital”.

> [...] pelo fato de os idosos de hoje não serem nativos da era digital e da cultura subjacente a este meio, existe a possibilidade de serem relativamente mais vulneráveis aos seus riscos do que os ditos nativos, razão pela qual podem necessitar de alguma supervisão e de instruções sobre formas de evitar tais riscos. (FREITAS; PY, 2016, *apud* ESTABEL; LUCE; SANTINI, 2020)

Define-se vulnerabilidade como “suscetibilidade de ser ferido ou atingido por uma doença; fragilidade” (VULNERABILIDADE, 2021); de estar exposto a algo. Sua origem vem da palavra latina para "ferida", *vulnus*.

Indo além da vulnerabilidade devido à idade, ainda existe a falta de informação e conhecimento necessários para se aventurar nos mares da Internet; o que aqui envolve as pessoas de todas as idades. Pois, assim como na nossa vida real, onde existem os comportamentos sociais (regras, leis e afins), para se utilizar a Internet de forma mais adequada, é preciso antes ter um conhecimento mínimo sobre os riscos e perigos que se pode encontrar no mundo virtual.

Embora não exista um manual de instruções oficial para isso, já que a Internet está em constante mudança e crescimento, com novas ameaças surgindo a todo

[8] Notícias falsas, muitas vezes de natureza sensacionalista, criadas para serem amplamente compartilhadas ou distribuídas com o objetivo de gerar receita, ou promover ou desacreditar uma figura pública, movimento político, empresa, etc.

momento, existem outras formas de se aprender sobre seu uso seguro e melhores práticas; seja por meios de comunicação mais abrangentes, como a TV, presente em 96,3% dos domicílios brasileiros, segundo uma pesquisa de 2019 do IBGE (2020); nas escolas, desde o primeiro contato com um computador com Internet; seja por meio de cursos profissionalizantes e/ou inclusivos específicos; aprendendo por conta ou ainda utilizando-se do conhecimento popular, o famoso “boca-a-boca”.

Com a popularização da Internet nos anos 2000, surgiu a necessidade de democratização do acesso à Internet no Brasil. Assim, nasceu a inclusão digital numa tentativa de garantir o mínimo de conhecimento tecnológico para todos os cidadãos e o acesso às tecnologias de informação e comunicação (TICs). A ideia era que todas as pessoas, principalmente as de baixa renda, pudessem ter acesso às informações, fazer pesquisas, enviar *e-mails* e facilitar sua própria vida fazendo uso dessas tecnologias. Isto garantiria um mínimo conhecimento sobre a tecnologia e reduziria os riscos de uma pessoa exposta na Internet. Chama-se esse aprendizado, sobre o uso da informação, de letramento informacional. Assim, qualquer pessoa que não possua um mínimo letramento informacional, pode ser considerada uma pessoa vulnerável às *fake news*.

O significado de letramento caracteriza-se como um processo de aprendizagem necessário ao desenvolvimento de competências e habilidades específicas para buscar e usar a informação. Conforme Kleiman (2005), o letramento não é uma alfabetização, apesar de a incluir e os dois estarem associados, não é também considerado um método ou uma habilidade, apesar de envolver um conjunto de habilidades e competências. Pode-se dizer que o letramento é o uso da língua, da escrita e da leitura de acordo com a situação e caracterizando-se como uma prática social, transpondo os propósitos da alfabetização, não estando presente apenas no dia a dia do cidadão, como ainda participa da realização das suas práticas sociais letradas.

> “Letramento” é um conceito criado para referir-se aos usos da língua escrita não somente na escola, mas em todo lugar. Porque a escrita está por todos os lados, fazendo parte da paisagem cotidiana: no ponto de ônibus, anunciando produtos, serviços e campanhas. No comércio, anunciando ofertas, para atrair clientes, tanto nas pequenas vendas, como nos grandes supermercados. No serviço público, informando ou orientando a comunidade. (KLEIMAN, 2005)

Assim, pode-se dizer que um cidadão “letrado” é aquele que além de saber ler e escrever, também responde adequadamente às demandas sociais da leitura e da escrita; que possui cultura, que é instruído.

O letramento informacional, segundo Gasque (2010), “constitui-se no processo de aprendizagem necessário ao desenvolvimento de competências e habilidades especificas para buscar e usar a informação”. Com isto, observa-se que o conceito de letramento informacional está intimamente ligado à autonomia da aprendizagem, também associado à percepção e capacidade de reflexão do indivíduo. Além disso, auxilia o indivíduo a buscar e gerar informações de forma eficiente, revelando-se, de fato, muito útil e vantajoso para o cidadão em termos de assimilação de conhecimento.

> No contexto contemporâneo, o indivíduo precisa ser “informacionalmente” letrado para atuar como cidadão crítico e reflexivo, dotado de autonomia e responsabilidade e, desse modo, colaborar na superação dos graves problemas de toda ordem que atingem hoje a humanidade. (GASQUE, 2010)

A cada ano o acesso à Internet tem sido mais facilitado, principalmente através de redes móveis, utilizadas pelos *smartphones*. Com a cobertura cada vez maior de redes 3G e 4G, de alta velocidade, alcançando a maior parte dos municípios do país, uma parcela significativa da população tem conseguido adquirir pelo menos um *smartphone* e um número celular, tendo assim conexão com a Internet tanto pelo *wifi* (quando disponível) quanto pelas redes móveis. Segundo um levantamento do Instituto Brasileiro de Geografia e Estatística, o IBGE (2021), cerca de 82,7% dos domicílios brasileiros têm acesso à Internet.

Desta forma, houve avanços consideráveis no aprendizado de uso dessas tecnologias, pois, quanto mais pessoas utilizarem um *smartphone*, maiores as chances de se passar o conhecimento da utilização para outras pessoas, devido não somente a esta popularização, mas também a padronização dos sistemas operacionais e aplicativos. Como é o caso do *Whatsapp*, aplicativo de mensagens mais utilizado no Brasil (TERRA, 2021), que se popularizou ao ponto de se tornar conhecido em todo o território nacional e ser apelidado informalmente apenas como “Zap”[9], em razão da sonoridade vinda do nome original, em inglês; e essa

[9] Como visto em “ZAP da Prefeitura de Assis, SP”. No *link*: https://www.assis.sp.gov.br/pagina/47/atendimento/zap-da-prefeitura. Acesso em: 25 out. 2021.

popularização não aconteceu somente pela facilidade e intuitividade do aplicativo, mas, também, porque o aprendizado era fácil de se passar adiante.

Um importante levantamento feito pelo IBGE (2021), sobre o uso da Internet no Brasil em 2019, fala sobre como são os dados sobre os tipos de conexão.

> A banda larga móvel passou de 80,2% nos domicílios em 2018 para 81,2% em 2019. Já a banda larga fixa passou de 75,9% para 77,9%. A proporção de domicílios que contam com os dois tipos de conexão saltou para 59,2% em 2019. O percentual era de 56,3%, em 2018.
> O IBGE destaca ainda que o telefone celular continua sendo a principal ferramenta utilizada pelos conectados. Ele foi encontrado em 99,5% dos domicílios com acesso à rede mundial de computadores. Depois vem o computador, com 45,1%, seguido pela televisão (31,7%) e tablet (12%). (IBGE, 2021)

Com um Brasil mais conectado do que nunca, tornou-se possível a expansão do acesso à informação e a capacitação dos cidadãos junto à novas tecnologias e meios de adquirir conhecimento, permitindo assim um mínimo de letramento informacional, mas ainda não o suficiente para estar livre de riscos cibernéticos e exposições de risco na Internet.

> Nota-se que o cidadão iletrado possui dificuldades na produção de conhecimento, uma vez que ele não é incapaz de empregar as informações assimiladas nas práticas sociais.
> Desta maneira, as chances dele ascender socialmente reduzem significativamente, devido a essa incapacidade de destinar as informações adequadamente e de gerar conhecimento. Além disso, com o mercado de trabalho caracterizado pela competitividade, a inabilidade referente à escrita, à leitura e ao uso eficaz da informação, é, indiscutivelmente, um fator que dificulta a mobilidade social vertical ascendente do indivíduo iletrado. Por outro lado, o cidadão letrado tem a capacidade de produzir informações, bem como de impulsionar o desenvolvimento socioeconômico do país por causa do volume de informações que domina. (MARANHÃO; CARVALHO; SILVA, 2013)

O letramento informacional tem relação direta com o desenvolvimento do senso crítico do indivíduo, pois, o cidadão, ao procurar e usar a informação, necessitará antes analisar o que deseja, para depois iniciar um processo de busca.

2.4 A ENGENHARIA SOCIAL

Entre os diversos crimes cibernéticos conhecidos, existem alguns tipos que dependem de uma técnica específica, que pode ser difícil de se eliminar por completo,

que é a engenharia social, pois, essa se baseia no comportamento humano para funcionar. É difícil se defender da engenharia social porque os seres humanos são imprevisíveis. Não há como saber quem cairá em um ataque de engenharia social.

A Engenharia Social se baseia em um instinto humano fundamental de confiança para roubar informações pessoais e corporativas que podem ser usadas para cometer os mais diversos crimes cibernéticos.

Whitman (2012) define o termo da seguinte forma: “A Engenharia Social é um conjunto de técnicas e habilidades utilizadas para induzir as pessoas a revelarem dados confidenciais, que se tornam informações úteis para o fraudador”. Por exemplo, um cibercriminoso pode usar *spear phishing*[10] para convencer um funcionário a divulgar as senhas da empresa. Em seguida, eles são usados para acessar redes corporativas, roubar dados e instalar *malware*.

Para que o cibercriminoso tenha sucesso, basta um *e-mail*, telefonema ou mensagem de texto que pareça ter vindo de um colega, amigo ou empresa conhecida. Em sua mensagem, o cibercriminoso pode usar um tom urgente para convencer a vítima a atualizar suas informações bancárias. Ou especifique que, para reivindicar um prêmio, ela deve fornecer as informações do cartão de crédito.

> Geralmente o engenheiro social é um tipo de pessoa agradável, educada, simpática e carismática. Mas, sobretudo criativa, flexível e dinâmica. Possuindo uma conversa bastante envolvente. Até, mesmo, pessoas sem conhecimento antecipado desta denominação, já cometeram algum ato de engenharia social involuntariamente (PEIXOTO, 2004, *apud* COELHO, 2013).

A engenharia social é perigosa porque as pessoas cometem erros. Mesmo que as vítimas saibam que devem ter cuidado com *e-mails* que prometem descontos ou ligações que as ameaçam com a perda de acesso imediato à sua conta se não fornecerem seus dados bancários.

O sucesso na engenharia social depende do comportamento humano, como estar ocupado, não prestar atenção, ser excessivamente confiante, complacente e simplesmente esquecer o básico da conscientização sobre a segurança cibernética. É fazer com que a pessoa comprometa sua segurança voluntariamente. Não é

[10] Spear *phishing* é um golpe proveniente de *e-mail* ou comunicação eletrônica, direcionado a um indivíduo, organização ou empresa específicos. Embora tenha a intenção de roubar dados para fins mal-intencionados, os criminosos virtuais também podem tentar instalar malware no computador do usuário. (KASPERSKY, 2021)

incomum que uma pessoa seja vítima de um ataque de engenharia social mais de uma vez. Desta forma, é importante focar no treinamento de conscientização sobre segurança cibernética centrado nas pessoas.

O engenheiro social também se aproveita da necessidade humana de se comunicar e interagir com outras pessoas, o que pode possibilitar encontrar alvos fáceis em pessoas que se expõe demais *online*. Com base em informações extraídas, é possível criar e manipular conteúdos e direcioná-los às pessoas para obter-se sucesso em um golpe criminoso.

2.5 OS TIPOS DE GOLPES MAIS CONHECIDOS

Uma das melhores maneiras de se proteger contra um ataque de engenharia social é ser capaz de identificá-los. Existem alguns tipos comuns de ataques de engenharia social, dos quais é comum ter conhecido alguém que já foi vítima ou ouvido falar do ataque.

2.5.1 *Phishing*

A palavra *phishing* é um neologismo homófono[11] de *fishing*, que significa "pesca" em inglês, se referindo a golpes que buscam “fisgar” informações e dados pessoais. A substituição da letra "f" pelo dígrafo "ph" pode ter ocorrido pela junção das palavras *phony* ("falso") e *fishing*.

O *phishing* usa táticas, incluindo *e-mails*, *sites* e mensagens de texto enganosos para roubar informações pessoais e corporativas confidenciais. Os criminosos que usam táticas de *phishing* são bem-sucedidos porque se escondem cuidadosamente atrás de *e-mails* e *sites* familiares à vítima pretendida.

É uma forma bem conhecida de obter informações de uma vítima inconsciente. Como normalmente funciona: um cibercriminoso, ou *phisher*, envia uma mensagem a um alvo que pede algum tipo de informação ou ação que possa ajudar em um crime mais significativo. A pergunta pode ser tão simples quanto encorajá-lo a baixar um anexo ou verificar seu endereço de correspondência.

[11] Homófono: palavra pronunciada da mesma forma que outra palavra.

É interessante notar que existem muitas formas de *phishing* que os engenheiros sociais escolhem, todas com diferentes meios de segmentação. O *phishing* de *spam* geralmente assume a forma de *e-mails* de maior alcance, não necessariamente visando um único usuário. O *spear phishing* tem como alvo usuários individuais, talvez se passando por um contato confiável. O *Whaling* tem como alvo celebridades ou executivos de alto nível.

O *phishing* também vem em algumas formas de entrega diferentes:

- *Vishing*, ou seja, *phishing* de voz, é quando uma chamada telefônica pode ser gravada, incluindo informações inseridas nos *PIN pads*.
- *Smishing*, ou seja, *phishing* de SMS, são textos que contêm *links* maliciosos.
- O *phishing* de *e-mail* está entre os métodos de *phishing* mais tradicionais, ou seja, *phishing* por *e-mail*, muitas vezes, entregando um *link* malicioso ou um *download*.
- *Angler phishing* é quando um cibercriminoso se faz passar por um atendente de atendimento ao cliente para interceptar suas comunicações e mensagens privadas.
- O *phishing* de URL é um *link* falsificado que você recebe e que contém *malware*.
- O *In-session phishing* ocorre quando a vítima já está em uma plataforma ou conta e é solicitado, por exemplo, para fazer login novamente.
- O *phishing* baseado em fax geralmente ocorre quando um *e-mail* falso de uma instituição confiável solicitou que a vítima imprima a mensagem e envie por fax suas informações confidenciais.
- *Spear Phishing*, é um crime cibernético que usa *e-mails* para realizar ataques direcionados contra indivíduos e empresas. Os criminosos usam táticas inteligentes para coletar dados pessoais sobre seus alvos e enviar *e-mails* que são familiares e confiáveis.

2.5.1.1 Exemplo de *phishing*

Um engenheiro social pode se passar por uma instituição bancária, por exemplo, pedindo aos destinatários de *e-mail* que cliquem em um *link* para fazer *login*

em suas contas. Aqueles que clicam no *link*, no entanto, são levados a um *site* falso que, como o *e-mail*, parece ser legítimo. Se eles fizerem *login* nesse *site* falso, eles estarão basicamente entregando suas credenciais de *login* e dando ao cibercriminoso acesso às suas contas bancárias.

Ou ainda, um golpe famoso no Brasil, que ainda é bastante praticado, que é conhecido como “Golpe do cartão de crédito clonado[12]” ou “Golpe do cartão de crédito por telefone”, em que criminosos ligam para as vítimas se passando pelo banco e avisando que enviarão um suposto funcionário do banco para buscar cartões das vítimas para averiguação.

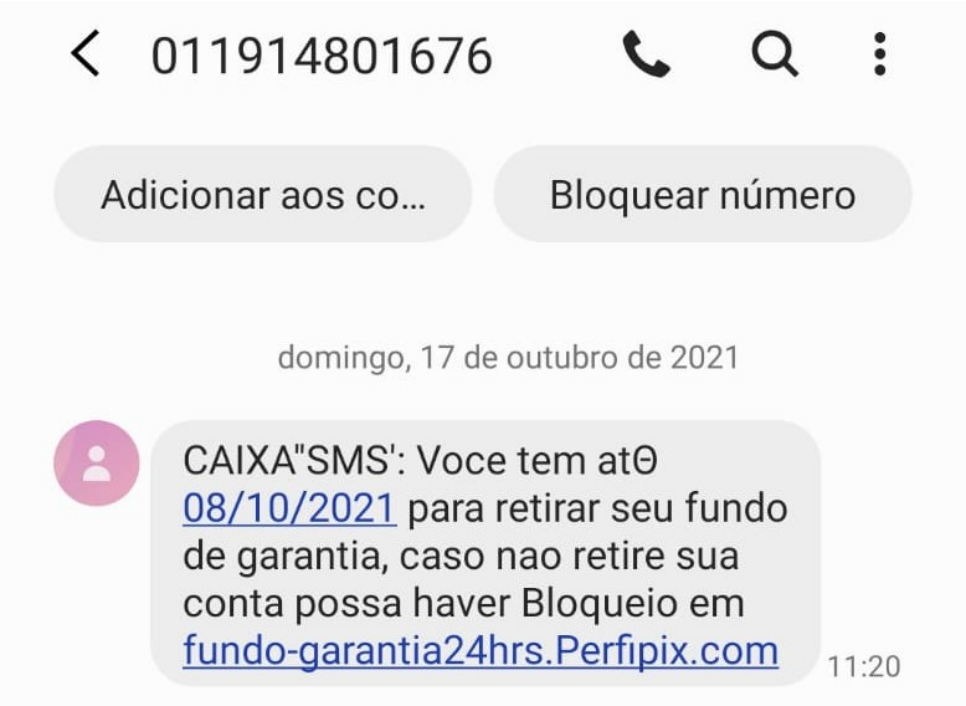
> Por usarem um software de centrais telefônicas que se chama URA, no entanto, as quadrilhas conseguem reter a ligação. Assim, quando a vítima desliga e liga para a central de atendimento pelo mesmo telefone logo em seguida, por mais que pense estar no controle da situação, a chamada é desviada para a quadrilha novamente. A recomendação, nesse caso, é usar outro telefone ou reiniciar o aparelho. (BRASIL, 2021)

Segundo a matéria da CNN Brasil (2021), a Polícia Civil do Distrito Federal, desde que começaram a contabilizar esse tipo em golpe, em 2018, as ocorrências desse crime vem aumentando. São de 300 a 400 ocorrências policiais de golpe do cartão por ano só no Distrito Federal.

