**O FENÔMENO DOS GOLPES DIGITAIS DE ENGENHARIA SOCIAL E DO VAZAMENTO DE DADOS PESSOAIS NA PANDEMIA DA COVID-19[[1]](#footnote-1)**

Mônica de Sá Dantas Paz[[2]](#footnote-2); Carla Elaine Freitas Santos[[3]](#footnote-3)

**Resumo:** Um dos fenômenos decorrentes da pandemia da COVID-19 é relativo aos golpes digitais que, com o uso de dados pessoais dos brasileiros e com a utilização de técnicas de persuasão, induzem as vítimas a confiar seus dados ou a realizar transações financeiras em benefício do golpista. Diante disso, o objetivo deste trabalho é apresentar alguns casos de golpes digitais ocorridos durante a pandemia da COVID-19 que, de alguma forma, tenha explorado o contexto e temas relativos à pandemia, analisando-os a partir da perspectiva da engenharia social e dos princípios e requisitos da LGPD. Para tanto, serão estudados de forma qualitativa os casos do golpe do motoboy e o golpe do boleto falso, envolvendo as marcas Itaú e Claro, respectivamente, atentando-se para o *modus operandi* dos golpes; as técnicas de engenharia social e outros tipos de ataques utilizados; as comunicações aos clientes e à imprensa das empresas envolvidas; e, por fim, as possíveis implicações da LGPD no caso.

**Palavras-chave:** segurança da informação; golpes digitais; LGPD; vazamentos de dados pessoais; COVID-19;

**1. Introdução**

O atual cenário pandêmico demandou, diante de uma turbulência sanitária e econômica, um maior uso e aplicações de tecnologias da informação e comunicação – TIC, dentre ferramentas, ambientes e práticas sociais nas mais diversas áreas da vida humana. Em termos de práticas econômicas e financeiras, a pandemia e o isolamento social estimularam o aumento das compras online, dos pagamentos digitais por boletos, cartões de crédito e aplicativos de *fintechs*, além do aumento do *home office*, do desemprego, da busca por registro como microempreendedores individuais (MEI) e pelo surgimento de vários negócios digitais ou da transformação digital de empresas já estabelecidas, dentre outras práticas sociotécnicas. Este cenário colocou muitas pessoas diante do seu primeiro ou mais intenso e avançado contato com as TIC, mesmo que elas não estivessem preparadas para todas as questões inerentes ao ambiente digital.

Um dos fenômenos decorrentes da pandemia da COVID-19 é relativo aos golpes digitais que com o uso de dados pessoais dos brasileiros e com a utilização de técnicas de persuasão induzem as vítimas a confiar e cometer erros, como o de ceder seus dados bancários ou realizar transações financeiras em benefício do golpista. São alvo desses golpes as mais variadas atividades para além das financeiras e econômicas, como as relativas à comunicação via aplicativos de mensagens instantâneas, *e-commerce* e instalação de aplicativos, dentre outros. Contudo, as atividades envolvendo pagamentos, recebimentos, financiamentos e outras transações financeiras merecem destaque pelo seu grande potencial em causar danos às suas vítimas e por se somarem à crise econômica vivenciada no país e no mundo (APURA, 2020; ESKIVE, THE HACK, 2020; FENABRAM, 2020; RNP, 2020).

Para entender este contexto, pode-se recorrer à segurança da informação, que é uma disciplina do campo da ciência da computação que deixou de ser uma preocupação apenas das grandes empresas e vem sendo popularizada com a transformação digital das pequenas e médias e de toda a sociedade. O aumento das ameaças digitais suscitou questões como quebra de privacidade e a capitalização dos dados, dentre outras (BIONI et al, 2020; KSHETRI, 2020; MODESTO, EHRHARDT JUNIOR, 2020; SILVEIRA, 2017). Com o atual destaque dado aos golpes digitais, a segurança da informação passa a ser uma preocupação cada vez mais em voga.

