A aplicação da legislação vigente brasileira nos casos de ataques de engenharia social

Natalia Tatagiba Lima[1*]; Eber Coloni Meira da Silva[2]

[1] Acadêmica do Curso de Direito, Centro Universitário São Lucas Ji-Paraná - JPR, Ji-Paraná, RO, Brasil. E-mail: ntltatagibalima@gmail.com
[2] Docente do Curso de Direito, Centro Universitário São Lucas Ji-Paraná - JPR, Ji-Paraná, RO, Brasil. E-mail: eber_coloni@hotmail.com

1. Introdução

A engenharia social é uma estratégia que visa obter acesso a informações confidenciais por meio de persuasão e manipulação psicológica. Segundo Kevin Mitnick (2003), a engenharia social usa influência e persuasão para enganar as pessoas, fazendo-as acreditar que o engenheiro social é alguém que não é, através de manipulação psicológica.

Caracterizada por técnicas que exploram as fragilidades e falhas humanas, a engenharia social se vale da falta de conscientização e de outras vulnerabilidades para driblar a segurança dos sistemas e dispositivos eletrônicos. Nesse sentido, os ataques de engenharia social não necessitam de tecnologia avançada ou requisitos técnicos complexos, tornando-os ainda mais perigosos.

A legislação brasileira reconhece a gravidade dos crimes relacionados à engenharia social e busca prever penalidades para os infratores. Existem leis específicas que tratam de crimes cibernéticos, como a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, e o Marco Civil da *Internet* (Lei nº 12.965/2014), que estabelecem medidas para combater esses tipos de crimes.

Para combater esses crimes, existem leis em vigor que preveem penalidades para os infratores. No entanto, a aplicação dessas leis ainda é limitada e enfrenta diversos desafios. Neste viés, é necessário saber o posicionamento da legislação brasileira em relação aos crimes de ataques de engenharia social.

Apesar da gravidade do problema, muitas pessoas ainda não conhecem as técnicas de engenharia social e não estão cientes dos riscos associados a essa forma de ataque. Posto isso, é fundamental que a população seja educada e conscientizada sobre os perigos da engenharia social e saiba como se proteger desses ataques.

Diante disto, o presente resumo proposto visa contribuir no combate dos crimes de engenharia social no Brasil, além de ajudar a conscientizar a população sobre a importância da segurança digital e da proteção de dados pessoais e corporativos, bem como no funcionamento da aplicação da legislação vigente brasileira em relação a estes ataques.

2. Materiais e métodos

A metodologia da presente pesquisa tem abordagem qualitativa, haja vista que é desenvolvida a partir de materiais publicados em livros, artigos, dissertações e teses, uma

vez que grande parte do objeto de análise será a legislação vigente que visa a proteção dos dados pessoais.

A coleta dos dados foi realizada por meio da busca e seleção das fontes de pesquisa. A análise dos dados foi realizada por meio da leitura e interpretação das informações contidas nas fontes selecionadas, buscando identificar as principais tendências, pontos de convergência e divergência, e perspectivas futuras para a aplicação da legislação nos casos de engenharia social.

A pesquisa foi conduzida nos idiomas português e inglês, abrangendo diversas fontes, como *sites*, artigos científicos, livros e legislação relacionada ao tema.

Não se aplica informações quanto o tamanho da população, visto que se trata de uma revisão puramente bibliográfica e não envolve o recolhimento de dados populacionais.

3. Resultados e Discussões

A engenharia social é um método de ataque cibernético que explora a vulnerabilidade humana como seu ponto frágil. Segundo LONG (2013), o aspecto humano continua sendo o maior desafio para a segurança da informação nas organizações, uma vez que os usuários podem não aderir às políticas de segurança, tornando o sistema suscetível a ataques de engenharia social.

A engenharia social utiliza psicologia para explorar vieses cognitivos e levar as pessoas a agirem irracionalmente, seguindo os objetivos do engenheiro social. Rodrigo Martins (2014) destaca que o engenheiro social cria uma fachada social para confundir suas potenciais vítimas, usando várias técnicas, como assumir identidades falsas ou simular especialização em um campo específico.