Golpes de *smishing* (*pishing* via mensagem SMS) são muito comuns, pois podem ser disparados em massa a partir de um número de celular pessoal, como mostrado na Figura 7.

[12] Golpe do cartão de crédito por telefone usa até música que imita **call center**. Disponível em: https://www.cnnbrasil.com.br/business/golpe-do-motoboy-cresce-na-pandemia-e-usa-ate-musica-que-imita-call-center/. Acesso em: 12 nov. 2021.

Figura 7 - Exemplo de *Smishing* com *link* malicioso tentando se passar por *link* de banco



Fonte: Captura de tela do *smartphone*. Acervo próprio.

2.5.2 Baiting

O *Baiting* depende do desejo humano de recompensa. Baiting é um ataque de engenharia social *online* e físico que promete à vítima algo em troca de sua ação. Por exemplo, conectar um *pendrive* USB deixado no chão “por acaso” ou baixar um anexo que promete algum tipo de prêmio. O computador e, potencialmente, a rede são infectados por um *software* que pode capturar credenciais de *login* ou enviar *e-mails* falsos.

2.5.2.1 Exemplo de *baiting*

Um exemplo físico de *baiting*, seria um engenheiro social deixar um *pendrive*, carregado com *malware*, em um local público onde os alvos o verão, como em um café ou banheiro. Além disso, o criminoso pode rotular o dispositivo de uma forma convincente e sugestiva como "confidencial" ou qualquer outro nome que desperte a curiosidade. Um alvo que morde a isca pega o dispositivo e o conecta a um computador para ver o que há nele. O *malware* irá se injetar automaticamente no

computador, podendo se espalhar dentro de uma rede corporativa e infectar mais dispositivos.

2.5.3 Pretexting

O nome desse golpe vem da palavra “pretexto”, que é exatamente o que o criminoso inventa para extrair informações importantes do usuário. No *pretexting*, o engenheiro social utiliza métodos para convencer o usuário a dar informações sigilosas sobre ele ou a empresa. Uma vez que a história fisga a pessoa, o criminoso tenta enganar a suposta vítima para que forneça algo de valor. Frequentemente, o engenheiro social está se passando por uma fonte legítima.

2.5.3.1 Exemplo de *pretexting*

Um cibercriminoso pode saber que a vítima comprou recentemente um item da Apple, então o cibercriminoso envia um *e-mail* fingindo ser um representante do atendimento ao cliente da Apple que precisa confirmar as informações do cartão de crédito da vítima.

2.5.4 Quid pro quo

Quid pro quo significa um favor por um favor, essencialmente "eu te dou isso e você me dá aquilo". No caso da engenharia social, a vítima fornece informações confidenciais, como *logins* de conta ou métodos de pagamento e, em seguida, o engenheiro social não devolve a sua parte na barganha. Os golpes *quid pro quo* dependem de uma troca de informações para convencer a vítima a agir. Esta técnica de engenharia social oferece um serviço à vítima em troca de um benefício.

2.5.4.1 Exemplo de Quid pro quo

Um exemplo é o criminoso se passar por um funcionário de suporte de TI que liga para as vítimas que têm tíquetes de suporte abertos. O cibercriminoso promete uma solução rápida se a pessoa desabilitar seu *software* antivírus ou confirmar suas credenciais de *login*.

2.5.5 *Tailgating* e *Piggybacking*

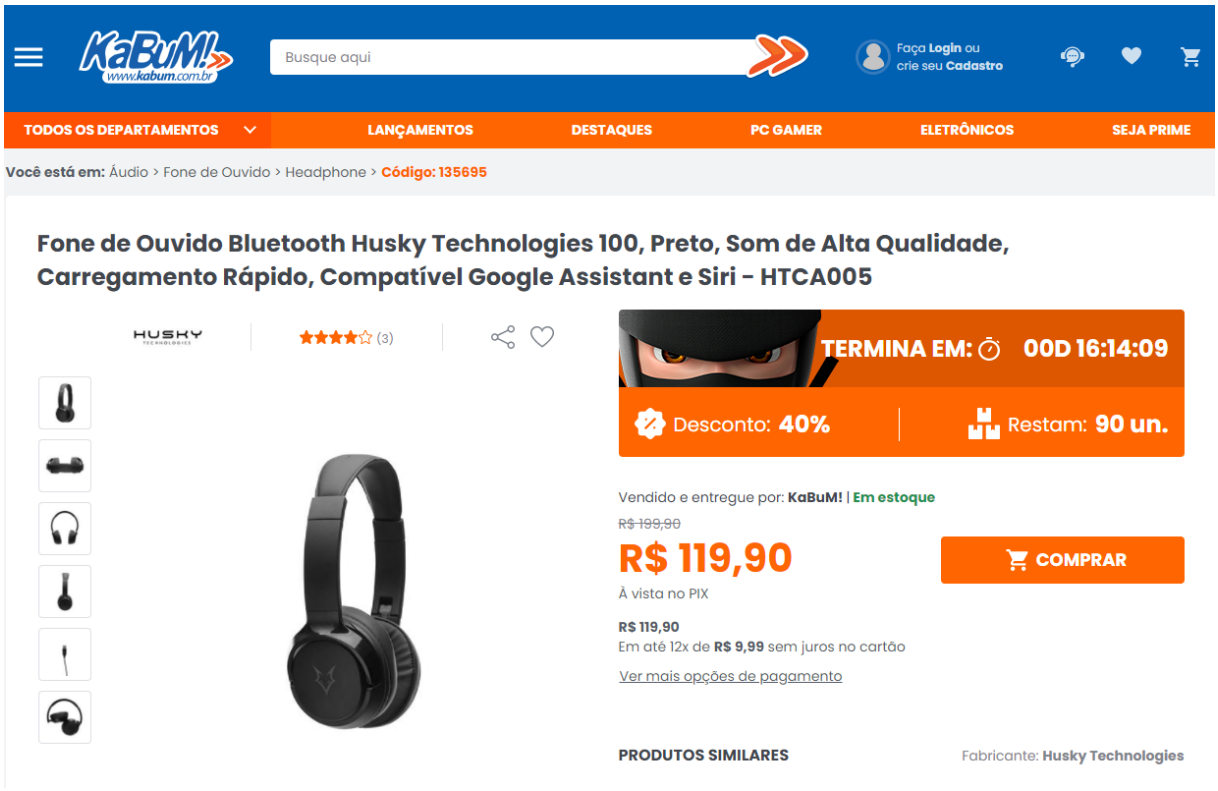
Tailgating é um ataque de engenharia social simplista usado para obter acesso físico para acessar um local não autorizado. A utilização não autorizada é alcançada seguindo de perto um usuário autorizado na área sem ser notado pelo usuário autorizado. Um invasor pode levar outro indivíduo atrás de si enfiando rapidamente o pé ou outro objeto na porta antes que ela seja completamente fechada e trancada. Esse golpe ressalta a necessidade de os funcionários prestarem atenção a quem está perambulando perto das portas e nunca hesitarem em pedir identificação.

O *Piggybacking*, também chamado no Brasil de “pegar carona” é muito semelhante ao *tailgating*. A principal diferença entre os dois é que, em um cenário *piggybacking*, o usuário autorizado fica ciente e permite que o outro indivíduo "tire carona" de suas credenciais. Um usuário autorizado pode se sentir compelido, por gentileza, a manter uma porta segura aberta para uma mulher segurando o que parece ser uma caixa pesada ou para uma pessoa que afirma ser um novo funcionário que esqueceu seu crachá de acesso.

2.6 OUTROS CASOS CONHECIDOS

Fora do ponto de vista estritamente técnico e com foco na cibersegurança, voltado para outras áreas fora da Tecnologia da Informação, a engenharia social também pode ser vista em ação, completamente legalizada, apesar de moralmente duvidosa. Está totalmente relacionada com a teoria da comunicação e manipulação de massas, como é possível observar nas campanhas de *marketing*, visando a melhora nas vendas, utilizada em *sites* que oferecem desconto especial, mas com uma contagem regressiva, como mostrado na Figura 8, criando uma ilusão forçada de que é necessário tomar uma decisão rápida de compra para não perder o super desconto da oferta.

Figura 8 - Promoção com contador regressivo no *site* da loja Kabum!



Fonte: Captura de tela retirada do *site* Kabum!

Esse tipo de técnica de *marketing* pode sim alavancar vendas, porém pode gerar um comportamento de risco em quem é alvo. O comportamento instintivo humano em tomar uma decisão rápida para não perder uma oportunidade acaba sendo priorizado em cima de uma análise racional do momento, podendo colocar uma pessoa em risco caso o *site* seja falso, com intuito de golpe.

2.6.1 O Caso da jornalista que permitiu ser hackeada

Em dezembro de 2014, a redatora do Telegraph Sophie Curtis decidiu ser voluntária e concordou em permitir que o *hacker* ético, John Yeo, um funcionário da empresa de segurança cibernética Trustwave, tentasse executar um ataque de engenharia social contra ela.

O trabalho de um *hacker* ético é fazer “testes de penetração[13]” para as empresas. Isso significa que eles assumem o papel de *hackers* reais e usam as

[13] Um teste de penetração, também conhecido como *pen test*, é um ataque cibernético simulado contra o sistema de um computador para verificar vulnerabilidades exploráveis.

mesmas ferramentas que *hackers* reais usam para tentar invadir os sistemas de computador de uma empresa, a fim de identificar vulnerabilidades. O *hacker* ético então conta à empresa o que eles encontraram, para que ela possa consertar as vulnerabilidades antes que um hacker real as descubra e explore.

John e sua equipe trabalharam incansavelmente para aprender o máximo que puderam sobre Sophie *online*, vasculhando a Internet por cada informação que pudessem encontrar sobre ela. Ela conta que buscaram identificar todas as contas de redes sociais, todas as contas de *e-mail* e todos os serviços *online* em que já se inscreveu e que nenhuma tentativa foi feita para invadir qualquer uma dessas contas inicialmente, simplesmente para levantar o máximo de informações possível para tentar construir um perfil de quem ela era. A partir daí usaram o Twitter para conseguir seu endereço de *e-mail* profissional, bem como ver alguns locais recentes em que participou de alguns encontros com outros jornalistas, conseguindo assim, a partir de objetos ao fundo de uma foto que ela havia postado, descobrir o celular que ela costumava usar, bem como o fato de seu noivo ser fumante e ser ciclista. Embora esses detalhes possam parecer irrelevantes, todos eles ajudaram os *hackers* a construir uma imagem de quem ela era, para que, quando se tratasse de lançar um ataque direcionado, eles pudessem torná-lo o mais pessoal possível.

Eventualmente, o time criou *e-mails* falsos, direcionados, fazendo com que Sophie não tivesse certeza se eram verdadeiros ou falsos. Em um desses *e-mails*, o time de *hackers* afirmavam ser membros de um grupo ativista mundial, que havia obtido arquivos confidenciais do governo do Reino Unido. Eles disseram que estavam trabalhando com jornais nacionais dos EUA, Alemanha, Itália, França, Brasil, Argentina e África do Sul para vazar o documento, e a convidaram para ser o principal canal de divulgação pública em nome do The Telegraph. O ponto de sucesso no ataque ocorreu quando disseram ter anexado "uma parte” do documento, que foi compactado e criptografado com uma senha forte "para reduzir o tamanho do arquivo e aumentar a segurança da comunicação". Eles disseram ainda que, se ela concordasse em publicar um artigo "de acordo com a data de lançamento global coordenada", eles lhe enviariam o documento completo e os arquivos relacionados. O documento anexado parecia ser um arquivo .rar, o que exigia uma ferramenta chamada WinRAR para extrair o arquivo. Também foi incluído no *e-mail* breves instruções para baixar o arquivo em um PC com Windows. Tudo parecendo bastante legítimo. Sophie acreditou que ela não poderia ignorar a possibilidade de que o arquivo

seria interessante para ela como jornalista, além do sentimento de urgência criado em cima da mensagem enviada a ela.

O arquivo baixado na verdade não era um arquivo .rar, mas sim um .exe com seu ícone camuflado para parecer um arquivo .rar verdadeiro e que, quando clicado, executou como qualquer aplicativo dentro do sistema operacional Windows, infectando imediatamente seu *laptop* e dando aos *hackers* acesso a tudo, incluindo sua *webcam*.

Por serem *hackers* éticos, eles pararam nesta parte, provando seu ponto de vista. Mas, para um *hacker* real, isso seria apenas o começo. Eles podiam ficar conectados ao computador por dias ou semanas, observando tudo o que era feito; eles poderiam instalar um *keylogger*[14] e registrar todas as senhas que ela digitava em todos os *sites* que visitou; eles podiam ler seus *e-mails*, entre muitas outras coisas.

2.6.2 O Massacre de Christchurch

O Massacre de Christchurch foi um atentado terrorista contra muçulmanos, ocorrido em 15 de março de 2019, na Nova Zelândia, que atingiu duas mesquitas e deixou 51 mortos.

Pouco mais de uma semana após o massacre, foram relatados golpes e ataques oportunistas relacionados à tragédia. Os relatos incluíam: fraude de doação *online*, *malware* incorporado em arquivos de vídeo, desconfiguração de *sites* da Nova Zelândia, e negação de serviço.

Eram disparados *e-mails* de *phishing* contendo *links* para *logins* em *sites* de banco *online* falsos. Esses *e-mails* também continham contas bancárias fraudulentas, onde as vítimas poderiam fazer doações para os afetados pela tragédia de Christchurch. Também foram compartilhados arquivos de vídeo maliciosos em *sites* comprometidos ou nas redes sociais, contendo imagens relacionadas ao ataque e que poderiam conter *malware* incorporado.

[14] *Keylogger* é um tipo de *software* espião usado para monitorar e registrar cada tecla pressionada em um computador específico. Frequentemente usado por cibercriminosos para roubar informações pessoais, credenciais de *login* e dados corporativos confidenciais.

2.7 POLÍTICA E O ESCÂNDALO DA CAMBRIDGE ANALYTICA

Em 2018, um escândalo em especial ganhou destaque na mídia. Foi o caso de um suposto uso indevido de dados por parte de uma empresa que atua no setor de *marketing*, a Cambridge Analytica. O problema foi noticiado simultaneamente, no dia 17 de março de 2018, pelos jornais The Guardian[15] e o The New York Times[16], logo tomando as principais manchetes dos maiores jornais de todo o mundo.

Tudo começou por volta de 2007, quando um pesquisador, David Stillwell, do Centro de Psicometria da Universidade de Cambridge desenvolveu um aplicativo para ser usado no Facebook que permitia que as pessoas fizessem testes de personalidade por conta própria e pudessem optar por compartilhar os resultados com os pesquisadores. O aplicativo apenas coletou dados sobre as pessoas que optaram por participar, e incluiu uma isenção de responsabilidade dizendo que as informações poderiam ser "armazenadas e usadas para fins comerciais, e também divulgadas a terceiros. O aplicativo foi desativado e 2012 e segundo o *site* da Universidade (CAMBRIDGE, 2021), coletou dados de mais de 6 milhões de voluntários durante todo seu período de atividade. Esses dados foram tornados anônimos e amostras deles foram compartilhadas com colaboradores acadêmicos registrados em todo o mundo por meio do projeto myPersonality, resultando em mais de 45 publicações científicas em periódicos revisados por pares.

Em março de 2013, David Stillwell, um estudante de PhD chamado Michal Kosinski e um terceiro pesquisador chamado Thore Graepel, publicaram um artigo com coautoria mostrando que os *likes*[17] do Facebook, mesmo para tópicos considerados mais simples e “bobos”, podem ser usados para prever detalhes sobre as pessoas. O artigo de Stillwell (2013) mostra que registros digitais de comportamento, facilmente acessíveis, como curtidas no Facebook, podem ser usados para prever de forma automática e precisa uma gama de atributos pessoais altamente sensíveis, incluindo: orientação sexual, etnia, pontos de vista religiosos e políticos, traços de personalidade, inteligência, felicidade, uso de substâncias

[15] Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: 12 nov. 2021

[16] Disponível em: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. Acesso em: 12 nov. 2021

[17] O botão *Like* (Curtir) é um recurso do *site* de rede social Facebook e permite que os usuários interajam facilmente com atualizações de *status*, comentários, fotos e vídeos, *links* compartilhados por amigos e anúncios.

viciantes, separação parental, idade e sexo. A análise apresentada é baseada em um conjunto de dados de mais de 58.000 voluntários que forneceram seus *likes* no Facebook, perfis demográficos detalhados e os resultados de vários testes psicométricos

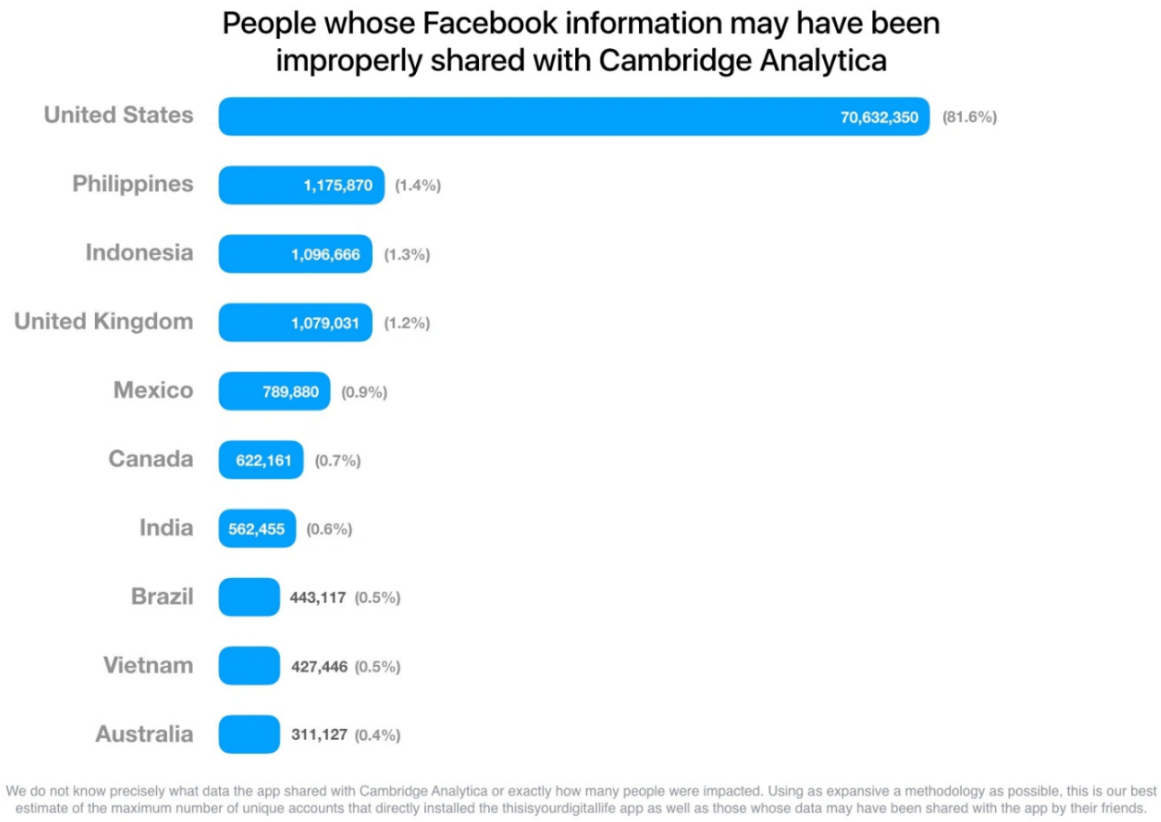
Na época, as curtidas de páginas do Facebook ainda eram públicas, o que significa que qualquer pessoa poderia coletar informações sobre todos que curtiram uma determinada página por conta própria. O artigo alertou sobre como essas previsões "podem representar uma ameaça ao bem-estar, à liberdade ou até à vida de um indivíduo" e concluiu com um apelo para que empresas como o Facebook deem aos usuários mais "transparência e controle sobre suas informações".