No contexto de um mundo hiperconectado e do incremento no uso de informações e, consequentemente, do seu valor, reforça-se em nível mundial a preocupação com a privacidade e proteção de dados pessoais, inclusive para que não sejam usados nos golpes mencionados. No Brasil, esse fato reflete-se na Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018), que apresenta um conjunto de princípios e regras para o tratamento de dados pessoais, fundamentada no respeito à privacidade, na inviolabilidade da intimidade, dentre outros fundamentos. Uma das motivações da LGPD é aumentar a responsabilização das organizações na implementação de medidas técnicas e administrativas para a proteção da segurança da informação, evitando vazamento e perda de dados, além de outras implicações.

Sendo assim, o objetivo deste trabalho é apresentar alguns casos de golpes digitais ocorridos durante a pandemia da COVID-19 que, de alguma forma, tenha explorado o contexto e temas relativos à pandemia, analisando-os a partir da perspectiva da engenharia social e dos impactos aos princípios e requisitos da LGPD. Para tanto, serão estudados de forma qualitativa os casos do golpe do motoboy e o golpe do boleto falso, envolvendo as marcas Itaú e Claro, respectivamente.

**2. A engenharia social como uma ameaça à segurança da informação**

Segurança da Informação é definida com base nas propriedades relativas à informação e aos sistemas informatizados, como confidencialidade, integridade e disponibilidade, correspondendo à proteção das propriedades (ou requisitos) das informações. Também podem ser consideradas outras propriedades como confiabilidade, irretratabilidade, privacidade, autenticidade etc. No ramo empresarial, a segurança da informação está intrinsecamente ligada à continuidade dos negócios por ajudar a evitar ou minimizar impactos operacionais e danos à imagem e à saúde financeira das empresas, seja atribuindo qualidades aos seus produtos e serviços, quanto evitando processos e outros meios de perder clientes, lucros e operabilidade (HINTZBERGEN *et al*, 2018; ABNT, 2013).

A segurança das informações compreende proteger todo o ambiente relacionado, o que inclui processos, sistemas, redes, pessoas e outros ativos, além da própria informação. Os ativos são objetos de ameaças (ABNT, 2013), que podem explorar suas vulnerabilidades inerentes. Diante disso, a segurança da informação gerencia e controla as ameaças que visem comprometê-las.

Uma categoria de informação é dado pessoal, que consiste em toda informação relacionada a pessoa natural identificada ou identificável (BRASIL, 2018). A proteção de dados pessoais e a segurança da informação são disciplinas fortemente relacionadas, pois a violação de uma de suas propriedades pode trazer fortes implicações nos fundamentos preconizados nas legislações sobre o tema.

Dentre as inúmeras fontes de ameaças à proteção dos dados pessoais estão os ataques de engenharia social. A Engenharia Social consiste na aplicação de técnicas de manipulação de pessoas com o intuito de ganhar sua confiança para conseguir coletar informações ou induzi-las a executar ações em prol do golpista (MANN, 2018). Para tanto, podem ser exploradas várias características típicas do comportamento humano padrão, como curiosidade, inocência, ganância, generosidade, insegurança, frustração, etc.

O ataque de engenharia social pode ser apenas uma das partes de um ataque maior, no qual se quer obter acesso a um sistema ou organização. Também pode ser um ataque que visa tirar vantagem da vítima, apresentando-se na forma de diferentes golpes (golpe do motoboy, por exemplo) e utilizando-se de diferentes técnicas, como o *phishing*, *hoax*, *e-mail* *spoofing*, *typosquatting*, etc.

*Phishing*, técnica na qual o atacante visa obter informações confidenciais como dados financeiros e credenciais de acesso, disfarçados de entidades terceiras para enganar a vítima. De acordo com a empresa de soluções em segurança Kaspersky (2020), cerca de um em cada oito usuários no Brasil acessaram um link para páginas maliciosas, colocando o Brasil no quinto lugar do ranking mundial de vítimas de *phishing*.

*Hoax* ou boatos é o emprego de mensagens com linguagem e conteúdo alarmista e sensacionalista no intuito de enganar e atrair as vítimas, seja para dar vantagem para os golpistas, seja para a propagação da mensagem em si.

*E-mail* *spoofing* é a técnica que visa dar autenticidade à mensagens dos golpistas, ao alterar o cabeçalho das mensagens de forma a falsificar o remetente, enganando o destinatário.