Como os ataques de engenharia social exploram o fator humano, é essencial para os atacantes criar situações em que as vítimas confiem neles e revelem suas vulnerabilidades. Portanto, a tecnologia é apenas um instrumento nesse tipo de ataque, com a pesquisa, planejamento e análise das linguagens corporais e verbais desempenhando um papel crucial, conforme MURAI e RODRIGUES (2021) observam.

A IBM identifica as táticas mais usadas na engenharia social, sendo ações como: se passar por uma marca confiável, se passar por agência governamental ou figura de autoridade, induzir medo ou sensação de urgência, apelar para a ganância e apelar à prestatividade ou curiosidade.

Além do elencado acima, a IBM também lista diversos tipos de engenharia social que envolvem estratégias de persuasão, engano e manipulação para obter acesso não autorizado a informações ou sistemas, além de alguns dos principais tipos de ataques de engenharia social, tais como:

1. ***Phishing*:** É uma técnica que envolve o envio de e-mails bem elaborados com anexos maliciosos ou *links* para enganar as vítimas e obter informações pessoais, como senhas e números de cartão de crédito.
2. ***Tailgating*:** ocorre quando alguém não autorizado se aproveita da confiança dos funcionários de uma organização para entrar em áreas restritas sem autorização.
3. ***Pretexting*:** Envolve a criação de histórias fictícias ou pretextos onde os atacantes assumem papéis de autoridade ou confiança para enganar as vítimas.

4. ***Quid Pro Quo*:** Os atacantes oferecem algo de valor aparente em troca de informações confidenciais, explorando o princípio da reciprocidade.
5. ***Scareware*:** Envolve a criação e disseminação de *software* ou mensagens falsas e alarmantes para assustar as vítimas e levá-las a tomar medidas precipitadas.
6. **Ataque *Watering Hole*:** Os atacantes infectam *sites* frequentemente visitados por um grupo específico de pessoas ou uma organização-alvo, a fim de comprometer dispositivos ou obter informações sensíveis.

A conscientização nestes ataques é fundamental para proteger indivíduos e organizações contra essa forma sofisticada de fraude e manipulação e, para evitar ataques de engenharia social, a Kaspersky sugere medidas, como: verificar a fonte das informações recebidas, desconfiar de perguntas de segurança que não são feitas por instituições que têm seus dados pessoais, não ceder à pressão do tempo, pois muitos ataques exploram a urgência, pedir identificação em situações suspeitas e utilizar um filtro de spam eficaz para identificar e-mails indesejados.

Outrossim, a Legislação Brasileira trata a respeito destes ataques, ainda que por vezes indiretamente, como na Lei Geral de Proteção de Dados Pessoais. A engenharia social e a Lei Geral de Proteção de Dados (LGPD) estão relacionadas à segurança da informação e à proteção da privacidade, mas tratam de aspectos diferentes. A LGPD é uma regulamentação brasileira que visa proteger a privacidade e os dados pessoais, estabelecendo regras para seu tratamento. Ela afeta os ataques de engenharia social de várias maneiras, tanto positivas quanto negativas.

A LGPD exige consentimento explícito para a coleta e processamento de dados pessoais, o que pode ser um obstáculo para os atacantes de engenharia social que obtêm informações sem consentimento. Além disso, obriga as organizações a notificar autoridades e titulares de dados em caso de violação, o que pode ter implicações legais para os infratores.

A aplicação da LGPD aumenta a conscientização sobre a importância da proteção de dados pessoais, tornando as pessoas mais cautelosas contra tentativas de engenharia social. Também coloca maior responsabilidade sobre as organizações na proteção dos dados pessoais, incentivando investimentos em segurança.

A legislação brasileira relacionada à engenharia social, segurança cibernética e proteção de dados é relevante e complexa. Ela inclui o Marco Civil da *Internet* (Lei 12.965/2014), que enfatiza a liberdade, a privacidade e a segurança dos dados online.

Além disso, o Código Penal Brasileiro contém disposições que podem ser aplicadas em casos de engenharia social. Crimes como estelionato e falsidade ideológica podem ser relevantes, dependendo das circunstâncias e das ações dos infratores.