Então, em 2014, um ano após a publicação do artigo de Stillwell e Kosinski, um dos professores de psicologia da Universidade, Aleksandr Kogan e seu sócio Joe Chancellor abriram uma empresa chamada Global Science Research. Seu cliente, SCL Elections, que mais tarde se tornaria Cambridge Analytica, queria que Kogan trabalhasse com o Centro de Psicometria da Universidade de Cambridge para reunir dados do Facebook sobre o eleitorado americano e usá-los para entender os tipos de personalidade das pessoas para fins de publicidade política. O Centro de Psicometria da Universidade de Cambridge recusou-se a trabalhar com a Cambridge Analytica, mas Aleksandr Kogan estava disposto.

Aleksandr Kogan criou então seu próprio aplicativo, o “This Is Your Digital Life”, ou apenas “thisisyourdigitallife”, para coletar os dados no Facebook sobre milhões de usuários sem seu conhecimento. O aplicativo não apenas coletou dados sobre as pessoas que optaram por ele, mas também coletou dados sobre os amigos desses usuários no Facebook. Segundo uma matéria para revista tecnológica Wired (LAPOWSKY, 2018), entrevistando o diretor do Centro de Psicometria da Universidade de Cambridge, John Rust, se apenas 100.000 pessoas optassem pelo aplicativo e se tivessem uma média de 150 amigos cada, Kogan teria acesso aos dados de 15 milhões de pessoas, que ele poderia usar para fins de persuasão política. Dessa forma, dos 270 mil usuários que deliberadamente compartilharam seus dados com o aplicativo, foi possível traçar, até onde acreditou-se de início, o perfil de até 50 milhões de eleitores americanos. Com essas informações em mãos, Cambridge Analytica é acusada de ter realizado campanhas de micro direcionamento para favorecer a eleição de Donald Trump, em 2016, empregando meios inescrupulosos, como a divulgação de notícias falsas para criar uma mudança significativa na opinião

pública. Após o escândalo, em 2018, o Facebook passou a reconhecer (Figura 9) que Kogan coletou dados de até 87 milhões de americanos e os vendeu para Cambridge Analytica.

Figura 9 - O número de pessoas que Facebook estima terem sido afetadas pelo escândalo, e o país de origem.



Fonte: Facebook[18].

2.7.1 O ex-funcionário que delatou a Cambridge Analytica

O cientista de dados Christopher Wylie, nascido em 19 de junho de 1989 no Canadá, foi um dos grandes responsáveis por ajudar no crescimento da Cambridge Analytica e também responsável por trazer a público o escândalo sobre a empresa. Em colaboração por mais de um ano com o jornal The Guardian, ele descreveu como a empresa ligada ao ex-conselheiro de Trump, Steve Bannon, compilou dados de usuários para atingir os eleitores americanos.

[18] Disponível em: https://about.fb.com/br/news/2018/04/uma-atualizacao-nos-nossos-planos-para-restringir-acesso-aos-dados-no-facebook/

Ao The Guardian, durante uma entrevista em vídeo (CAMBRIDGE, 2018), disponível no Youtube[19], Wylie fala sobre como se sente responsável pelo escândalo e o descreve como um experimento totalmente antiético, que usou um país inteiro, sem seu consentimento ou consciência, e que brincou com a psicologia de uma nação inteira no contexto do processo democrático. Para Wylie, a Cambridge Analytica não era uma empresa qualquer. E afirma que é incorreto chamar a Cambridge Analytica de uma empresa puramente de ciência de dados ou de algoritmos, mas sim uma máquina de propaganda de serviço completo. Ele diz que se for possível controlar todos os fluxos de informação ao redor de oponentes, é possível influenciar como eles percebem o espaço de batalha e assim se torna possível então influenciar como eles irão se comportar e reagir. Wylie diz ainda que para mudar a política, primeiro precisa-se mudar a cultura, porque a política flui da cultura e, portanto, para mudar a cultura, primeiro precisa-se entender o que são as unidades da cultura. As pessoas são as unidades da cultura e assim, se o desejo for mudar a política, primeiro precisa-se mudar as pessoas para mudar a cultura.

Segundo Wylie, Steve Bannon tratava a manipulação dos dados dos eleitores estadunidenses como se fosse uma guerra cultural. E Wylie ficou responsável em construir as armas para Bannon lutar nessa guerra imaginária, mas, para isso Wylie precisaria conseguir uma fonte de dados gigantesca, o que custaria muito dinheiro. Porém, o problema foi resolvido assim que entraram em contato com Aleksandr Kogan, na Universidade de Cambridge em 2014. O que Kogan lhes ofereceu foi algo que era muito mais barato, muito mais rápido e com uma qualidade que não se comparava. Então, ao entrar no aplicativo, a Cambridge Analytica não veria apenas o perfil do Facebook do usuário que permitiu o acesso aos dados, mas também todos os perfis do Facebook de todos os amigos daquele usuário, sem a autorização deles. Foi preciso apenas acessar algumas centenas de milhares de pessoas para conseguir dados da maior parte da América.

Ele termina a entrevista dizendo que acha complicado generalizar e dizer que não confia mais em ninguém, mas que prefere viver com uma dose saudável de ceticismo em relação ao que está vendo, o que está ouvindo e com quem está falando.

[19] Cambridge Analytica whistleblower: 'We spent $1m harvesting millions of Facebook profiles' – Disponível em: https://www.youtube.com/watch?v=FXdYSQ6nu-M&ab_channel=TheGuardian

2.8 COMO SE DEFENDER DA ENGENHARIA SOCIAL

2.8.1 Como funciona o ataque

Como a maioria dos tipos de manipulação, a engenharia social baseia-se primeiro na confiança, ou falsa confiança, e depois na persuasão. Geralmente, existem quatro etapas para um ataque de engenharia social bem-sucedido.

1. Preparação: O engenheiro social reúne informações sobre suas vítimas, incluindo onde podem acessá-las, como nas redes sociais, *e-mail*, mensagem de texto, etc.
2. Infiltração: o engenheiro social aborda suas vítimas, geralmente se passando por uma fonte confiável e usando as informações coletadas sobre a vítima para se validar.
3. Exploração: O engenheiro social usa a persuasão para solicitar informações de sua vítima, como logins de conta, métodos de pagamento, informações de contato, etc., que ela pode usar para cometer seu ataque cibernético.
4. Desligamento: o engenheiro social interrompe a comunicação com a vítima, comete o ataque e sai rapidamente.

Dependendo do tipo de ataque de engenharia social, essas etapas podem durar de horas a meses. Não importa o período de tempo, conhecer os sinais de um ataque de engenharia social pode ajudar a identificar e impedir um ataque rapidamente.

2.8.2 Sinais de um ataque de engenharia social

A engenharia social pode acontecer em qualquer lugar, *online* e offline. E, ao contrário dos ciberataques tradicionais, nos quais os cibercriminosos são furtivos e querem passar despercebidos, os engenheiros sociais costumam se comunicar com suas vítimas à vista de todos. Existem alguns sinais que podem ajudar a identificar um ataque.

- Um “amigo” envia uma mensagem estranha: Os engenheiros sociais podem se passar por indivíduos confiáveis na vida de uma pessoa, incluindo um amigo, chefe, colega de trabalho e até mesmo uma instituição bancária, e enviar mensagens visíveis contendo *links* maliciosos ou *downloads*. É preciso conhecer melhor os amigos e, se algo incomum for recebido por um conhecido ou amigo, é interessante perguntar a respeito.
- Emoções intensificadas: quanto mais irritável uma pessoa estiver, maior será a chance de baixar a guarda. Os engenheiros sociais são ótimos em estimular as emoções, como medo, excitação, curiosidade, raiva, culpa ou tristeza. Em suas interações *online*, é importante considerar a causa desses gatilhos emocionais antes de agir sobre eles.
- Urgência e pressão do tempo: os engenheiros sociais não querem que haja tempo para pensar sobre suas táticas. É por isso que muitos ataques de engenharia social envolvem algum tipo de urgência, como um software de segurança cibernética que precisa ser baixado para limpar um vírus do computador. Ou um contador regressivo que ao terminar, ocasiona a perda de uma superoferta. Ou ainda a pressão por tomar alguma decisão importante rapidamente.
- Ofertas exageradamente boas: se a oferta parece boa demais para ser verdade, é potencialmente um ataque de engenharia social.
- Receber ajuda não solicitada: os engenheiros sociais podem entrar em contato disfarçados de uma empresa que fornece suporte para um problema real existente, semelhante a um esquema de suporte técnico. E assim a vítima pode ter a inocência de acreditar que eles são quem dizem ser e fornecer-lhes acesso aos dispositivos pessoais ou contas.
- O remetente não consegue provar sua identidade: em caso de existir alguma suspeita com um engenheiro social em potencial e ele não puder provar sua própria identidade, ou ainda se alterar por ser questionado sobre tal, por exemplo, é provável que ele não seja confiável.
- Avaliações falsas: não se aplica apenas a empresas que pagam pelas avaliações em lojas de aplicativos e *sites* de venda de produtos, para tornar seu produto mais atraente para os compradores. Avaliações

falsas podem ser usadas para fazer com que um *site* ou serviço pareça mais confiável e verdadeiro, o que incentiva a enviar informações pessoais, levando a vítima a ter seus dados capturados.

2.8.3 Como se defender

A melhor defesa contra os ataques de engenharia social é educar-se sobre seus riscos, sinais de alerta e soluções. O bom senso deve ser sempre levado em conta e tomar alguns cuidados extras também. Além de manter um certo ceticismo, sem exagero, com tudo o que está em volta, pois os ataques não acontecem somente *online*, na Internet.

Segundo a Norton Security (PILETTE, 2021), existem alguns cuidados a se tomar, que podem ajudar na defesa contra a engenharia social, como:

- Não clicar em *links* que não solicitados ou demasiadamente suspeitos.
- Não compartilhar em demasia informações pessoais *online*.
- Ter cuidado com amizades apenas *online*.
- Lembrar-se dos sinais de engenharia social.
- Reconhecer o que ofertas de ganhos e vantagens em demasia podem ser golpes.
- Proteger contas e redes.
- Usar a autenticação de dois fatores.
- Usar apenas senhas fortes e exclusivas e mudá-las com frequência.
- Considerar um gerenciador de senhas para controlar suas senhas fortes.
- Definir filtros de *spam*.
- Não permitir estranhos em sua rede *wifi*.
- Usar uma rede privada virtual (VPN).
- Monitorar a atividade das contas *online* com mais cuidado.
- Proteger os dispositivos.
- Não deixar os dispositivos sem supervisão.
- Usar *software* de segurança cibernética.
- Manter os *softwares* sempre atualizados.

Ainda, investir na educação de pessoal, dando ênfase à conscientização da segurança cibernética para reduzir o risco humano. Aproveitar as vantagens de ferramentas gratuitas, como simulações de *phishing*, simulações de *ransomware* e avaliação de segurança cibernética para fortalecer o conhecimento.

Educar-se sobre os vários tipos de golpes de engenharia social. Usando exemplos do mundo real ver como é fácil para qualquer pessoa ser pego de surpresa pela engenharia social. Promover comunicação contínua e campanhas sobre engenharia social, segurança cibernética, *phishing, ransomware* e os riscos que podem vir com *e-mails*, *URLs*, anexos, chamadas telefônicas e seres humanos.

2.9 A GDPR EUROPEIA E A LGPD BRASILEIRA

Logo após os acontecimentos de março de 2018 com a Cambridge Analytica, entrou em vigor na Europa, em 25 de maio de 2018, a *General Data Protection Regulation* (GDPR), ou Regulamento Geral sobre a Proteção de Dados (RGPD) em português. O escândalo chamou a atenção e indignação da mídia, do público, de parlamentares e reguladores em todo o mundo, demonstrando que sim, as pessoas se preocupam com violações de sua privacidade e abuso de poder.

A GDPR estava em desenvolvimento desde janeiro de 2012, mas, antes da regulação entrar em vigor, a proteção de dados na União Europeia (EU) era regida pela *Data Protection Directive* (Diretiva de Proteção de Dados) de 1995.

Em 14 agosto de 2018 foi aprovada no Brasil a Lei Geral de Proteção de Dados, a LGPD, (Lei 13.709/18), que entrou em vigor somente em agosto de 2020. O principal objetivo da lei é regulamentar o tratamento de dados pessoais de clientes e usuários de empresas públicas ou privadas.

A partir de agosto de 2021, qualquer empresa que incluir em sua base de dados de clientes quaisquer informações pessoais, por mais básicas que sejam, como nome e *e-mail*, deverá seguir o que está previsto na nova Lei Geral de Proteção de Dados. E, em caso de descumprimento, a empresa poderá ser multada em um valor que pode ser de até 2% (dois por cento) do faturamento (multa simples ou diária) e limitada a R$ 50 milhões, por infração (art. 52 da LGPD)[20]; as fiscalizações e as sanções previstas pela LGPD passarão a ocorrer sob a ação da Autoridade Nacional de

[20] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Proteção de Dados (ANPD). A ANPD é um órgão independente e parte do Poder Executivo do Governo Federal e é composta por membros não remunerados, que formam um conselho diretor de cinco pessoas indicadas pelo Poder Executivo e aprovadas pelo Senado e também por outros servidores, divididos entre sociedade civil, instituições científicas, setor produtivo, Senado, Câmara dos deputados e Ministério Público, por empresários e trabalhadores.

A Lei Geral de Proteção de Dados, foi criada para acompanhar o modelo europeu, a GDPR. Mas, enquanto a LGPD ainda está começando a aplicar as penalidades, a GDPR já aplicou multas de valores bastantes altos em algumas empresas como no Whatsapp[21], em 225 milhões de Euros, por não ser claro com os cidadãos sobre como compartilha as informações pessoais dos usuários com a empresa matriz, o Facebook; na Amazon[22], em 746 milhões de Euros, e no Google[23], em 50 milhões de Euros, por não ser transparente e claro na maneira como informa usuários sobre seu trato com dados pessoais e por não obter consentimento apropriado dos usuários para envio de anúncios publicitários personalizados.

No Brasil, diversas páginas já estão adequadas à LGPD e mostram avisos em suas páginas iniciais sobre a coleta e armazenamento de dados, assim como dispõe de política de privacidade próprias, como mostrado na Figura 10 e na Figura 11.

[21] Disponível em: https://olhardigital.com.br/2021/09/02/Internet-e-redes-sociais/whatsapp-foi-multado-em-mais-de-r-1-bi-apos-violar-lei-de-privacidade-da-uniao-europeia/. Acesso em: 15 nov. 2021.

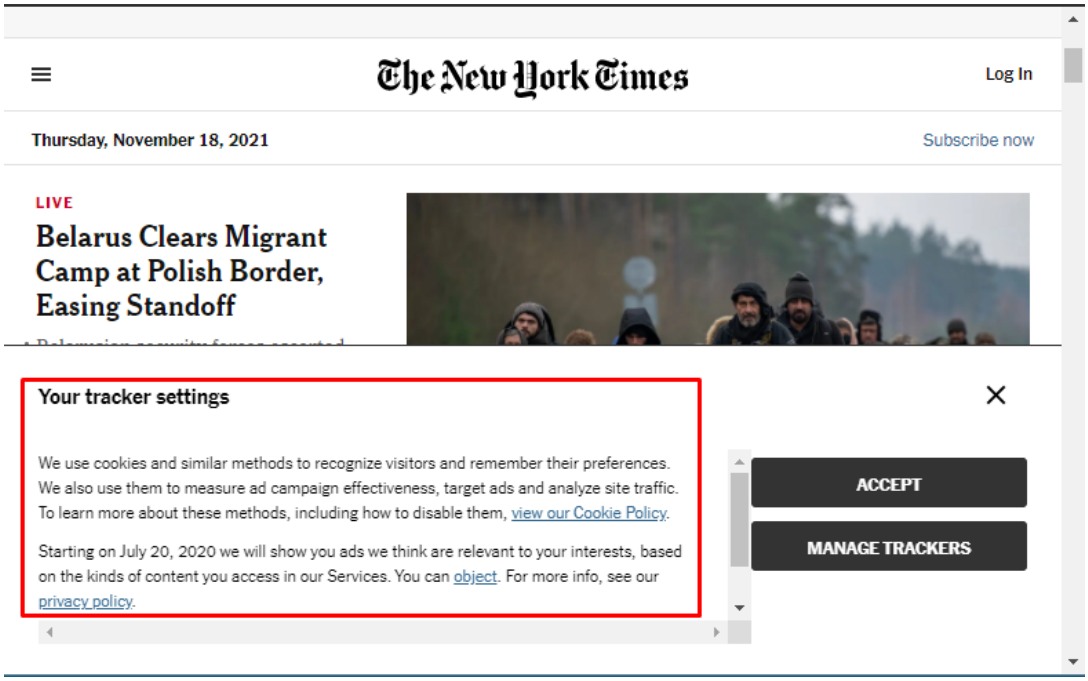
[22] Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/07/30/amazon-recebe-multa-recorde-de-746-milhoes-de-euros-na-uniao-europeia-por-questoes-de-privacidade.ghtml. Acesso em: 15 nov. 2021.