*Typosquatting* é a técnica de criar URL falsas mais semelhantes às que se quer falsificar, com o uso de erros de grafia e de símbolos. Dessa forma, a vítima é direcionada a um site falso.

Outra forma de engenharia social é a obtenção de informações restritas e sigilosas, através de contatos telefônicos ou físicos. O atacante representa um papel e realiza um levantamento inicial de informações sobre a empresa ou a vítima para tornar a sua história mais convincente e aumentar a probabilidade de sucesso na sua investida.

Este artigo tem como foco a engenharia social, dentre tantas outras ameaças à segurança da informação, por ser a principal técnica explorada nos golpes estudados neste trabalho que têm como alvo o indivíduo, logo explorando suas vulnerabilidades.

**3. Golpes financeiros durante a pandemia da COVID-19**

Diferentes tipos de golpes foram registrados no Brasil e no mundo desde os primeiros meses da pandemia da COVID-19 com o objetivo de obtenção de vantagem financeira. Alguns exemplos brasileiros são apresentados a seguir de acordo com o tipo de contato ou mídia utilizada pelos golpista para abordar suas vítimas segundo a FEBRABAN (2020a), RNP (2020), PROCON SP (2020) e G1 (2020):

* Golpes com contato pessoal:
  + Golpe do delivery ou Golpe do entregador, que cobra um valor elevado em uma máquina de pagamento com o visor quebrado, alegando se tratar de uma taxa extra;
  + Golpe da troca de cartão no caixa eletrônico ou Golpe da troca de cartão, um falso atendente do banco presta ajuda à vítima e, ao final, entrega um outro cartão a ela, ficando com o cartão da vítima. O cartão também pode ser furtado sob a alegação de que o caixa eletrônico não devolveu o cartão ou, ainda, que o funcionário precisará ficar com o cartão para resolver pendências da conta. A troca de cartão também pode ser realizada por falsos vendedores no comércio.
  + Golpe do cartão não presente, quando os dados do cartão são copiados, por exemplo, durante uma compra presencial e são usados em compras online pelos criminosos;
* Golpes via telefone e contato pessoal:
  + Golpe do falso motoboy, que coleta o cartão supostamente clonada na residência da vítima;
  + Golpe do extravio do cartão, no qual, após o roubo da correspondência com o cartão, por telefone, os criminosos induzem a vítima a desbloquear o cartão via site ou aplicativo;
* Golpes por telefone:
  + Golpe do falso funcionário, que liga para as vítimas em busca de dados financeiros mediante suposta clonagem do cartão da vítima ou a induz a realizar transferências de modo a desbloquear o itoken, realizar uma mudança de segmento de conta ou para estornar um crédito indevido;
  + Golpe da central falsa, semelhante ao anterior, engana a vítima e a conduz a digitar a sua senha e fornecer informações pessoais, que são coletadas pelos criminosos;
  + Golpe do vale-presente, o golpista se passa por advogado de um parente da vítima que estaria com dificuldades financeiras e solicita que sejam comprados vales-presentes, como os da Google Play, para ajudá-lo[[4]](#footnote-4).
* Golpes por aplicativos:
  + Golpe do WhatsApp, que clona a conta da vítima após a mesma entregar ao golpista o seu código de acesso e este, uma vez de posse da lista de contatos, pede empréstimos para os contatos da vítima;
  + Fraudes com o FGTS emergencial através do aplicativo Caixa Tem;
  + Roubo de conta de *digital influencer*, que utiliza a popularidade de personalidades da Internet para promover produtos e campanhas de arrecadação, muitas vezes falsos ou inexistentes.
* Golpes por e-mail:
  + Golpe do falso leilão, que coleta dados financeiros da vítima em um site falso;
  + Golpe do e-commerce falso, que anuncia produtos inexistentes a fim de coletar dados das vítimas e de receber pagamentos por produtos inexistentes;
  + Golpe do boleto falso, que induz a vítima a realizar um pagamento para os golpistas, pensando estar pagando as suas contas legítimas;
* Golpes por e-mail ou SMS:
  + Golpes de recadastramento em serviços ou do bloqueio de conta, que coletam dados da vítima através de links para formulários falsos com a desculpa de fazer a manutenção de serviços como a da Netflix; e inúmeros outros golpes.