O Código Penal Brasileiro foi modificado pela Lei nº 14.155/2021 para lidar com desafios emergentes no cenário digital, especialmente relacionados à engenharia social. Dois tipos de crimes nessa área são identificáveis: o furto por fraude, enquadrado no artigo 155, parágrafo 4°, envolve enganar a vítima para obter acesso a informações valiosas que são então subtraídas de forma fraudulenta. A maioria dos crimes de engenharia social se encaixa na segunda categoria, tipificada no artigo 171, relacionada ao estelionato, onde o infrator usa manipulação ou fraude para induzir a vítima a realizar

ações prejudiciais, frequentemente envolvendo enganos, promessas falsas ou representações fraudulentas.

A Lei nº 14.155, atualizada em maio de 2021, trouxe modificações significativas ao Código Penal Brasileiro, com o objetivo de impor penas mais severas para crimes envolvendo invasões de dispositivos, furtos, má conduta em ambientes digitais e obtenção enganosa de informações, muitas vezes por meio de e-mails fraudulentos, redes sociais ou contatos telefônicos enganosos que levam indivíduos ao erro.

A Lei de Crimes Cibernéticos (Lei 12.737/2012) é relevante no contexto dos crimes cibernéticos, tratando de invasões de dispositivos e sistemas de informática. No Brasil, os ataques de engenharia social são considerados crimes, conforme a Lei 12.737/2012, conhecida como Lei Carolina Dieckmann, elaborada em resposta a um notório incidente de invasão de fotos íntimas e dados pessoais da atriz. Essa lei pode ser aplicada quando a engenharia social envolve a obtenção não autorizada de informações por meio de dispositivos eletrônicos.

Além disso, a proteção ao consumidor, regida pelo Código de Defesa do Consumidor, é relevante em situações de engenharia social que envolvam a oferta de produtos ou serviços enganosos ou fraudulentos. A Lei de Acesso à Informação estabelece diretrizes para o acesso à informação pública e pode ser aplicada em casos em que a engenharia social seja usada para obter informações de órgãos públicos.

4. Considerações finais

A engenharia social é uma ameaça cada vez mais sofisticada que explora a vulnerabilidade humana como seu ponto frágil. Os engenheiros sociais utilizam técnicas psicológicas para manipular vítimas e obter informações confidenciais ou acesso não autorizado a sistemas. A conscientização é fundamental para proteger indivíduos e organizações contra esses ataques, e medidas de segurança, como verificar a fonte das informações e desconfiar de solicitações suspeitas, são cruciais.

Além disso, a legislação brasileira, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD) e as atualizações no Código Penal, desempenha um papel importante na abordagem de crimes de engenharia social. A LGPD, em particular, aumenta a conscientização sobre a proteção de dados pessoais, mas também apresenta desafios, como a falsificação de consentimento.

Em última análise, a proteção contra a engenharia social requer uma abordagem holística que envolva educação, conscientização, tecnologia e conformidade legal. Essa ameaça em constante evolução exige vigilância contínua e esforços coordenados para garantir a segurança das informações e a privacidade dos indivíduos no ambiente digital..

5. Referências

BRASIL. Casa Civil. Decreto-Lei nº 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm >.

BRASIL. Casa Civil. Lei 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de

dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF, 30 nov. 2012. Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>;

BRASIL. Casa Civil. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da *Internet* no Brasil. Brasília, DF, 23 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>;

BRASIL. Casa CivilLei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 14 ago. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>;

BRASIL. Casa Civil. Lei nº 14.155, de 27 de maio de 2021. Lei que Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela *internet*; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Diário Oficial da União, Brasília, DF, 27 mai. 2021.

[1] BRASIL. Casa Civil. Lei 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor, Brasília, DF, 11 set. 1990. Disponível em < https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm >;

IBM.O que é engenharia social?. Disponível em < https://www.ibm.com/br-pt/topics/social-engineering >

KASPERSKY. Modos para evitar ataques de engenharia social. Disponível em: < https://www.kaspersky.com.br/resource-center/threats/how-to-avoid-social-engineering-attacks >

LONG, Rebecca M. Using phishing to test social engineering awareness of financial employees. EWU Masters Thesis Collection. 2013. Pág. 156. Disponível em: <http://dc.ewu.edu/theses/156>;

MARTINS, Rodrigo. Engenharia Social. 2014. Disponível em: <https://atitudereflexiva.wordpress.com/2014/08/26/engenharia-social/>;

MURAI, Aline Sayuri e RODRIGUES, Thaís de Souza. Engenharia social: o fator humano na segurança da informação. Disponível em < http://www.each.usp.br/petsi/jornal/?p=2824>.