[23] Disponível em: https://forbes.com.br/negocios/2019/01/franca-multa-google-em-e-50-milhoes/. Acesso em: 15 nov. 2021.

Figura 10 - Aviso de coleta de cookies no *site* g1.globo.com

Fonte: Captura de tela retirada da página inicial do *site* de notícias G1.

Figura 11 - Aviso de coleta de cookies no *site* nytimes.com



Fonte: Captura de tela retirada da página inicial do *site* The New York Times.

O surgimento das *fake news* e a maneira como os fatos podem ser distorcidos, muitas vezes sem mentir completamente, para se adequar a uma agenda específica é, por si só, um exemplo de engenharia social. Espalhar notícias falsas por meio de grupos organizados no Twitter e no Facebook é outra forma de engenharia social. A criação de leis e regulamentos para coibir e punir o vazamento de dados traz mais uma arma na luta contra esse grande problema que são as *fake news* e os problemas causados por elas.

3 *FAKE NEWS*

O termo *Fake news*, que traduzido do inglês significa, literalmente, “Notícias Falsas”, é recente e se popularizou em 2016 nas eleições presidenciais dos Estados Unidos.

> As eleições norte-americanas de 2016 são um grande exemplo da propagação de *fake news* e, nesse caso, como a propagação de notícias falsas pode servir para um fim específico como ferramenta política, no sentido de acirrar a disputa eleitoral, podendo influenciar pessoas nas redes sociais ou no ambiente da Internet, evidenciando como a geração de desinformação pode gerar vantagens e manipular a opinião pública. Nesse ano que efetivamente o termo *fake news* ganhou notoriedade e mereceu atenção por parte da sociedade. (FAUSTINO, 2019)

Com o avanço das tecnologias da informação, acesso à Internet, inclusão digital[24], maiores possibilidades de busca de informação, surgiu um novo desafio no meio político. As redes sociais e o mundo digital *online* possibilitaram a disseminação maior de uma forma de populismo[25] e da manipulação descarada da opinião pública. O surgimento das *fake news* foi tão marcante nas eleições presidenciais dos EUA, que o Dicionário Oxford elegeu o neologismo *Post-truth* (pós-verdade) como a palavra do ano em 2016, cujo significado, segundo Hancock (2016), é “relativo ou referente a circunstâncias nas quais os fatos objetivos são menos influentes na opinião pública do que as emoções e as crenças pessoais”. A pós-verdade se tornou um termo muito utilizado e aceito por razão da grande quantidade de *fake news* disseminadas nas eleições norte americanas e que distorciam a realidade de tal forma, que parecia uma realidade alternativa.

A manipulação de informações verdadeiras, convertendo-as em algo falso e tendencioso pode trazer grandes prejuízos à toda uma sociedade, como lembra Faustino (2019):

> Um exemplo da utilização das redes sociais e manipulação de conteúdo, nas eleições norte-americanas de 2016, foi o escândalo da Cambridge Analytica.

[24] Ato de trazer para o mundo da informática pessoas que têm pouco ou nenhum contato com o computador, com o objetivo de qualificá-las para o trabalho, dar-lhes oportunidade de entrar na comunicação eletrônica, facilitar-lhes o trabalho de pesquisa com o uso da Internet etc. (MICHAELIS, 2021)

[25] Prática política que se baseia em angariar a simpatia das classes menos favorecidas e de menor poder aquisitivo pregando a defesa de seus interesses, geralmente através de ações paternalistas e assistencialistas. (MICHAELIS, 2021)

> A empresa inglesa utilizava informações dos usuários de Internet buscando impulsionar os comportamentos e direcionando para um tipo de voto a favor de determinado candidato. Ela mapeava o perfil do usuário, buscava o conteúdo próximo àquele perfil e depois direcionava. Esse conteúdo muitas vezes não era, necessariamente, ligado à verdade, mas apenas adequado ao tipo de perfil-alvo. As *fake news* encontraram nas redes sociais o ambiente perfeito para a sua propagação. No caso das eleições norte-americanas de 2016, foram fundamentais para o resultado final daquele pleito, pois facilitaram a circulação do conteúdo falso e a participação e engajamento das pessoas com esse tipo de mentira, onde a circulação da desinformação on-line, devido a sua estrutura e velocidade, criou um ambiente perfeito de desinformação.

Apesar do termo recente, as notícias falsas, ou com informações distorcidas com relação à verdade, existem há séculos. O sensacionalismo sempre vendeu bem. No início do século 19, os jornais divulgavam furos e denúncias, mas também histórias falsas para aumentar a circulação. As *fake news* sempre estiveram presentes ao longo da história, hoje com este nome, o meio utilizado para divulgação e o potencial de persuasão que o material falso adquiriu nos últimos anos.

Muito antes de o Jornalismo ser prejudicado pelas *fake news*, escritores já propagavam falsas informações sobre seus desafetos por meio de comunicados e obras. Anos mais tarde, a propaganda tornou-se o veículo utilizado para espalhar dados distorcidos para a população, o que ganhou força no século XX.

Uma matéria do jornal El País (ALTARES, 2018), cita o trabalho de um historiador francês, Marc Bloch, autor de um ensaio chamado *Réflexions d'Un Historien Sur les Fausses Nouvelles de la Guerre*, (Reflexões de um historiador sobre a notícias falsas da guerra) e publicado em 1921. Segundo a matéria, ele:

> [...] Retornou das trincheiras da Primeira Guerra Mundial alucinado com a importância que as notícias falsas haviam tido. Isso o levou a refletir sobre sua origem e difusão, num texto que poderia ter sido escrito na era do Brexit, de Vladimir Putin e de Donald Trump, nestes tempos das redes sociais e de mensagens virais. "As notícias falsas mobilizaram as massas. As notícias falsas, em todas as suas formas, encheram a vida da humanidade. Como nascem? De que elementos extraem sua substância? Como se propagam e crescem?", escreve, para afirmar um pouco mais adiante: "Um erro só se propaga e se amplifica, só ganha vida com uma condição: encontrar um caldo de cultivo favorável na sociedade onde se expande. Nele, de forma inconsciente, os homens expressam seus preconceitos, seus ódios, seus temores, todas as suas emoções". Em outras palavras, as notícias falsas necessitam de gente que queira acreditar nelas.

O jornal cita também três grandes conflitos em que os Estados Unidos participou, no século XX, por conta de notícias falsas.

> [...] A guerra de Cuba (1898), com a manipulação dos jornais; a guerra do Vietnã (1955-1975), com o incidente do golfo de Tonkin, e a invasão do Iraque de 2003, com as inexistentes armas de destruição em massa de Saddam Hussein. “A guerra contra a Espanha [em 1898] foi obra de Hearst e de Pulitzer”, escreveu o repórter Manuel Leguineche em seu ensaio sobre o nascimento do jornalismo sensacionalista, Yo Pondré la Guerra (“eu porei a guerra”, El País Aguilar). “Foi sua grande oportunidade de mudar a história, de criar uma psicose de guerra, de fabricá-la, por meio de sensacionalismo, tiragem, circulação milionária, venda maciça, chute no estômago do leitor”.

As mentiras que se espalham e convencem as massas não surgiram com as redes sociais. Elas vieram bem antes da Internet, mas sempre necessitaram de um público menos crítico, manipulável, que acreditasse realmente na informação que lhes fosse conveniente, mesmo que distorcida da realidade.

3.1 NOTÍCIAS FALSAS E AS MÍDIAS SOCIAIS

Plataformas de mídia social como Facebook e Twitter permitem o compartilhamento de informações entre seus usuários, e muitas dessas plataformas apresentam itens de “notícias”, anúncios ou “conteúdo patrocinado” de uma maneira que torna difícil distinguir fontes de notícias reais de *sites* falsificados ou fraudulentos. A maior parte do espaço de anúncio da plataforma de mídia social é vendida por meio de corretores, o que significa que a plataforma geralmente não tem ideia do que está sendo anunciado em seu *site*. Essas características tornam as plataformas de mídia social um lugar ideal para o surgimento de notícias falsas.

Aplicativos de mensagens instantâneas agregaram ao dia a dia uma forma muito mais rápida e prática de comunicação e difusão de informação e, por estas facilidades e por sua fácil utilização, no Brasil[26],o Whatsapp se tornou um dos principais espalhadores de *fake news* no seu seguimento.

O Facebook e Instagram são as redes sociais mais usadas[27] hoje pelos brasileiros. Seguidos pelo *site* de vídeos Youtube. Todas esses sendo locais de ampla criação e divulgação de *fake news*, o que não é o propósito de nenhuma dessas redes. Felizmente, com uso de algoritmos e *machine learning* [28] é possível rastrear *fake news*

[26] Desde 2020, WhatsApp lidera como aplicativo mais popular com 99% de adesão: Disponível em: https://olhardigital.com.br/2021/09/02/Internet-e-redes-sociais/desde-2020-whatsapp-lidera-como-aplicativo-mais-popular-com-99-de-adesao/. Acesso em: 20 nov. 2021

[27] Disponível em: https://www1.folha.uol.com.br/mercado/2019/04/facebook-registra-tendencia-de-queda-no-brasil-diz-datafolha.shtml. Acesso em: 20 nov. 2021.

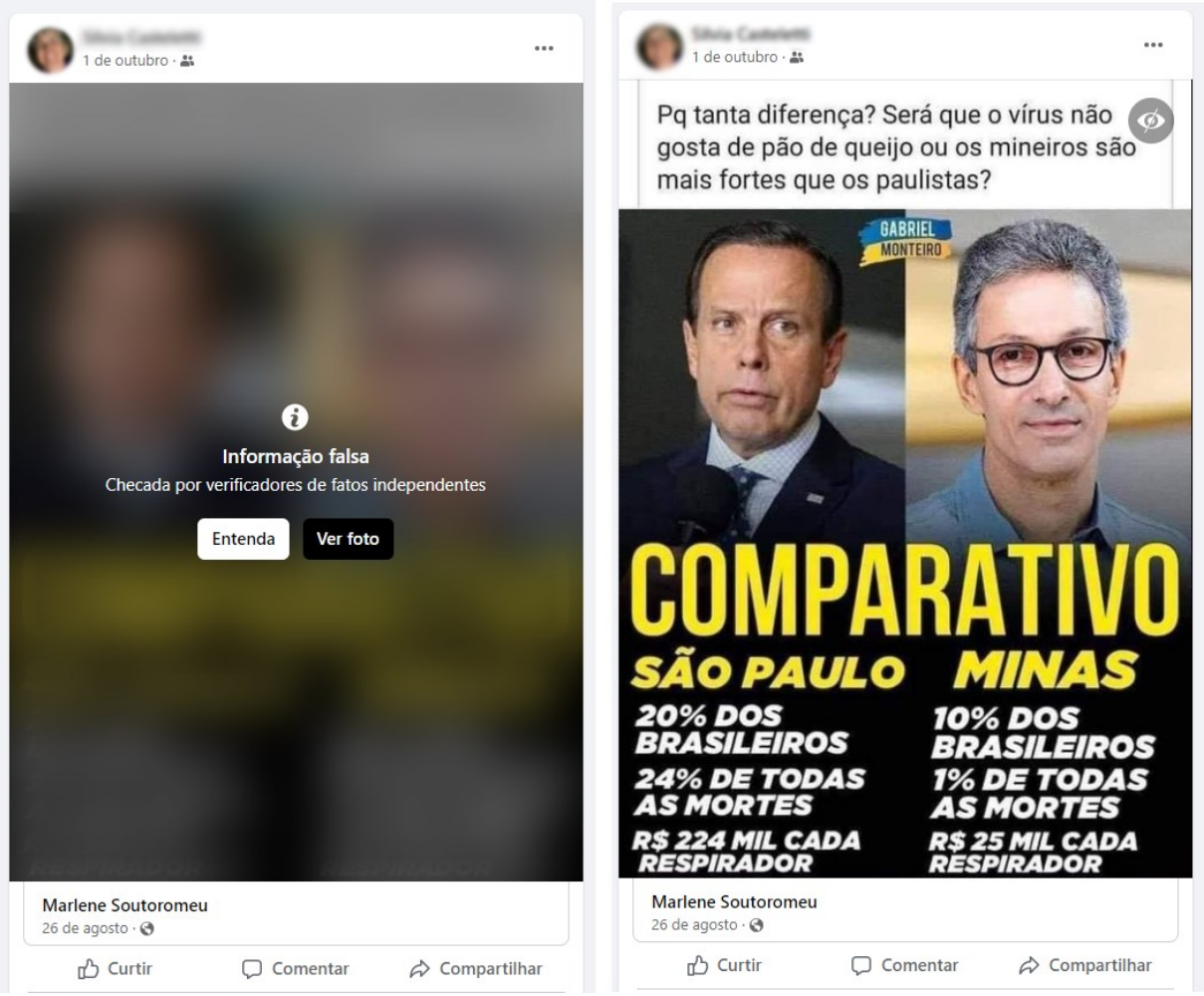
[28] Disponível em: https://brasil.elpais.com/tecnologia/2020-06-11/fake-news-seguem-padroes-concretos-e-os-algoritmos-ja-conseguem-rastrea-los.html. Acesso em: 20 nov. 2021.

nas redes e tentar combater este problema, ao mesmo tempo em que educa os usuários.

3.2 CASOS NAS REDES

Mesmo com a atividade do algoritmo anti *fake news* do Facebook, ainda é possível deparar-se com usuários estimulados a continuar postando suas convicções, mesmo que informados de que estão compartilhando *fake news*, como observado na Figura 12.

Figura 12 - Usuária do Facebook em postagem contendo *fake news*.



Fonte: Captura de tela. Acervo próprio, 2021.

No exemplo da Figura 12, é possível observar que a imagem à direita é uma continuação da imagem à esquerda e que nesta primeira imagem existe um botão

“Entenda” e outro botão “Ver foto”. O botão “Ver foto” revela o que foi ocultado por ser *fake news* enquanto o botão “Entenda” revela por qual motivo a postagem foi marcada como *fake news,* e ainda indica o *link*[29] para a checagem dos fatos e também por qual agência verificadora foi feita a checagem, como mostrado na Figura 13.

Figura 13 - Quadro mostrado após clicar no botão "Entenda" na postagem sinalizada como *fake news*.

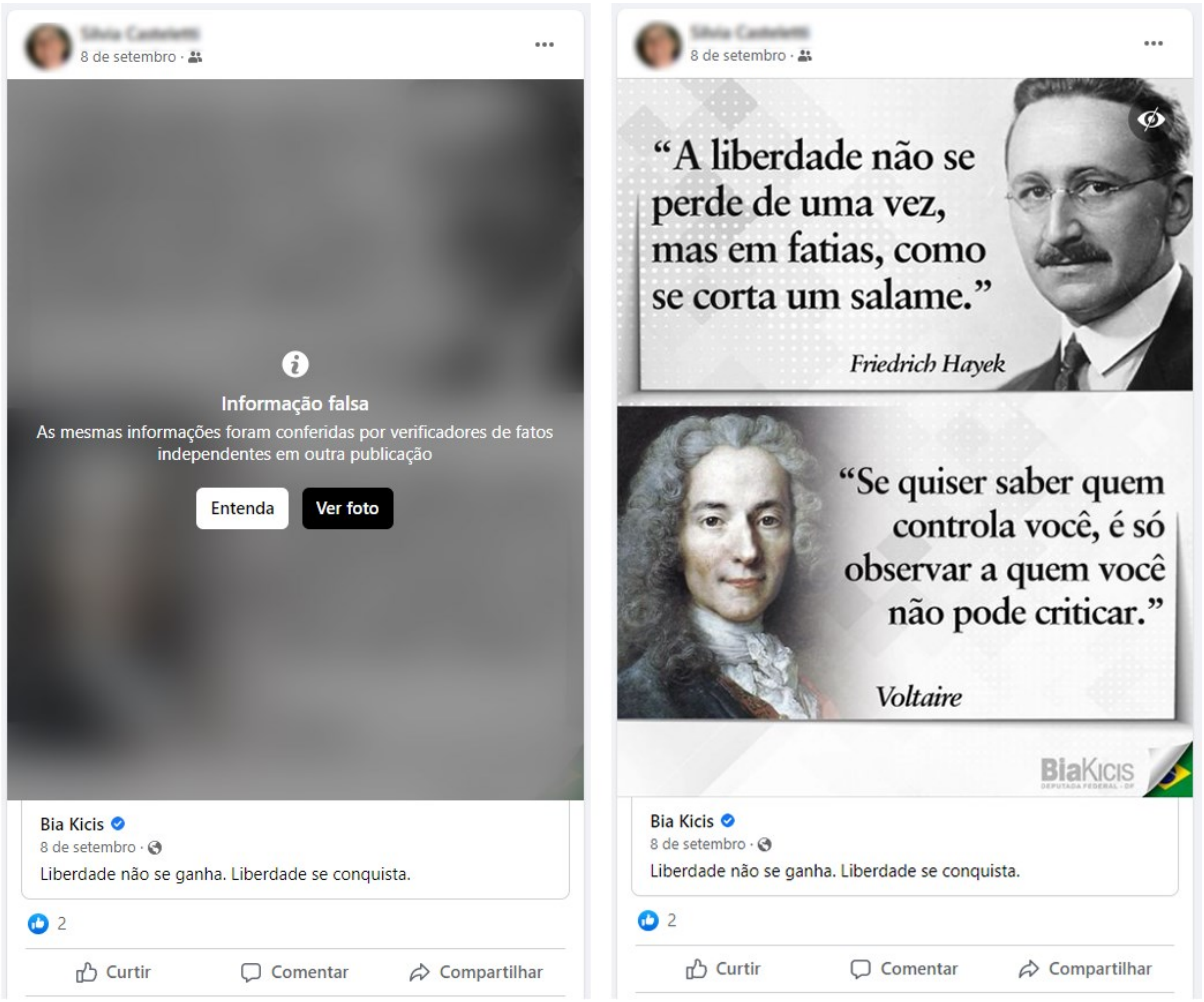
Fonte: Captura de tela. Acervo próprio, 2021.