Dentre os golpes observados, destacam-se dois tipos de golpes digitais que vitimizam pessoas, utilizando-se de forma fraudulenta de suas **relações com grandes empresas** de prestação de serviços financeiros e de serviços de telecomunicações. São o “golpe do falso motoboy” e o “golpe do boleto falso”.

Alguns dos golpes citados anteriormente não são necessariamente golpes digitais, mas sim apenas golpes financeiros, sem o uso de mídias e tecnologias digitais para aplicar o golpe de engenharia social. Porém, ao final, usam redes digitais para realizar compras, contratações, transferências e saques em espécie. É o caso, por exemplo, do golpe do falso motoboy, como veremos a seguir. Contudo, consideramos que todos os golpes citados cabem no contexto desse estudo, pois são as tecnologias digitais que possibilitam a concretização do golpe e do prejuízo às vítimas.

Para estudar tais casos, a metodologia adotada é a de pesquisa exploratória (GIL, 1991), através do estudo de caso sobre os golpes digitais de engenharia social mencionados, dos quais serão relatados e analisados: o *modus operandi* dos golpes; as técnicas de engenharia social e outros tipos de ataques utilizados e as comunicações aos clientes e à imprensa das empresas envolvidas. Uma análise dos golpes sob a ótica da LGPD é apresentada, abordando suas implicações para a vítima, o golpista e as empresas potencialmente envolvidas.

Para tanto, o *corpus* do estudo será formado por: notícias e reportagens retiradas de sites da grande mídia e de sites especializados em tecnologia e segurança sobre os casos estudados; postagens de reclamantes vítimas dos golpes citados em serviços como o Reclame Aqui; mensagens enviadas pelas empresas envolvidas aos seus clientes sobre os incidentes estudados; conteúdos sobre segurança da informação coletadas dos sites das empresas envolvidas.

**3.1 O *modus operandi* do golpe do falso motoboy**

No golpe do falso motoboy, o golpista liga para a vítima alertando sobre um comprometimento na segurança do seu cartão de crédito, anunciando que o mesmo foi clonado, que deve ser bloqueado e que, em seguida, um motoboy ou um funcionário do banco o coletará na residência da vítima para perícia e devido descarte.

Na ligação telefônica, o golpista se identifica como sendo de uma das empresas bancárias ou seguradoras de cartão de crédito, indica a possibilidade de compras não autorizadas no cartão da vítima, que é solicitada a reconhecer ou não uma determinada compra inexistente. Como a vítima desconhece a compra, o golpista indica a necessidade de bloqueio do cartão e, para tanto, deve ser fornecida a senha do cartão.

Caso a vítima escolha não passar as informações na ligação recebida e prefira ligar para o número conhecido de sua empresa para confirmar a situação, o golpista pode “prender a ligação”, ou seja, não desliga a ligação, permanecendo na mesma enquanto a vítima disca para o número real, que não será conectado. Após escutar a discagem, o golpista reproduz músicas e mensagens gravadas, como a da empresa real, e outro golpista entra em ação, atendendo a vítima e confirmando a história falsa. Ainda durante a ligação, antes da coleta do cartão em domicílio, a vítima pode acabar fornecendo o seu endereço residencial e é aconselhada a inutilizar a tarja magnética do cartão, mas nada é falado em relação ao chip.

Com o cartão da vítima em mãos e, provavelmente, com o chip íntegro, o golpista tem acesso a dados que o permite realizar compras e assinaturas de serviços de forma presencial e online. A vítima fica com o prejuízo e com a tarefa de tentar reaver seu dinheiro através de contratos de seguros junto a sua empresa prestadora de serviços financeiros.

O golpe do motoboy também é conhecido como: golpe do falso motoboy (A GAZETA, 2020), golpe do cartão de crédito clonado (GZH, 2020) e golpe do falso funcionário (RC, 2020). É importante notar que existe uma variante desse golpe, na qual o golpista apenas coleta dados financeiros da vítima por telefone sem o envio do motoboy à sua casa, o que também é denominado de golpe do falso funcionário (FEBRABAN, 2020a).