Por mais que o Facebook reconheça um post com *fake news,* ele não remove a publicação. É possível encontrar postagens mais antigas de usuários, também marcadas como *fake news,* que permanecem intactas pela rede social (Figura 14). Segundo um porta-voz[30] do Facebook, a plataforma remove "conteúdo no Facebook e Instagram que viole nossos Padrões da Comunidade, que não permitem desinformação que possa causar danos reais às pessoas".

[29] Meme usa dados falsos para promover Romeu Zema e faz comparação imprecisa sobre combate à pandemia em SP e MG. Disponível em: https://politica.estadao.com.br/blogs/estadao-verifica/meme-faz-comparacao-imprecisa-sobre-combate-a-pandemia-em-sp-e-mg-e-usa-dados-falsos-para-exaltar-desempenho-de-romeu-zema/. Acesso em: 20 nov. 2021.

[30] Facebook e Instagram removem vídeo de Jair Bolsonaro por violação de regras. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/03/30/facebook-e-instagram-removem-video-de-jair-bolsonaro-por-violacao-de-regras.ghtml. Acesso em: 20 nov. 2021.

Figura 14 - Usuária do Facebook em postagem contendo *fake news*, em postagem mais antiga.

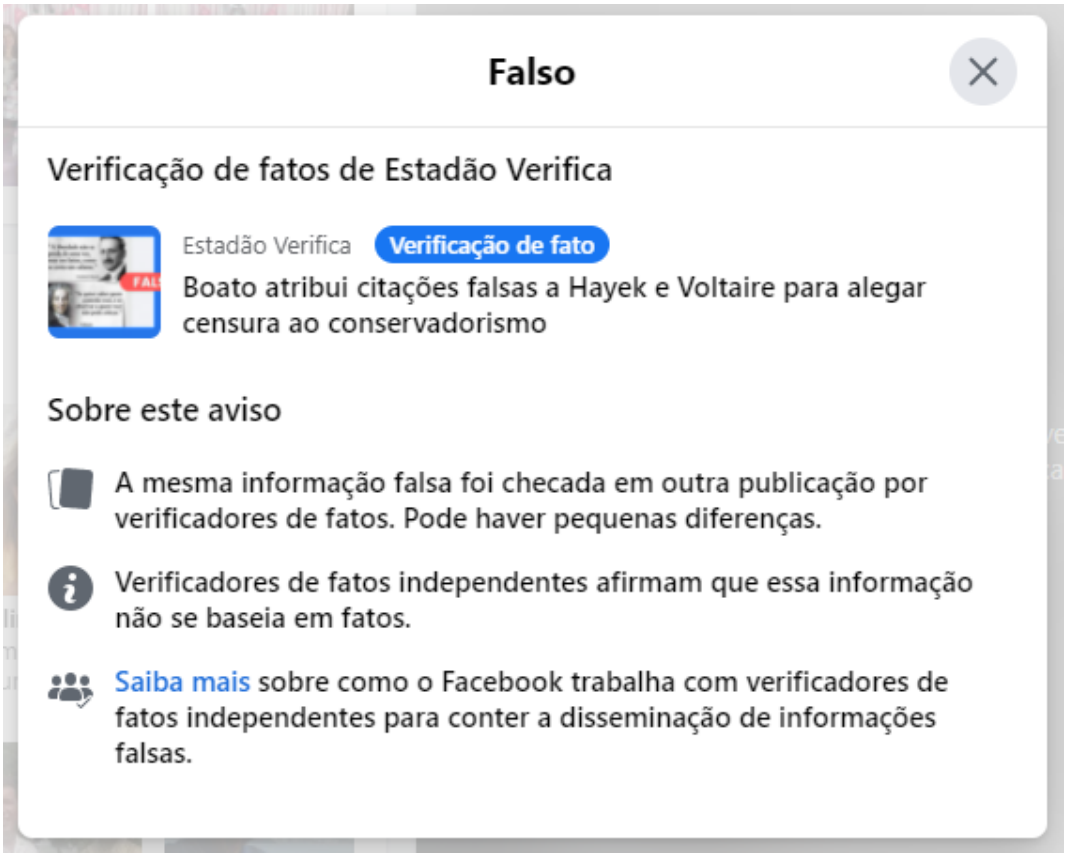


Fonte: Captura de tela. Acervo próprio, 2021.

Como demonstrado no exemplo anterior, da Figura 14, também é exibido o botão "Entenda" neste *post* sinalizado como *fake news*, mostrando novamente um quadro com o *link*[31] para a checagem da informação verdadeira, como pode ser visto na Figura 15.

[31] Boato atribui citações falsas a Hayek e Voltaire para alegar censura ao conservadorismo. Disponível em: https://politica.estadao.com.br/blogs/estadao-verifica/hayek-liberdade-salame-voltaire-quem-controla/. Acesso em: 20 nov. 2021.

Figura 15 - Quadro mostrado após clicar no botão "Entenda" na postagem sinalizada como *fake news*.



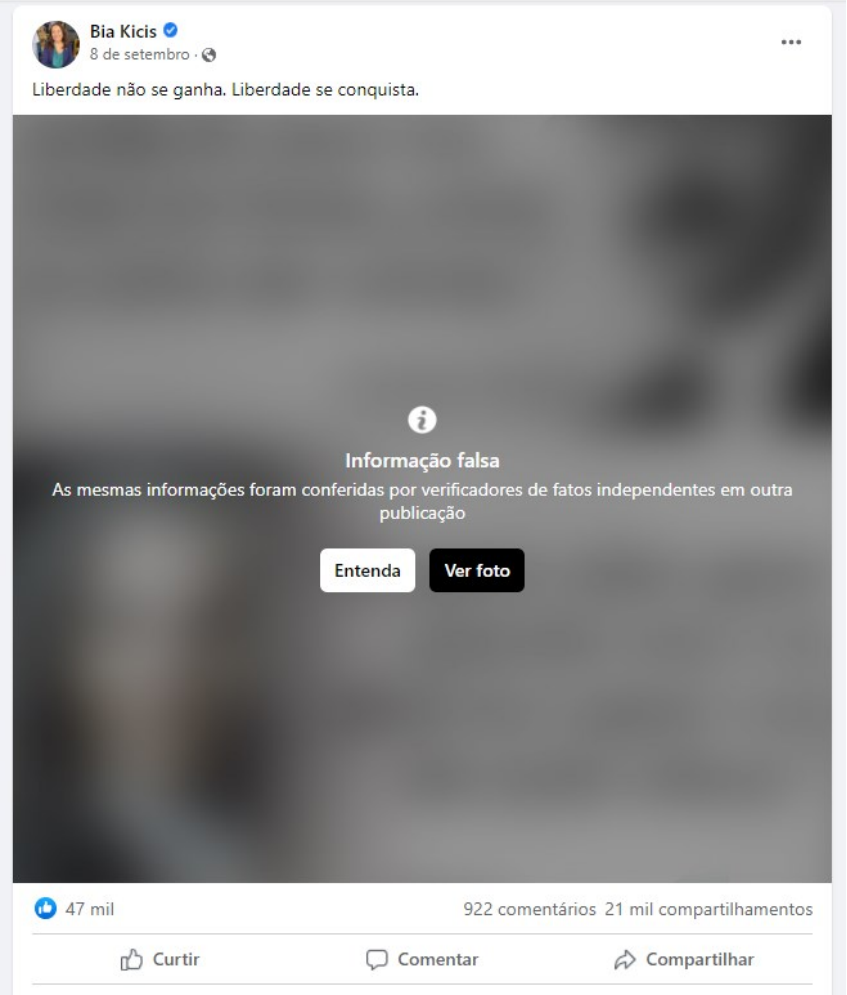
Fonte: Captura de tela. Acervo próprio, 2021.

Um ponto importante aqui é observar que na Figura 14, o autor original da postagem, como pode ser visto logo abaixo da imagem, é Bia Kicis. A conta ainda possui perfil verificado[32], que significa que o Facebook confirmou que uma página ou perfil é a presença autêntica da figura pública, como pode ser visto pelo ícone de checagem na cor azul. Bia Kicis é uma Deputada Federal pelo Partido Social Liberal (PSL), ou seja, é realmente uma pessoa pública, uma política. Ainda assim, com sua publicação sinalizada como *fake news* no dia 08 de setembro de 2021, a deputada não removeu a publicação. Sendo possível acessar o *post* pela página da deputada no Facebook ou ainda via *link*[33] direto.

[32] Disponível em: https://www.facebook.com/help/196050490547892

[33] Disponível em: https://www.facebook.com/biakicisoficial/posts/2082022318630986. Acesso em: 21 nov. 2021.

Figura 16 - Postagem original da deputada Bia Kicis em sua página no Facebook.



Fonte: Captura de tela. Acervo próprio, 2021.

Na Figura 16, é possível notar que a publicação da deputada atingiu 47 mil *likes*, 922 comentários e 21 mil compartilhamentos. Considerando-se que uma pessoa tem em média, no Facebook, 150[34] amigos, podendo chegar ao máximo de 5 mil amigos (limite imposto pela rede social), os compartilhamentos da postagem de Bia Kicis com *fake news* poderiam ter atingindo (aparecido na linha do tempo do usuário), no mínimo, 3.150.000 (três milhões cento e cinquenta mil) pessoas (21 mil compartilhamentos únicos multiplicados por 150 amigos); E no máximo para 105.000.000 (cento e cinco milhões) de pessoas (21 mil compartilhamentos únicos multiplicados por 5 mil amigos); Isto sem levar em consideração que o Facebook não

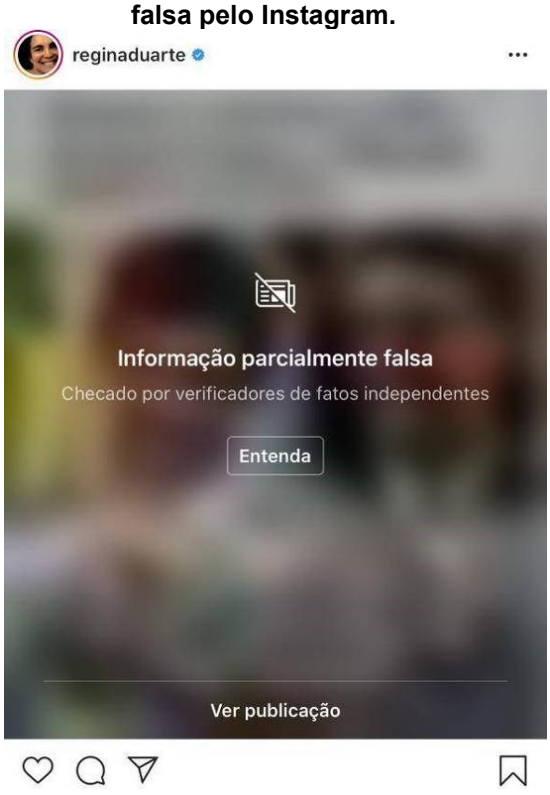
[34] Disponível em: https://www.uol.com.br/vivabem/noticias/redacao/2018/08/23/existe-um-numero-maximo-de-amigos-que-uma-pessoa-consegue-ter.htm. Acesso em: 21 nov. 2021.

mostra todos os nossos compartilhamentos para todos os nossos amigos, para evitar sobrecarga[35] na linha do tempo. É um número alto, apesar do risco desta *fake news* não gerar riscos físicos para ninguém.

O Instagram[36] (empresa pertencente ao Facebook), no final de 2019 também começou a trabalhar no combate às *fake news* sinalizando publicações parcial ou totalmente falsas. Segundo o *site* de tecnologia Tecnoblog (VENTURA, 2019), “se a foto ou o vídeo tiver conteúdo considerado falso por uma agência independente de checagem de fatos, ele será borrado e terá o aviso de que a informação não procede”.

Em abril de 2020, a então secretária especial de Cultura Regina Duarte, teve uma publicação sinalizada como parcialmente falsa pelo Instagram ao postar uma imagem com o texto “Liberação da cloroquina/hidroxicloroquina pela Anvisa, já com posologia para tratamento da Covid-19 (Figura 17).

Figura 17 - Publicação de Regina Duarte marcada como parcialmente falsa pelo Instagram.



Fonte: Folha de São Paulo[37].

[35] Disponível em: https://www.tecmundo.com.br/facebook/9223-por-que-nao-consigo-ver-todas-as-atualizacoes-dos-meus-amigos-no-facebook-.htm. Acesso em: 21 nov. 2021.

[36] Disponível em: https://olhardigital.com.br/2019/12/17/noticias/instagram-lanca-recurso-para-sinalizar-e-combater-desinformacao/. Acesso em: 22 nov. 2021.

[37] Disponível em: https://www1.folha.uol.com.br/colunas/monicabergamo/2020/04/instagram-avisa-que-regina-duarte-publicou-noticia-parcialmente-falsa.shtml. Acesso em: 23 nov. 2021.

O Instagram colocou este aviso porque a autorização concedida pela Anvisa era para pesquisa com hidroxicloroquina no tratamento da Covid-19 e não liberação para uso contra o Covid-19. Segundo o aviso do Instagram, a informação foi verificada pela AFP América Latina.

Segundo os principais veículos brasileiros de notícias (Estadão[38], Yahoo[39], El País[40], Terra[41]), em outubro de 2021, o Facebook[42] e o Instagram removeram uma *live* do Presidente do Brasil com informações falsas relacionando a vacina da Covid e Aids. Segundo o Facebook, as políticas da rede não permitem alegações de que as vacinas de Covid-19 matam ou podem causar danos graves às pessoas. O YouTube[43] seguiu as outras duas redes e suspendeu o canal por uma semana. Segundo a plataforma, o vídeo viola diretrizes contra desinformação médica sobre a Covid-19. Na *live*, para embasar sua afirmação, o presidente citava "relatórios oficiais do governo do Reino Unido", que depois foram desmentidos[44] pelo Departamento de Saúde e Assistência Social do Reino Unido, após contato de jornalistas brasileiros.

No Brasil, em 27 de abril de 2021, foi instaurada a "CPI da Pandemia" e finalizada em 26 de outubro de 2021. Em seu relatório[45] final, o presidente é chamado de líder e porta-voz da comunicação enganosa, devido as comprovadas inúmeras notícias falsas espalhadas por ele durante seu mandato. O relatório ainda acusa a família do presidente de agravar a pandemia de covid-19 através de uma campanha de desinformação. De acordo com uma matéria do jornal El País (OLIVEIRA, 2021), o relatório ainda aponta que:

---

[38] Disponível em: https://politica.estadao.com.br/noticias/geral,facebook-e-instagram-excluem-live-de-bolsonaro-com-fake-news-sobre-aids-e-a-vacina-da-covid,70003879214. Acesso em: 22 nov. 2021.

[39] Disponível em: https://br.noticias.yahoo.com/facebook-instagram-derrubam-live-bolsonaro-aids-vacina-covid-19-102216627.html. Acesso em: 22 nov. 2021.

[40] Disponível em: https://brasil.elpais.com/brasil/2021-10-25/facebook-e-instagram-bloqueiam-live-semanal-de-bolsonaro-apos-presidente-vincular-aids-a-vacina-contra-covid-19.html. Acesso em: 22 nov. 2021.

[41] Disponível em: https://www.terra.com.br/noticias/coronavirus/facebook-e-instagram-excluem-live-de-bolsonaro-com-fake-news-sobre-aids-e-a-vacina-da-covid,7af851c0f6762c4026e42c6fceb06df4o953yzk9.html. Acesso em: 22 nov. 2021.

[42] Disponível em: https://g1.globo.com/tecnologia/noticia/2021/10/25/live-bolsonaro.ghtml. Acesso em: 22 nov. 2021.

[43] Disponível em: https://g1.globo.com/tecnologia/noticia/2021/10/25/youtube-live-bolsonaro.ghtml. Acesso em: 23 nov. 2021.

[44] Disponível em: https://g1.globo.com/fato-ou-fake/coronavirus/noticia/2021/10/22/e-fake-que-relatorios-do-governo-do-reino-unido-sugerem-que-vacinados-contra-covid-tem-desenvolvido-aids.ghtml. Acesso em: 23 nov. 2021.

[45] Disponível em: https://www12.senado.leg.br/noticias/arquivos/2021/10/26/relatorio_final-26102021-12h40-1.pdf

> Há ainda o núcleo de produção e disseminação de *fake news*, no qual estão influenciadores como o blogueiro bolsonarista Allan dos Santos, os veículos de mídia organizados, como Terça Livre e Brasil Paralelo, e os perfis anônimos —não raramente, robôs comandados por membros do gabinete do ódio, aponta o documento. Por fim, há o núcleo de financiamento, que sustenta economicamente a organização, gerando o impulsionamento das *fake news*, e é representado pelos empresários Otávio Fakhoury, que integra o Instituto Força Brasil, e Luciano Hang, ambos investigados pela CPI.

Assim, entende-se que as *fake news* usadas como massa de manobra de toda uma população podem ter um custo muito alto. Não sendo apenas boatos espelhados por pessoas aleatórias, mas sim por um chefe de estado conhecido por toda a nação. Uma pessoa pública de grande influência.

O *site* de notícias G1 fez uma extensa reportagem[46] sobre famílias que sofreram perdas pela Covid-19 ocasionadas principalmente por conta das *fake news.* Nesta reportagem, são entrevistadas quatro pessoas que contam suas histórias em matérias diferentes. Rodrigo[47], um dos entrevistados diz que seu pai deixou de ir ao hospital por acreditar em tratamento precoce por ter sido vítima das *fake news*; Adriana[48] diz que sua mãe ignorou o médico, mentiu para a família e morreu sem acreditar que estava com Covid porque só via *fake news*; Marconi[49] diz que ignorou pedido de seu filho para usar máscara e foi parar no hospital porque achava que Covid não era tão grave; Iomar[50] diz que não levava a sério a pandemia até perder a esposa, irmão e sogros, e diz ainda que poderia ter se cuidado mais.

Em 2014, a dona de casa Fabiane Maria de Jesus foi espancada por moradores, no Guarujá, após o compartilhamento de *fake news* em um grupo de Facebook referente à cidade.

---

[46] Disponível em: https://g1.globo.com/saude/coronavirus/noticia/2021/10/18/vitimas-do-negacionismo-as-mortes-causadas-pela-desinformacao-na-pandemia-da-covid-19.ghtml. Acesso em: 23 nov. 2021.

[47] Disponível em: https://g1.globo.com/saude/coronavirus/noticia/2021/10/19/ele-deixou-de-ir-ao-hospital-por-acreditar-em-tratamento-precoce-e-nao-levar-a-covid-a-serio-meu-pai-foi-vitima-das-fake-news.ghtml. Acesso em: 23 nov. 2021.

[48] Disponível em: https://g1.globo.com/saude/coronavirus/noticia/2021/10/21/ela-ignorou-o-medico-mentiu-para-a-familia-e-morreu-sem-acreditar-que-estava-com-covid-so-via-fake-news-diz-filha.ghtml. Acesso em: 23 nov. 2021.

[49] Disponível em: https://g1.globo.com/saude/coronavirus/noticia/2021/10/20/ele-ignorou-o-pedido-do-filho-para-usar-mascara-e-foi-parar-no-hospital-de-cadeira-de-rodas-achava-que-covid-nao-era-tao-grave.ghtml. Acesso em: 23 nov. 2021.

[50] Disponível em: https://g1.globo.com/saude/coronavirus/noticia/2021/10/22/ele-nao-levava-a-serio-a-pandemia-ate-perder-a-esposa-o-irmao-e-os-sogros-para-a-covid-poderia-ter-me-cuidado-mais.ghtml. Acesso em: 23 nov. 2021.

> Dias antes do linchamento, uma página no Facebook chamada “Guarujá Alerta”, com 56 mil curtidas, publicou informações sobre “uma mulher que está raptando crianças para realizar magia negra”, supostamente na região. Além da frase “se é boato ou não devemos ficar alerta”, o administrador postou imagens: um retrato falado (associado a um crime cometido no Rio, em 2012) e a foto de uma mulher loira, que tampouco tinha a ver com o caso. As duas eram bem diferentes entre si. E nenhuma delas parecia Fabiane, que morreu ao ser confundida com a tal sequestradora. (CARPANEZ, 2018)

Além de *fake news* relacionadas a boatos, existem também as *fake news* relacionadas a golpes. Algumas muito divulgadas por *whatsapp*, prometendo prêmios para pessoa que divulgarem *links* de supostas promoções para o maior número de pessoas possível.

Figura 18 - *Link* enviado por Whatsapp se passando por promoção de passagens aéreas da companhia Gol

Fonte: Captura de tela. Acervo próprio, 2021.

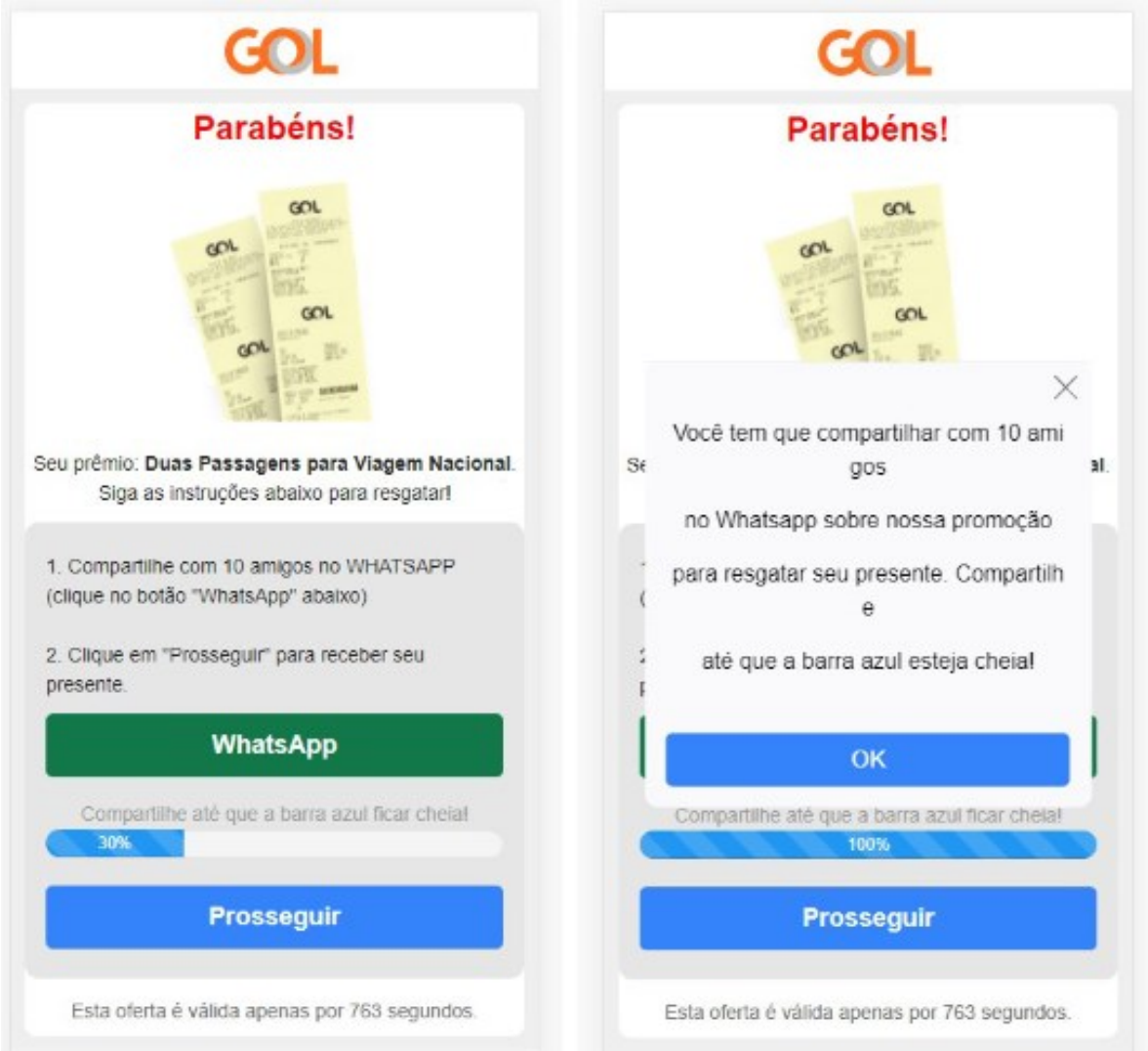
Como pode ser visto na Figura 18, neste trabalho foi analisado um *link enviado* por Whatsapp, com endereço seguro (HTTPS), dando a entender que existe uma promoção de passagens grátis oferecidas pela companhia Gol. O endereço leva a acreditar que realmente se trata do *site* da companhia. Porém o endereço verdadeiro é https://www.voegol.com.br. O endereço falso é muito parecido com o endereço verdadeiro da companhia aérea Gol, tendo o golpista apenas trocado as letras de lugar; o que faz total diferença para um domínio na Internet, mas para uma pessoa leiga informacionalmente, pode não fazer.

Figura 19 - *Site* falso se passando pela Gol, acessado de um smartphone.

Fonte: Captura de tela. Acervo próprio, 2021.

Na Figura 19, é possível ver que o *site* tenta passar a ideia de que se forem respondidas algumas perguntas, é possível concorrer às passagens aéreas da Gol. Existe um contador, mas mostrando a quantidade de passagens restantes, o que gera a sensação de urgência no internauta. O *site* tenta ainda passar uma ideia de idoneidade, colocando supostos comentários de quem teria conseguido as passagens da “promoção”.

Figura 20 – *Site* falso solicitando o compartilhamento da promoção com mais 10 amigos.



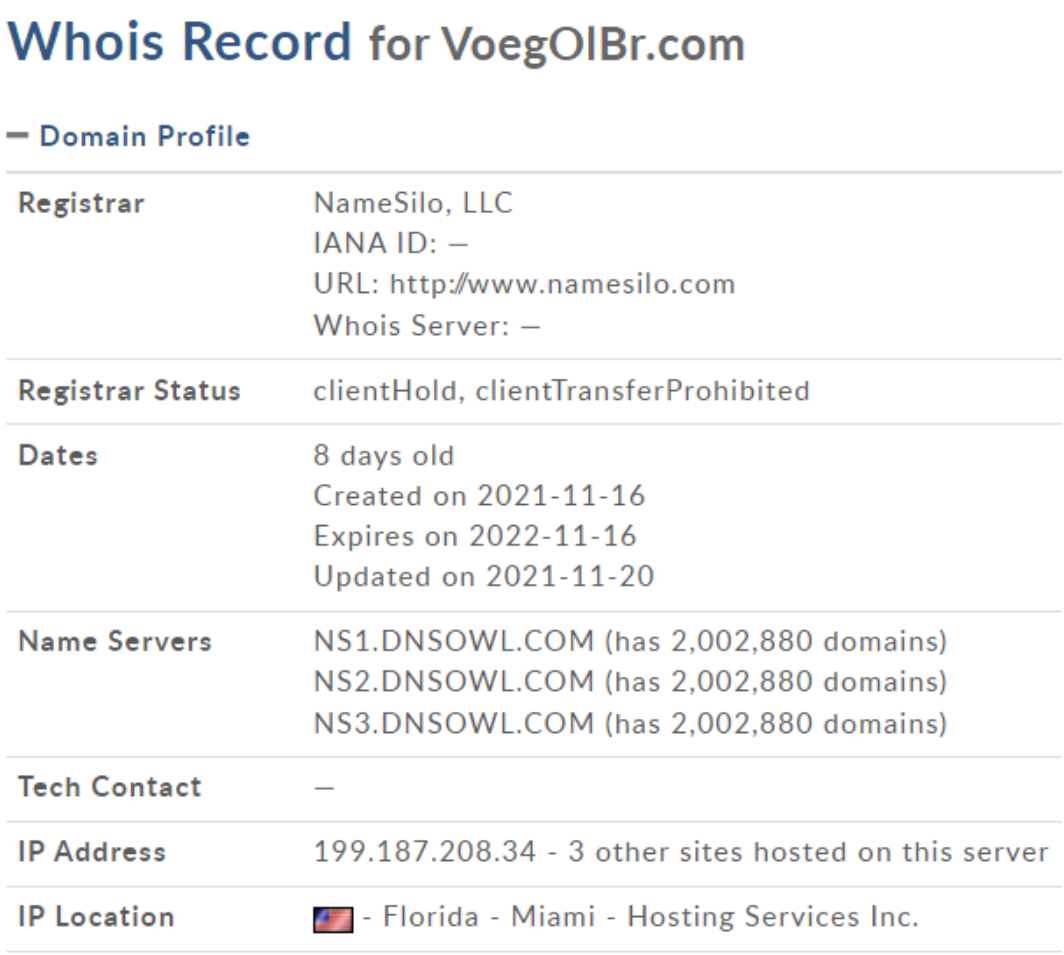
Fonte: Captura de tela. Acervo próprio, 2021.

A Figura 20, mostra o *site* pedindo para que a promoção seja compartilhada com outras 10 pessoas no Whatsapp para validar as passagens que serão dadas, mas mesmo completando os 10 compartilhamentos, o *site* continua pedindo mais compartilhamentos, infinitamente.

O domínio não tem final .br, então foi preciso usar a ferramenta *Whois* em um *site* estrangeiro[51]. A Figura 21 mostra o resultado da pesquisa.

[51] Disponível em: https://whois.domaintools.com/voegolbr.com. Acesso em: 23 nov. 2021.

Figura 21 - Resultado da busca *Whois* sobre o *site* voegolbr.com.



Whois Record for VoegOlBr.com

— Domain Profile

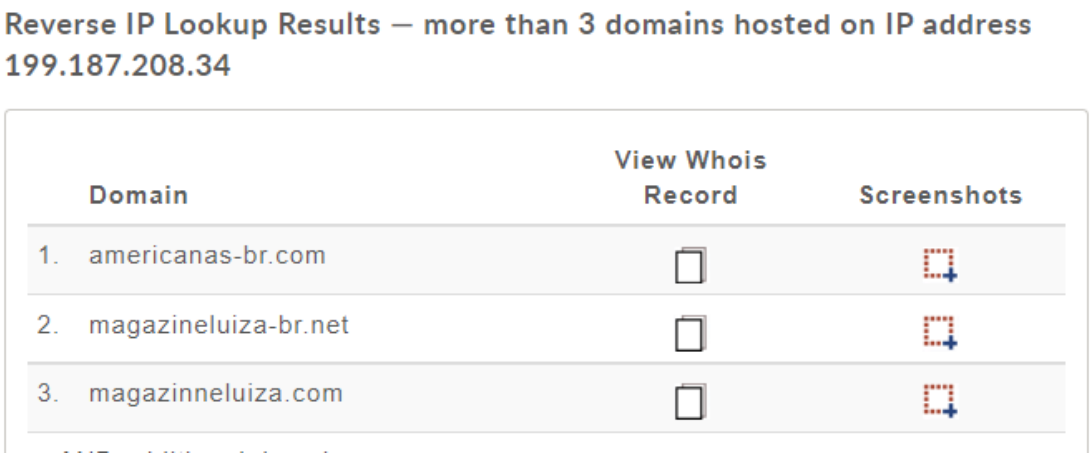
Registrar	NameSilo, LLC IANA ID: — URL: http://www.namesilo.com Whois Server: —
Registrar Status	clientHold, clientTransferProhibited
Dates	8 days old Created on 2021-11-16 Expires on 2022-11-16 Updated on 2021-11-20
Name Servers	NS1.DNSOWL.COM (has 2,002,880 domains) NS2.DNSOWL.COM (has 2,002,880 domains) NS3.DNSOWL.COM (has 2,002,880 domains)
Tech Contact	—
IP Address	199.187.208.34 - 3 other sites hosted on this server
IP Location	- Florida - Miami - Hosting Services Inc.

Fonte: Captura de tela. Acervo próprio, 2021.

É possível ver que o *site* está hospedado em Miami, nos EUA. Não possui informações de quem o registrou e ainda existem outros 3 *sites* relacionados ao IP que esse *site* responde. Com este trabalho, foi possível verificar[52] quais *sites* eram, e assim analisar que os endereços desses *sites* tentam imitar o nome de outras lojas *online*, trocando apenas algumas letras de lugar no endereço, seguindo um padrão. Como pode ser observado na Figura 22.

[52] Disponível em: https://reverseip.domaintools.com/search/?q=voegolbr.com. Acesso em: 23 nov. 2021.

Figura 22 - *Sites* relacionados com o IP do *site* voegolbr.com



Fonte: Captura de tela. Acervo próprio, 2021.

A Gol agora avisa em seu *site* oficial sobre uma possível tentativa de golpe que está ocorrendo e para que as pessoas fiquem atentas (Figura 23).

Figura 23 - *Site* oficial da companhia aérea Gol avisando sobre possível golpe acontecendo em seu nome.

Fonte: Captura de tela. Acervo próprio, 2021.

É preciso bastante atenção à golpes desse tipo, pois, são elaborados com a intenção de parecer o mais verdadeiro possível. Por esta razão é preciso sempre desconfiar de promoções que prometem coisas incomuns, como passagens aéreas gratuitas, pois são produtos de preço elevado.

3.3 COMO DETECTAR *FAKE NEWS*

Com algumas verificações é possível detectar a tendência de uma notícia ser verídica ou não. Como por exemplo:

3.3.1 Quem

Buscar informações de quem escreveu aquilo que se está lendo; verificar o nome do autor, suas qualificações, profissão e outros artigos escritos por ele; verificar se o autor é um especialista na área e se o autor trabalha em uma organização respeitável.

Verificar a seção "Sobre nós". Na parte superior ou inferior do *site*, deve haver uma seção chamada "Sobre nós". Esta seção descreve o objetivo do *site*; verificar se a organização possui uma equipe autorizada de jornalistas ou escritores ou se eles convidam membros do público em geral para contribuir.

3.3.2 O que

Analisar se o artigo informa sobre todos os lados do assunto, pois, os artigos de notícias devem fornecer fatos a partir de vários pontos de vista. Se o artigo mostrar apenas um lado do argumento, os leitores devem ter em mente que eles não estão vendo a história completa e o artigo pode conter parcialidade. Também verificar as fontes citadas no artigo que apoiam as afirmações da história e, se possível, procurar as fontes *online*. Checar se são fontes confiáveis e se elas apoiam as afirmações feitas.

O conteúdo deve corresponder ao título do artigo, pois, o título deve fornecer uma ideia do que trata todo o artigo, mas também pode ser usado para persuadir a acreditar em algo antes de ler o artigo. Os autores podem usar isso a seu favor e falsificar suas manchetes para fazer as pessoas lerem o artigo completo ou

acreditarem na afirmação sem ler o artigo. Além do título, verificar se há erros ortográficos ou gramaticais no texto. Artigos bem pesquisados são normalmente lidos e relidos antes de serem postados.

3.3.3 Quando

Observar quando o artigo foi publicado, pois, artigos mais antigos podem não conter fatos atualizados e podem ter *links* quebrados. Indivíduos que compartilham um artigo mais antigo podem descobrir que algumas informações foram refutadas ou desmascaradas. O conteúdo reaproveitado ou atualizado tende a ter uma isenção de responsabilidade no início ou no final do artigo. Organizações de notícias podem redirecionar um artigo se um evento atual for relacionado.

A data também é importante, pois fornece uma indicação de quando o artigo foi publicado. Os *sites* podem mostrar carimbos de hora e data no artigo, mas é possível que eles possam ser modificados. É interessante fazer uma pesquisa para ver se há artigos semelhantes escritos por outras organizações de notícias.

3.3.4 Onde

Verificar se o endereço da *web* (URL) parece correto. Digitar o endereço da *web* incorreto direcionará o leitor para uma página da *web* que não pretendia visitar. Isso pode levar o leitor a uma página com vírus de computador. É preciso ter cuidado com URLs de *sites* que parecem oficiais ou reais. Um *site* de aparência chamativa pode conter notícias falsas. Semelhante a um número de telefone, um pequeno erro pode levar a um *site* completamente diferente. Com poucas exceções, as URLs, incluindo seus domínios (.com.br, .com, etc.), podem ser adquiridos por qualquer pessoa. Muitos domínios não exigem registro completos ou verificam documentos para garantir a autenticidade do cadastro. Alguns indivíduos enganam os usuários usando nomes de domínio para imitar o *site* oficial de uma organização. Quando não se sabe a URL, pode se usar um mecanismo de busca e analisar os resultados para o resultado que estiver procurando.