O que se pode apontar neste caso em relação à engenharia social é que as vítimas são envolvidas em uma história falsa na qual elas são vítimas de terceiros, o que pode deixá-las emocionalmente abaladas diante da sensação de invasão e de perdas financeiras. Ao se sentirem prejudicadas, ficam vulneráveis a receber instruções e ajuda de desconhecidos que apresentam cargo, vocabulário, tecnologia de centrais de atendimento e soluções que denotam conhecimento no tema abordado, adquirindo assim a confiança da pessoa. Além disso, o golpista se utiliza da imagem de uma grande empresa para conquistar a confiança da vítima e, ainda, este golpista, além de apresentar um problema, orienta a vítima para uma possível solução. A partir desse cenário de risco financeiro, a vítima é levada a acreditar na história e a entregar seus dados e o cartão.

Segundo a Federação Brasileira de Bancos - FEBRABAN (2020), “o golpe do falso motoboy teve aumento de 65% durante o período de isolamento social”. Diante dessa difusão, o golpe do falso motoboy também tem recebido muita atenção da mídia, que tem produzido matérias sobre o tema, alertando sobre o funcionamento do golpe e, até mesmo, apresentando gravações com a tentativa do golpe em andamento, como o caso da matéria do Fantástico (2020), dentre outros (A GAZETA, 2020; RC, 2020; GZH, 2020)[[5]](#footnote-5).

**3.1.1 O caso Itaú**

O golpe do falso motoboy foi objeto de alerta para empresas do ramo financeiro, como Itaú, Credicard e Hipercard, dentre outras, que mobilizaram, de forma integrada, a sua comunicação com os clientes, enviando-lhes mensagens eletrônicas e SMS, além de disponibilizar conteúdos informativos em seus sites.

No que se refere ao Banco Itaú, há registro do uso de SMS, desde meados de abril, para prevenir seus clientes com o seguinte conteúdo: “Itau: Atencao com o golpe do falso motoboy! Nao enviamos ninguem a sua casa para retirar cartao, computador, tablet, celular ou chip. Compartilhe!”. Já em maio, houve comunicação do Itaucard com seus clientes em mensagem intitulado “Atenção ao Golpe do Motoboy!”[[6]](#footnote-6).

O tema é reforçado para quem visita o site do Itaú, na seção Segurança, que hospeda conteúdos informativos sobre medidas de proteção para compras online, alertas sobre fraudes e golpes envolvendo cartões, Pix e contatos falsos, além de explicações sobre LGPD, privacidade e termos de uso para os seus sites e aplicativos. Para tanto, várias mídias são utilizadas como: dicas rápidas em lista enumerada, como o caso de “compras online com segurança” que é acompanhado de vídeo explicativo; subpáginas, como “LGPD e privacidade”[[7]](#footnote-7), “conheça o dispositivo de segurança iToken”[[8]](#footnote-8) e “dicas de segurança Pix”[[9]](#footnote-9); textos em PDF, como “e-book de dicas de prevenção a fraude”; e, pelo menos, sete vídeos, como “golpes em compras online” e “o que é phishing?”, que também podem ser acessados no canal do banco Itaú no Youtube[[10]](#footnote-10), juntamente com mais vídeos de outras temáticas.

O golpe do motoboy é tratado em vídeo intitulado “como funciona o golpe do motoboy?”, que se trata de uma animação que explica como ocorre o golpe, quais os riscos e formas de proteção, além do convite ao compartilhamento do conteúdo.

Ainda na seção sobre segurança do site do banco Itaú, estão disponibilizados os seus termos de uso de sites e aplicativos, bem como o canal, via e-mail, para que os clientes reportem golpes e e-mails suspeitos, além da sua certificação ISO/IEC 27001:

O Sistema de Gestão da Privacidade Online do Itaú Unibanco recebeu a certificação ISO 27001, que é referência internacional em segurança da informação. A Auditoria foi realizada pela Fundação Vanzolini e foi concedida depois de uma avaliação da norma e procedimentos da Gestão da Segurança da Informação na captação de dados pessoais cadastrados nos servidores internet do Banco Itaú Unibanco S.A., através das páginas componentes do site www.itau.com.br. Isso reforça o compromisso do banco com a segurança e a privacidade de todos os clientes e não clientes que utilizam o site Itaú (ITAÚ, s.d.).