As plataformas de mídia social não são organizações de notícias. Estas são plataformas para as pessoas criarem e/ou compartilharem conteúdo. Até pouquíssimo tempo atrás, o monitoramento de notícias falsas era virtualmente inexistente em

plataformas de mídia social e blogs. Hoje já existem algoritmos que verificam se determinados *posts* contém *fake news* ou não. É preciso ter cuidado com vídeos e fotos, pois as imagens podem ter sido manipuladas. Embora os *softwares* de edição de foto e vídeo permitam que cineastas e artistas criem ambientes realistas, estes *softwares* também fornece a qualquer pessoa as mesmas ferramentas para manipular uma imagem ou vídeo para caber em sua história. Deve-se usar a pesquisa reversa de imagens do Google para ver onde mais uma imagem apareceu.

Os *blogs* contêm conteúdo escrito informalmente e administrado por um indivíduo ou um pequeno grupo. Qualquer pessoa pode se registrar em um *blog* ou criar um *site*. *Sites* e blogs podem usar manchetes sensacionais para despertar o interesse do leitor. Os indivíduos podem gerar receita de publicidade a partir de visualizações de páginas. Eles podem escrever artigos de um determinado ponto de vista para públicos-alvo específicos. Deve-se ter cuidado com *sites* que usam linguagem forte para gerar um clique ou reação.

Verificar as informações que foram encontradas usando outro *site*. Deve-se encontrar a fonte original das informações. Estar ciente de que as pessoas podem postar suas notícias falsas em um *site* semelhante. Jornais e noticiários sérios contratam repórteres e jornalistas para reunir e relatar as notícias. Essas organizações de notícias aderem a políticas e normas rígidas

O *site* The International Federation of Library Associations and Institutions (IFLA)[53] criou um infográfico que auxilia na identificação de uma notícia falsa seguindo os passos apresentados na Figura 24:

[53] O IFLA se apresenta como o principal organismo internacional que representa os interesses de serviços de biblioteca e informação e seus usuários. É a voz global da biblioteca e da profissão de informação.

Figura 24 - Infográfico de como identificar notícias falsas

Fonte: The International Federation of Library Associations and Institutions (IFLA)[54].

[54] Disponível em: https://www.ifla.org/publications/node/11174.

3.3.5 Exemplos

A iniciativa de checar se determinada notícia é falsa ou não depende, principalmente, do interesse do leitor, pois esta ação demanda uma avaliação mais criteriosa do que apenas olhar rapidamente a chamada da notícia.

Pessoas com maior letramento informacional, mais conhecimento técnico e com leitura mais crítica, possuem maior potencial em reconhecer uma *fake news* mais rapidamente do que as pessoas que não são assim.

Neste trabalho foi analisado um grupo público[55] do Facebook, chamado “Eu Amo os Animais - Memes e Notícias[56]”, com 91,7 mil membros. Foi possível notar um comportamento diferente pelo descrito nas informações sobre o grupo, que dizem: “Postaremos aqui no grupo imagens, fotos, notícias e vídeos de animais que amamos; também mostraremos a felicidade que os animais nos passam”. Neste trabalho foram analisados os primeiros 50 *posts* da página, com o seguinte resultado: 35 eram *posts* sobre *fake news,* 14 eram *posts* com imagens caça-*likes*[57] e apenas 1 era *post* sobre animais.

Foi possível analisar e verificar através desse trabalho que as publicações nesse grupo seguem alguns padrões. Os *posts* caça-*likes* geralmente trazem mensagens pedindo para curtir e comentar a foto publicada ou com dizeres sobre ser o aniversário da pessoa apresentada na foto e pedir felicitações e curtidas. Isso gera engajamento[58] na publicação e faz com que ela apareça para mais pessoas. A Figura 25 mostra esses dois exemplos, sendo a primeira foto de um grupo de trabalhadores uniformizados e a segunda foto uma bebê.

[55] Grupo público: qualquer pessoa dentro ou fora do Facebook pode ver quem está no grupo e as publicações dos membros.

[56] Disponível em: https://web.facebook.com/groups/385123742117027/. Acesso em: 22 nov. 2021.

[57] Facebook declara guerra às postagens “caça-likes”. Disponível em: https://super.abril.com.br/tecnologia/facebook-declara-guerra-as-postagens-caca-likes/. Acesso em: 21 nov. 2021.

[58] O que é engajamento no Facebook? Disponível em: https://tecnoblog.net/403137/o-que-e-engajamento-no-facebook/. Acesso em: 22 nov. 2021.

Figura 25 - Publicações do tipo caça-*likes* no grupo sobre animais.

Fonte: Colagem de capturas de tela. Acervo próprio, 2021.

O Google possui uma ferramenta de pesquisa de imagem que permite verificar em quais *sites* determinada imagem já esteve hospedada. Neste trabalho foi usada esta ferramenta e, assim, foi possível descobrir que a foto do segundo *post* se trata de uma bebê nascida com microcefalia resultante da gestação de uma mãe que foi infectada pelo Zika vírus, como é possível verificar na Figura 26.

Figura 26 - Pesquisa de imagem no Google mostrando a origem da imagem utilizada como caça-*likes*.

Fonte: Captura de tela. Acervo próprio, 2021.

O uso de imagens retiradas de qualquer lugar aleatório da Internet torna muito mais fácil o trabalho de quem está criando este tipo de conteúdo enganoso. Nem sempre é possível rastrear a imagem através do Google, mas é importante fazer o teste. Na Figura 27 é possível ver outro exemplo[59] de caça-*likes,* com a imagem de uma idosa, possivelmente hospitalizada com a mensagem de que ficaria feliz por ser parabenizada por seu aniversário. O *post* original foi feito pelo perfil de um homem, de nome Leandro Conceição. Neste trabalho foi utilizada novamente a ferramenta de pesquisa de imagem do Google para analisar a imagem do *post,* revelando, como mostrado na Figura 28, que esta imagem teve sua origem em uma matéria do *site* G1[60].

[59] Disponível em: https://web.facebook.com/groups/385123742117027/posts/1073593203270074. Acesso em: 22 nov. 2021.

[60] Disponível em: https://g1.globo.com/ms/mato-grosso-do-sul/noticia/2019/02/14/idosa-que-teve-medicacao-trocada-por-paciente-com-mesmo-nome-consegue-vaga-em-hospital-de-ms-aliviada.ghtml. Acesso em: 22 nov. 2021.

Figura 27 - Publicação do tipo caça-*likes* com imagem de idosa em situação de saúde.

Fonte: Captura de tela. Acervo próprio, 2021.

Figura 28 - Pesquisa de imagem no Google mostrando a origem da imagem utilizada como caça-*likes*.

Fonte: Captura de tela. Acervo próprio, 2021.

Já os *posts* de *fake news* são mais sensacionalistas, com títulos chamativos e postados em *sites* duvidosos, com constantes erros de português e informações

faltantes, fora do padrão jornalístico ou científico; não havendo, talvez, nem a necessidade de ser feita toda a checagem para se concluir que se trata de uma notícia falsa. Na Figura 29 é possível ver duas capturas de tela no grupo, sobre duas *fake news* diferentes.

Figura 29 - Postagens de *fake news* no grupo sobre animais.

Fonte: Colagem de capturas de tela. Acervo próprio, 2021.

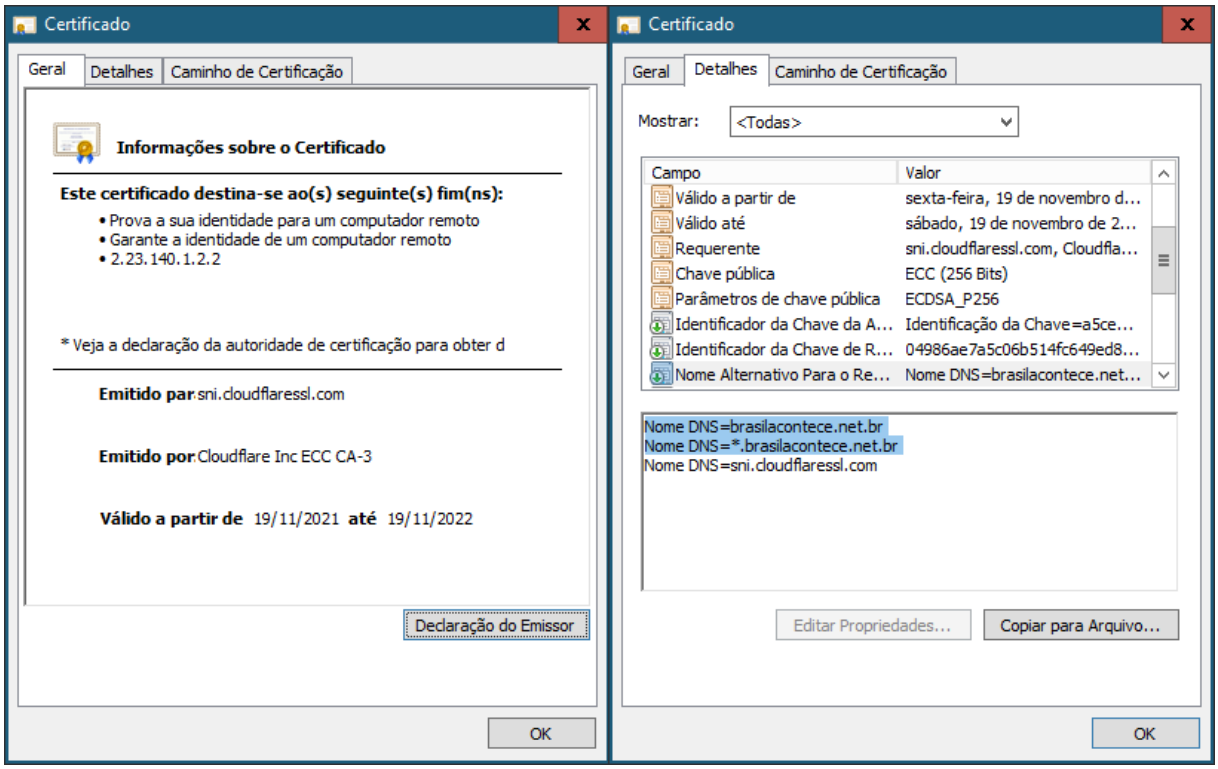
Ao abrir o *link*[61], o *site* carregado lembra muito um *blog* baseado na plataforma *Wordpress*, e repleto de propagandas. Possivelmente o intuito do *site* é justamente reunir visualizações para estas propagandas vindas de curiosos que clicaram no *link* para ler a publicação sensacionalista por completo. O *site* não passa confiança alguma.

Apesar da navegação estar sendo feita de forma segura (HTTPS), isso não significa que a página em si seja confiável e segura. Foi verificado neste trabalho que

[61] Disponível em: https://brasilacontece.net.br/luto-no-masterchef-acaba-de-chegar-as-pressas-triste-noticia-sobre-jacquin-aos-56-anos-descanse-em-paz/. Acesso em: 22 nov. 2021.

o certificado da página está ativo e assinado por uma Autoridade Certificadora reconhecida e, por isso, considerado como válido (Figura 30).

Figura 30 - Certificado HTTPS válido para o *site* brasilacontece.net.br



Fonte: Captura de tela. Acervo próprio, 2021.

Através da ferramenta *Whois* é possível verificar quem registrou determinado domínio. Neste trabalho foi verificado que o domínio brasilacontece.net.br tem seu registro no Brasil, então é possível fazer a verificação diretamente pelo *site* Registro.br. Através da ferramenta foi possível descobrir que o domínio foi registrado em 16 de abril de 2019, por uma pessoa chamada Ingrid Drews Peres, tendo seu DNS localizado nos servidores da empresa Cloudflare e a hospedagem com a empresa Godaddy, e também o *e-mail* do responsável pelo registro. Como mostra a Figura 31.

Figura 31 - Resultado da ferramenta Whois sobre o domínio do *site* de *fake news*.

Domínio **brasilacontece.net.br**

TITULAR	Ingrid Drews peres
DOCUMENTO	565.783.858-00
PAÍS	BR
CONTATO DO TITULAR	INDPE3
CONTATO TÉCNICO	INDPE4
SERVIDOR DNS	aurora.ns.cloudflare.com
SERVIDOR DNS	reese.ns.cloudflare.com
SACI	Sim
CRIADO	16/04/2019 #19549908
EXPIRAÇÃO	16/04/2022
ALTERADO	27/03/2021
PROVEDOR	GODADDY (86)
STATUS	Publicado

Contato (ID) **INDPE3**

NOME	Ingrid Drews peres
EMAIL	fcamarques1313@gmail.com
PAÍS	BR
CRIADO	16/04/2019
ALTERADO	16/04/2019
PROVEDOR	GODADDY (86)

Fonte: Captura de tela. Acervo próprio, 2021.

Mesmo com estas informações, mostrando o *site* devidamente registrado e operante, não é possível ter certeza de que a pessoa que o registrou é realmente quem consta no registro *Whois*. E ainda que este *site,* aparentemente, tente apenas coletar acessos para gerar monetização nas propagandas inseridas nele, ainda poderia carregar consigo malwares e infectar quem o acesse.

3.4 COMO COMBATER *FAKE NEWS*

O combate às *fake news* precisa ser efetivo, bem direcionado e constante. Como em uma espécie de batalha que envolve muito mais do que apenas soluções simples e rápidas para que funcione. São necessárias estratégias bem elaboradas e o uso de todos os recursos possíveis para obter-se um resultado de excelência.

Assim que as *fake news* começaram a se tornar um problema de maior escala, foram surgindo, paralelamente, métodos para as combater. Esses métodos vem sendo aprimorados com o tempo, ajudando a sociedade no enfrentamento das *fake news* e direcionamento para as informações verdadeiras de fato.

O foco das *fake news* são sempre pessoas, que consumirão seu conteúdo e executarão ações a partir disso. A criação delas também parte de pessoas, pois, não são máquinas criando informações falsas sem contexto algum. A inteligência artificial ainda está atualmente num patamar do qual depende de muito aprendizado para criar contextos críveis iguais aos de uma pessoa, além de que isto demandaria custo e tempo. O criador de conteúdo falso precisa ter entendimento do cenário atual da sociedade ao qual está inserido para se usar de referência e criar notícias atrativas, que possam ser espalhadas mais facilmente e cridas sem muito critério, de forma parecida como faz um engenheiro social, que estuda seu alvo.

Além do letramento informacional, é preciso trabalhar em conjunto com ferramentas, novas ideias e envolver também pessoas nessa luta, criando uma espécie de malha comunitária que conecta pessoas com o mesmo objetivo de trazer à luz a verdade sobre os fatos como ela realmente é.

3.4.1 Agências verificadoras

Mesmo antes da popularização das *fake news*, existiam *sites* que verificavam boatos e farsas espalhadas na Internet. O *site* E-farsas[62] é um dos mais antigos nessa categoria no Brasil, fundado em 2002 e ativo até o momento. Hoje continua atuando também como portal para checagem de *fake news*.

[62] Disponível em: https://www.e-farsas.com/sobre. Acesso em: 22 nov. 2021.

Após a popularização das *fake news,* surgiram portais *online* dedicados em fazer *fact checking*[63] (checagem de fatos) em informações que viralizavam na Internet, a fim de descobrir se de fato se tratava de notícias falsas ou não. Esses portais são chamados de Agências de Checagem ou Agências Verificadoras de Fatos.

No Brasil as principais agências são a Agência Lupa[64], Aos Fatos[65], Fato ou Fake[66] e Comprova[67]. Também existe o Estadão Verifica[68] que se classifica como núcleo de checagem de fatos do jornal O Estado de São Paulo.

Todas essas agências possuem equipes sérias, responsáveis pela pesquisa e elucidação dos fatos, o que demanda bastante trabalho. Essas agências servem como mecanismos de defesa para os cidadão no combate às *fake news* trazendo acesso à verdade e aos fatos.

3.4.2 Projeto de Lei das *Fake News*

Em maio de 2020 foi aprovado no Senado brasileiro o Projeto de Lei 2630/20, também conhecido como PL das *Fake news*, de autoria do Senador Alessandro Vieira (CIDADANIA/SE) e, que se sancionado pelo presidente, criará a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet.

O projeto propõe regras para os principais provedores de redes sociais, como Facebook e Instagram, e serviços de mensageria instantânea, como WhatsApp e Telegram. Segundo o relator do projeto[69], o deputado Orlando Silva (PCdoB-SP), é nítido que o serviço de mensagem tem mais funcionalidades além da qual foi inicialmente criado, como disparos em massa, criando a viralização de determinadas notícias.

Em sua última atualização[70], em novembro de 2021, o relator do projeto estendeu ainda a aplicação da lei para ferramentas de busca, como Google e Yahoo.

---

[63] Disponível em: https://guiadoestudante.abril.com.br/estudo/fact-checking-conheca-5-agencias-de-checagem-de-noticias/. Acesso em: 22 nov. 2021.

[64] Disponível em: http://www.lupa.news/

[65] Disponível em: https://www.aosfatos.org/

[66] Disponível em: https://g1.globo.com/fato-ou-fake/

[67] Disponível em: https://projetocomprova.com.br/

[68] Disponível em: https://politica.estadao.com.br/blogs/estadao-verifica/

[69] Disponível em: https://pcdob.org.br/noticias/grupo-de-trabalho-adia-analise-do-relatorio-do-pl-das-fake-news/. Acesso em: 20 nov. 2021.

[70] Disponível em: https://www.camara.leg.br/noticias/823776-veja-as-principais-mudancas-feitas-pelo-relator-do-projeto-de-lei-das-fake-news/. Acesso em: 20 nov. 2021.

O relator excluiu do texto alguns artigos polêmicos, existentes na primeira versão do projeto, que poderiam possibilitar o rastreamento de usuários como o que previa a guarda, por três meses, dos registros de mensagens em encaminhamentos em massa e o que possibilitava às empresas requererem documento de identidade dos responsáveis pelas contas, em caso de denúncias de desrespeito à lei. Também possibilitou a criação de um novo crime, que trata sobre promover ou financiar disparo em massa de mensagens falsas com o uso de contas automatizadas (robôs), sendo a pena proposta de 1 a 5 anos e multa.

A Lei das *fake news* ainda está passando por adaptações e atualizações. O intuito é proteger cada vez mais os cidadãos e tentar impedir qualquer interferência na democracia brasileira, evitando assim a impunidade caso aconteçam casos como o escândalo da Cambridge Analytica no Brasil.

3.4.3 O papel do profissional de Segurança da Informação

O profissional de Segurança da Informação tem a capacidade e conhecimento necessários para auxiliar no combate às *fake news,* sendo esse amplamente capacitado para criar novas ferramentas dentro da área de computação, além de poder lidar com as ferramentas já existentes no mercado, as direcionando para este fim.

Mesmo que a inteligência artificial não seja usada para a criação de *fake news* em algumas situações, ela pode ser usada pelo profissional de Segurança da Informação como um meio na identificação de *fake news* nas redes. Dentro do ramo de inteligência artificial, existe o *machine learning*[71] (aprendizado de máquina), que é um método de análise de dados e automatização da construção de modelos analíticos, baseando-se na ideia de que sistemas podem aprender com dados, identificar padrões e tomar decisões com o mínimo de intervenção humana.

Dentro do contexto do *machine learning* existe o *data mining* (mineração de dados) que consiste em utilizar grandes bases de dados para trazer percepções sobre comportamentos que se repetem de maneira consistente. Com o *data mining* é

[71] Disponível em: https://www.ibm.com/br-pt/analytics/machine-learning. Acesso em: 10 dez 2021.

possível reunir grandes quantidades de dados para se usar a Ciência de Dados[72] com Análise Preditiva[73] e aplicar estatística para prever comportamentos futuros individuais a partir de padrões.

Um exemplo de ferramenta neste formato é o *Bot Sentinel*[74], criado em 2018 por Christopher Bouzy para ajudar a combater a desinformação dentro do Twitter. O *Bot Sentinel* classifica contas do Twitter inautênticas chamadas de *bots*[75], responsáveis, também, por disseminar todo tipo de informação falsa, e as adiciona a um banco de dados disponível publicamente, no qual qualquer pessoa pode navegar. Ele utiliza *machine learning* para funcionar com base nas regras do Twitter como um guia ao selecionar contas do Twitter para treinar seu modelo. Segundo informações do *site* do projeto, o sistema pode classificar corretamente as contas com uma precisão de 95%.

Desta forma, o profissional de Segurança da Informação pode trabalhar também no desenvolvimento de novos algoritmos de detecção de *fake news* se baseando em comportamento do usuário e padrões dentro das redes e também na melhoria de algoritmos já existentes. Assim, ajudando a educar e informar o usuário não letrado informacionalmente sem esbarrar em questões políticas e jurídicas (como discussões sobre liberdade de expressão[76]).

Futuramente, com a computação quântica, essas análises poderão ser ainda mais rápidas, podendo auxiliar no combate às *fake news* antes mesmo delas se espalharem na rede como acontece hoje.

---

[72] Ciência de Dados é uma área interdisciplinar que reúne estatística e ciência da computação.

[73] Disponível em: https://www.ibm.com/br-pt/analytics/predictive-analytics. Acesso em: 10 dez 2021.

[74] Disponível em: https://botsentinel.com/.

[75] Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-are-bots. Acesso em: 10 dez 2021.

[76] Disponível em: https://www.oabes.org.br/artigos/as-fake-news-e-a-liberdade-de-expressao-a-democracia-geme-76.html. Acesso em: 10 dez 2021.

4 CONCLUSÕES

Desde o começo das civilizações, o ser humano teve a necessidade, o anseio, de se comunicar. O instinto de sobrevivência humano faz com que mensagens sejam repassadas para seus iguais no intuito de ajudar e informar o próximo. A confiança também é uma peça do instinto humano de sobrevivência, sempre explorada e usada, como conta a história.

Com a evolução humana e suas tecnologias, os meios de se transmitir mensagens também evoluiu, fazendo com que a comunicação se tornasse muito mais complexa, mas também muito mais inclusiva. Na mesma proporção, evoluíram as formas de se conseguir tirar vantagens da própria espécie, seja por intenções de ganhos próprios, ganhos para outrem ou, ainda, apenas por falta de caráter.

Por meio desse trabalho, foi possível analisar a origem do surgimento das primeiras formas de comunicação humana até onde chegou sua evolução na atualidade. Foi possível ainda entender como se comportam as pessoas que ficam na busca por brechas da "máquina" humana para tirar vantagens (os engenheiros sociais) e também entender suas vítimas, que são alvos fáceis quando não se policiam em atitudes básicas do dia a dia.

Ainda, este trabalho tentou elucidar o que é o letramento informacional e porque sua falta pode ser a principal porta de entrada para que pessoas sejam vítimas de *fake news*. Também permitiu o entendimento detalhado sobre como as *fake news* funcionam*,* sua difusão e capacidade de destruição, podendo resultar em morte (de diversas formas), ou agravamento de crises sanitárias de países inteiros. Também foi possível notar a uma polarização política em países que afetaram a confiança da população nos veículos de notícias, desacreditando muitas pessoas sobre a verdade e os fatos; dando voz para o "achismo" e teorias mirabolantes sem respaldo científico algum.

Através do estudo realizado neste trabalho concluiu-se que a melhor forma de combate às *fake news* deve ser feito através do conhecimento, da educação. Com a evolução da tecnologia, principalmente nas áreas de inteligência artificial e *machine learning,* é possível para os profissionais de Segurança da Informação disporem de conhecimentos avançados para desenvolver ferramentas próprias de análise para a detecção de *fake news* e redirecionamento educativo. Este trabalho tem a intenção

de demonstrar o efeito negativo das *fake news* e instigar a conscientização sobre a identificação e a não disseminação de informações falsas ou duvidosas. Para o futuro, existe a proposta de que novos profissionais da área de Tecnologia da Informação se interessem mais por este tema e analisem as melhores ferramentas no mercado para identificação de *fake news* e averiguem melhorias em seus sistemas e criem novos tipos de sistemas de identificação de *fake news* baseados em inteligência artificial.

Como objetivo principal deste estudo, foram analisadas diversas referências de obras acadêmicas relacionadas e concluído que as campanhas informativas em todos os meios possíveis de comunicação são as principais “armas” no combate às *fake News*, incluindo também a comunicação pessoal entre indivíduos, que pode exigir um maior esforço das pessoas, mas que terá validado o trabalho. O combate às *fake news* deve ser constante e depende de cada cidadão, cada unidade de cultura da sociedade, para que no futuro as *fake news* sejam lembradas como algo do passado, uma fase da humanidade que foi superada; apenas mais um assunto estudado nos livros de história.

5 REFERÊNCIAS

ABASS, Islam Abdalla Mohamed, Social Engineering Threat and Defense: A Literature Survey, **Journal of Information Security**, v. 09, n. 04, p. 257–264, 2018.

ALTARES, Guillermo. **A longa história das notícias falsas**: Utilização política das mentiras começou muito antes das redes sociais, e a construção de outras realidades era uma constante na Grécia antiga. [*S. l.*], 18 jun. 2018. Disponível em: https://brasil.elpais.com/brasil/2018/06/08/cultura/1528467298_389944.html. Acesso em: 20 nov. 2021.

BERNARDI, Ana Julia Bonzanini. **Redes sociais, *fake news* e eleições**: medidas para diminuir a desinformação nos pleitos eleitorais brasileiros. 2019. Disponível em: https://lume.ufrgs.br/handle/10183/197602. Acesso em: 25 mar. 2021.

BRASIL, CNN. Golpe do cartão de crédito por telefone usa até música que imita call center: Idosos são os principais alvos das quadrilhas que aplicam esses golpes. **CNN Brasil**, [*S. l.*], 18 set. 2021. Disponível em: https://www.cnnbrasil.com.br/business/golpe-do-motoboy-cresce-na-pandemia-e-usa-ate-musica-que-imita-call-center/. Acesso em: 18 nov. 2021.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach: Whistleblower describes how firm *link*ed to former Trump adviser Steve Bannon compiled user data to target American voters. **The Guardian**, UK, 17 mar. 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: 6 nov. 2021.

CAMBRIDGE Analytica whistleblower: 'We spent $1m harvesting millions of Facebook profiles'. [S.l.]: The Guardian, 2018. (13 min.), color. Legendado. Disponível em: https://www.youtube.com/watch?v=FXdYSQ6nu-M&ab_channel=TheGuardian. Acesso em: 07 nov. 2021.

CAMBRIDGE, University of. **The Psychometrics Centre: myPersonality database**. 2021. Disponível em: https://www.psychometrics.cam.ac.uk/productsservices/mypersonality. Acesso em: 02 nov. 2021.

CARPANEZ, Juliana. **Veja o passo a passo da notícia falsa que acabou em tragédia em Guarujá**. [*S. l.*], 27 set. 2018. Disponível em: https://www1.folha.uol.com.br/cotidiano/2018/09/veja-o-passo-a-passo-da-noticia-falsa-que-acabou-em-tragedia-em-guaruja.shtml. Acesso em: 23 nov. 2021.

CERTNZ. **Christchurch tragedy-related scams and attacks**. 2019. Disponível em: https://www.cert.govt.nz/individuals/alerts/christchurch-tragedy-related-scams-and-attacks/. Acesso em: 02 nov. 2021.

COELHO, Cristiano Farias; RASMA, Eline Tourinho; MORALES, Gudelia, ENGENHARIA SOCIAL: UMA AMEAÇA À SOCIEDADE DA INFORMAÇÃO, **Exatas & Engenharias**, v. 3, n. 05, 2013.

Coelho, C. F., Rasma, E. T., & Morales, G. (2013). ENGENHARIA SOCIAL: UMA AMEAÇA À SOCIEDADE DA INFORMAÇÃO. *Exatas & Engenharias*, *3*(05). https://doi.org/10.25242/885X305201387

CURTIS, Sophie. **How hackers took over my computer**: we hear about hacking every day - but are individuals really vulnerable? Sophie Curtis volunteered to find out. 2014. Disponível em: https://www.telegraph.co.uk/technology/Internet-security/11153381/How-hackers-took-over-my-computer.html. Acesso em: 05 nov. 2021.

ESTABEL, Lizandra Brasil; LUCE, Bruno Fortes; SANTINI, Luciane Alves. Idosos, fake news e letramento informacional. **Revista Brasileira de Biblioteconomia e Documentação**, São Paulo, v. 16, p. 1-15, 2020. Disponível em: https://lume.ufrgs.br/handle/10183/218275. Acesso em: 10 dez. 2021.

FAUSTINO, André. ***FAKE NEWS***: a liberdade de expressão nas redes sociais na sociedade da informação. São Caetano do Sul: Lura Editorial, 2019. 188 p.

GASQUE, Kelley Cristine Gonçalves Dias. Arcabouço conceitual do letramento informacional. **Ciência da Informação**, Brasília, DF, v.39, n.3, p. 83-92, set./dez., 2010. Disponível em: http://www.scielo.br/pdf/ci/v39n3/v39n3a07.pdf. Acesso em: 25 out. 2021.

HANCOCK, Jaime Rubio. **Dicionário Oxford dedica sua palavra do ano, 'pós-verdade', a Trump e Brexit**: no debate político, o importante não é a verdade, mas ganhar a discussão. No debate político, o importante não é a verdade, mas ganhar a discussão. 2016. Disponível em: https://brasil.elpais.com/brasil/2016/11/16/internacional/1479308638_931299.html. Acesso em: 08 jun. 2021.

IBGE. **Pesquisa mostra que 82,7% dos domicílios brasileiros têm acesso à Internet**. 2021. Disponível em: https://www.gov.br/mcom/pt-br/noticias/2021/abril/pesquisa-mostra-que-82-7-dos-domicilios-brasileiros-tem-acesso-a-Internet. Acesso em: 20 out. 2021.

IBGE. **Uso de Internet, televisão e celular no brasil**. 2020. Disponível em: https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-Internet-televisao-e-celular-no-brasil.html. Acesso em: 20 out. 2021.

IMPRENSA. In: MICHAELIS, Dicionário Brasileiro da Língua Portuguesa. UOL, 2021. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/imprensa/. Acesso em: 07 maio 2021.

INCLUSÃO DIGITAL. In: MICHAELIS, Dicionário Brasileiro da Língua Portuguesa. UOL, 2021. Disponível em: https://michaelis.uol.com.br/busca?id=7mp9e. Acesso em: 08 maio 2021.

KLEIMAN, Angela B. **Preciso "ensinar" o letramento? Não basta ensinar a ler e a escrever?** Campinas: Editora da Unicamp, 2005.

LAIGNIER, Pablo; FORTES, Rafael (org.). **Introdução à História da Comunicação**. Rio de Janeiro: E-Papers, 2009. 134 p.

LAPOWSKY, Issie. The Man Who Saw the Dangers of Cambridge Analytica Years Ago: Researchers at the Psychometrics Centre knew better than most how Facebook data can be manipulated, but investigations and suspensions have halted their work. **Wired**, [*S. l.*], 19 jun. 2018. Disponível em: https://www.wired.com/story/the-man-who-saw-the-dangers-of-cambridge-analytica/. Acesso em: 5 nov. 2021.

LIMA, Pablo de Andrades *et al*, Estudo sobre *Fake news*: modo de operação e como atenuar a sua propagação, **Anais da Escola Regional de Redes de Computadores (ERRC)**, p. 198–199, 2019.

LUCE, Bruno Fortes; ESTABEL, Lizandra Brasil, LETRAMENTO INFORMACIONAL E MÍDIAS SOCIAIS:, **Revista Brasileira de Pós-Graduação**, v. 16, n. 35, p. 1–14, 2020.

MARANHÃO, S. M.; CARVALHO, G. A.; SILVA, G. J. Letramento informacional: uma modalidade de ascensão social. **Múltiplos Olhares em Ciência da Informação**, v. 3, n. 2, 2013. Disponível em: http://hdl.handle.net/20.500.11959/brapci/70526. Acesso em: 13 dez. 2021.

MARTINO, Luís Mauro Sá, **Teoria da comunicação: Ideias, conceitos e métodos**, 4. ed. Rio de Janeiro: Editora Vozes, 2009, p.23.

MARTINO, Luiz C. **Teorias da Comunicação: Conceitos, escolas e tendências**. Petrópolis: Vozes, 2010.

MARTINS, Thiago Souza. Introdução à LGPD: o caso Cambridge Analytica. **Jusbrasil**, [*S. l.*], p. 1, 20 ago. 2019. Disponível em: https://tico080970.jusbrasil.com.br/artigos/745956107/introducao-a-lgpd-o-caso-cambridge-analytica. Acesso em: 7 nov. 2021.

OLIVEIRA, Joana. **Bolsonaro é "líder e porta-voz" das '*fake news*' no país, diz relatório final da CPI da Pandemia**. [*S. l.*], 20 out. 2021. Disponível em: https://brasil.elpais.com/brasil/2021-10-20/bolsonaro-e-lider-e-porta-voz-das-fake-news-no-pais-diz-relatorio-final-da-cpi-da-pandemia.html. Acesso em: 23 nov. 2021.

PI, Privacy Internacional. **Cambridge Analytica, GDPR - 1 year on - a lot of words and some action**. [*S. l.*], 30 abr. 2019. Disponível em: https://privacyinternational.org/news-analysis/2857/cambridge-analytica-gdpr-1-year-lot-words-and-some-action. Acesso em: 6 nov. 2021.

PILETTE, Chloe. **What is social engineering? A definition + techniques to watch for**. [*S. l.*], 26 jun. 2021. Disponível em: https://us.norton.com/Internetsecurity-emerging-threats-what-is-social-engineering.html. Acesso em: 17 nov. 2021.

POPULISMO. In: MICHAELIS, Dicionário Brasileiro da Língua Portuguesa. UOL, 2021. Disponível em: https://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=populismo. Acesso em: 08 maio 2021.

PRENSA. In: MICHAELIS, Dicionário Brasileiro da Língua Portuguesa. UOL, 2021. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/prensa. Acesso em: 07/06/2021.

PROTO-HUMANO. In: MICHAELIS, Dicionário Brasileiro da Língua Portuguesa. UOL, 2021. Disponível em: https://michaelis.uol.com.br/busca?id=EZPVX. Acesso em: 31 maio 2021.

SASTRE, Angelo; OLIVEIRA, Claudia Silene Pereira de; BELDA, Francisco Rolfsen, A influência do "filtro bolha" na difusão de *Fake news* nas mídias sociais: reflexões sobre as mudanças nos algoritmos do Facebook, **Revista GEMInIS**, v. 9, n. 1, p. 4–17, 2018.

SECURITY, Mitnick. **6 Types of Social Engineering Attacks**. [*S. l.*], 5 abr. 2021. Disponível em: https://www.mitnicksecurity.com/blog/6-types-of-social-engineering-attacks. Acesso em: 17 nov. 2021.

SPEAR *PHISHING*. In: KASPERSKY, O que é spear *phishing*? Definição e riscos. Kaspersky. 2021. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/spear-*phishing*. Acesso em: 08 junho 2021.

STILLWELL, David; KOSINSKI, Michal; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. **PNAS**, [*s. l.*], v. 110, ed. 15, p. 5802-5805, 9 abr. 2013. DOI 10.1073. Disponível em: https://www.pnas.org/content/110/15/5802. Acesso em: 5 nov. 2021.

TERRA, Portal. **WhatsApp e o Instagram são os aplicativos mais populares no Brasil, diz pesquisa**. 2021. Disponível em: https://www.terra.com.br/noticias/whatsapp-e-o-instagram-sao-os-aplicativos-mais-populares-no-brasil-diz-pesquisa,3170de4e21cb7b5610040eb6e6e5b66de6lzvsrt.html. Acesso em: 20 out. 2021.

TOWNSEND, Kevin. **Engenharia social: não se trata apenas de golpes de phishing**. [*S. l.*], 3 maio 2019. Disponível em: https://blog.avast.com/pt-br/social-engineering-hacks. Acesso em: 17 nov. 2021.

VENTURA, Felipe. Facebook e Instagram vão sinalizar notícias falsas em posts e Stories. [S. l.], 22 out. 2019. Disponível em: https://tecnoblog.net/311651/facebook-instagram-sinalizar-noticias-falsas-posts-stories/. Acesso em: 22 nov. 2021.

VULNERABILIDADE. In: MICHAELIS, Dicionário Brasileiro da Língua Portuguesa. UOL, 2021. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/vulnerabilidade/. Acesso em: 20 out. 2021.

WHITMAN, Michael E.; MATTORD, Herbert J. **Principles of information security**. 4ª ed. Boston: Course Tecnology, 2012. 656 p.

YABRUDE, Angela Theresa Zuffo *et al*, Desafios das *Fake news* com Idosos durante Infodemia sobre Covid-19: Experiência de Estudantes de Medicina, **Revista Brasileira de Educação Médica**, v. 44, 2020.