Fica claro que a empresa faz investimento em discurso e produção de conteúdo sobre informação e conscientização sobre segurança da informação para evitar que seus clientes sejam vítimas de golpes com o seu nome, o que em certa medida poderia comprometer o relacionamento entre cliente e empresa. Indo além, há um esforço em construir uma imagem de empresa que preza e zela pela segurança das informações e patrimônio das pessoas.

Segundo o site Reclame Aqui, o Banco Itaú resolve 74% das reclamações feitas pelos usuários, o que é uma taxa considerada boa[[11]](#footnote-11). Não foram encontrados registros sobre o golpe em questão, contudo, é válido mencionar que “golpe” é uma das palavras suprimidas pelo site que a substitui por “[Editado pelo Reclame Aqui]”, o que dificulta um pouco a busca.

**3.2 O *modus operandi* do golpe do boleto falso**

No golpe do boleto falso, os golpistas utilizam-se de dados reais da vítima, com os quais são criados e enviados boletos falsos, porém idênticos ao real, fazendo a vítima pagar ao golpista, mantendo a dívida com a empresa.

Os golpistas preferem utilizar-se, de forma fraudulenta, da imagem de grandes e populares empresas, que costumam fornecer o boleto como forma de pagamento para os seus clientes.

Em termos de técnicas de engenharia social, em alguns casos, os golpistas oferecem descontos para fornecer à vítima uma sensação de ganho e de desconto, levando-a a antecipar o pagamento e aproveitar a oportunidade o quanto antes.

O boleto falso também pode ser gerado através de arquivos maliciosos (malwares) instalados no computador da vítima, que alteram conteúdos de boletos originais.

**3.2.1 O caso Claro**

Este golpe levou a Chevrolet Serviços Financeiros e a Claro NET, dentre outras empresas, a orientar seus clientes sobre como reconhecer um boleto original, evitando prejuízos e reclamações.

Um caso que ganhou destaque foi o da Claro Net, empresa que fornece serviço de conexão à internet, telefone e conteúdos por assinatura. Uma forma habitual de pagamento aceito pela empresa é o boleto, que costuma ser enviado com antecedência em relação à data de vencimento da mensalidade.

Contudo, por volta de agosto e outubro, vários clientes começaram a se queixar de terem recebido um boleto falso em nome da Claro/NET, contendo os seus dados reais como nome, endereço, CPF, data de vencimento, número de contrato, plano, etc. A mensagem oferecia um desconto em decorrência da pandemia e prometia desbloquear o serviço dos inadimplentes:

Olá,

Devido a [sic] pandemia que estamos enfrentando no Brasil e no mundo, iremos oferecer durante os próximos meses um desconto muito especial. Aproveite este desconto de **50%** em sua fatura e evite o bloqueio do seu serviço.

Caso seu sinal esteja bloqueado, após a identificação da baixa desta fatura em nosso sistema seu sinal será reabilitado.

**Atenção:** Para sua maior comodidade anexamos neste e-mail o PDF da 2ª via de sua fatura com o desconto aplicado”[[12]](#footnote-12).

Poucas horas depois, às 9:50, aproximadamente, os clientes Claro receberam uma mensagem eletrônica oficial intitulada “COMUNICADO IMPORTANTE: Saiba como identificar uma fatura Claro”. No corpo da mensagem, a Claro (2020) introduz o problema:

FIQUE ATENTO ÀS TENTATIVAS DE FRAUDES NO AMBIENTE DIGITAL. Tentativas de fraudes com descontos em boletos, infelizmente são uma realidade em nosso dia a dia. Por isso, a Claro compartilha algumas informações para que você esteja protegido nestas situações.

Confira algumas dicas para verificar se a sua fatura é verdadeira.

Na sequência, são apresentados o e-mail e a conta Whatsapp oficiais da empresa, bem como o código inicial correto dos boletos autênticos da empresa. Por fim, o e-mail também indica a seção do site da empresa que aborda o tema da segurança.

Na mensagem enviada aos clientes, a empresa não menciona nada em relação a um possível vazamento ou uso não autorizado de dados controlados pela empresa, o que justificaria o uso dos dados pessoais corretos dos clientes. Contudo, em 2019, houve indícios de que uma falha no sistema da Claro poderia ter exposto os dados de milhares de clientes. Esta falha de segurança foi admitida pela empresa, embora ela não reconheça possíveis prejuízos aos clientes (OLHARDIGITAL, 2019)[[13]](#footnote-13). Ainda, em 2020, arquivos de 2018 com dados dos clientes Claro estariam a venda na dark web, segundo o grupo The Hack (ISTOÉDINHEIRO, 2020)[[14]](#footnote-14).

No Catálogo de Fraudes da RNP, que apresenta mais de 12 mil mensagens fraudulentas que circulavam pela internet, desde 2008, há registro do golpe em questão com data de agosto de 2020, sendo incluindo do catálogo desde primeiro de setembro. Outros golpes que se utilizam da marca Claro também estão catalogados, contudo não mencionam a pandemia como pretexto, mas ocorreram durante o período de crise.

De 22 mensagens fraudulentas, todas continham queixas sobre boleto falso; 5 mencionaram boleto em aberto ou falta de identificação de pagamento no sistema; e os 6 seguintes registros foram sobre a pandemia:

* Assunto da mensagem: Sua fatura Claro net por e-mail - <DATA>
  + Data de inclusão: 02/09/20, https://catalogodefraudes.rnp.br/frauds/14646
* Assunto da mensagem: Sua fatura Claro net por e-mail - 08/2020
  + Data de inclusão: 01/09/20, https://catalogodefraudes.rnp.br/frauds/14639
* Assunto da mensagem: Sua fatura por e-mail - 08/2020
  + Data de inclusão: 28/08/20, https://catalogodefraudes.rnp.br/frauds/14632
* Assunto da mensagem: Sua fatura Claro net por e-mail - 08/2020
  + Data de inclusão: 26/08/20, https://catalogodefraudes.rnp.br/frauds/14628
* Assunto da mensagem: Sua fatura Claro net por e-mail - <DATA>
  + Data de inclusão: 24/08/20, https://catalogodefraudes.rnp.br/frauds/14619
* Assunto da mensagem: Sua fatura Claro net por e-mail - 08/2020
  + Data de inclusão: 14/08/20, https://catalogodefraudes.rnp.br/frauds/14601

Apesar da diferença nos títulos, o texto da mensagem é o mesmo, mudando apenas os dados do cliente e as datas de registro da fraude, que variam entre agosto e setembro de 2020. Além disso, algumas mensagens mencionaram que a data da cortesia era a mesma do envio da mensagem. Ou seja, estratégias para criar um sentimento de vantagem e de urgência que podem levar a vítima a cometer o erro de pagar o boleto falso.

No site Reclame Aqui, a Claro aparece como uma das piores empresas segundo a avaliação dos reclamantes. Talvez porque este parece não ser um canal oficial utilizado pela empresa para responder às queixas de seus clientes. Segundo a página relativa à empresa no site Reclame Aqui[[15]](#footnote-15), nos últimos 6 meses (01/06/2020 - 30/11/2020), foram registradas 39.569 reclamações não respondidas, o que já se equipara a 2019 com 40.750 registros e a 2018 com 34.825 reclamações. Ou seja, houve um aumento de registros em 2020 (01/12/2019 - 30/11/2020) que já registra 74.747 queixas. O mesmo acontece com a NET, empresa que hoje é de propriedade da Claro.

Para a pesquisa “boleto falso da claro net site:reclameaqui.com.br”[[16]](#footnote-16), no site de pesquisa da Google, coletamos e analisamos os cinco primeiros resultados[[17]](#footnote-17). Em todos os casos houve queixa em relação ao vazamento de dados pessoais. Mesmo quem não sofreu o golpe, apresentou-se indignado com a possível quebra de sua privacidade:

[...] sendo assim o motivo da minha reclamação é baseado no fornecimento dos meus dados de forma indevida me gerando uma cobrança falsa e consequentemente problemas. [...][[18]](#footnote-18)

[...] SO QUE ENGRAÇADO QUE TINHA MEUS DADOS PESSOAIS E O NUMERO DE CONTRATO COM A NET/CLARO; AGORA PERGUNTO COMO VAZARAM ESSAS INFORMAÇÕES PARA QUE FIZESSEM UM BOLETO FALSO. COMO A NET/CLARO PERMITIU QUE INVADISSEM ASSIM FACILMENTE SUA PLATAFORMA DE DADOS. [...][[19]](#footnote-19)

Estou abrindo a reclamação pois ou a empresa está disponibilizando os dados dos clientes (nome, cpf, endereço, número do contrato) e faz parte dessa [Editado pelo Reclame Aqui] ou a empresa não está muito afim de proteger os dados dos seus clientes. [...]

Como já citamos, muitas empresas estão investindo na produção de conteúdo de conscientização, mas para alguns, estas iniciativas não são suficientes diante da baixa qualidade em segurança dos serviços prestados:

[...] Colocar uma página no site de vocês dizendo alerta para os boletos falsos é tentar se livrar da culpa. Se essas cobranças são de [Editado pelo Reclame Aqui], há alguma coisa muito errada com a facilidade que eles podem conseguir nossos dados! [...][[20]](#footnote-20)

Dos cinco comentários analisados, quatro denunciaram a fraude, mas apenas um acabou tornando-se uma vítima do mesmo e, com a queixa, busca retratação junto com a empresa utilizada pelos fraudadores.

Minha esposa recebeu um boleto falso (mais de uma vez), oferecendo um desconto de 50% sobre um boleto com atraso, onde nesse e-mail constava todas as informações da minha esposa, como e-mail, endereço residencial, CPF, nome completo e o endereço de e-mail de remetente era corporativo da NET, assim, como já havíamos recebido diversas vezes nos meses anteriores e nunca precisamos, dessa vez, decidimos utilizar esse boleto[...][[21]](#footnote-21)

Interessante notar que, mesmo não sendo a primeira vez, as pessoas envolvidas se deixaram levar pela situação atual, o que reforça o argumento da engenharia social explorando as vulnerabilidades humanas.

**3.3 Análise dos golpes e vazamento de dados pessoais na ótica da privacidade e proteção de dados pessoais**

Segundo a LGPD, todo e qualquer tratamento de dados pessoais realizado por pessoa natural ou jurídica de direito público ou privado no território brasileiro, salvo as exceções em seu artigo 4º, devem obedecer aos requisitos da citada legislação. A utilização dos dados pessoais para realização de golpes não se encaixa nas hipóteses de exceção da lei, o que abre a possibilidade de interpretação dos seus requisitos.

Partimos também do pressuposto que tais golpes são facilitados por usar informações verdadeiras, que levam os clientes dessas empresas a acreditar que estão em uma transação legítima. A fonte dessas informações pode ser o roubo de dados, tanto junto aos clientes previamente (ex: *phishing*) quanto junto à prestadora dos serviços através de ataques cibernéticos, falhas técnicas ou anuência do pessoal interno que leva a um vazamento de dados.

A análise da LGPD é, então, apresentada considerando a visão do golpe e do vazamento de dados com suas possíveis implicações para a vítima e para a empresa controladora dos dados vazados - todas diretamente relacionadas a uma inestimável relevância jurídico-social ao indivíduo e a sociedade.

O conceito "Controlador de dados" consiste em pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. O Controlador define quais são os dados e as finalidades de seu uso, respondendo primariamente pela proteção dos dados e privacidade dos titulares envolvidos, mesmo quando a violação ocorre em fornecedores ou terceiros contratados, que atuam no papel de "operador" perante a legislação.

A privacidade é um direito da pessoa natural garantido em lei, estabelecido em dispositivos como a Constituição Federal e, mais recentemente, detalhada pela Lei Geral de Proteção de Dados. A LGPD está ancorada em um conjunto de fundamentos que representam os principais motivadores de seus requisitos. A partir destes fundamentos, é possível observar que, do ponto de vista da vítima, sob a ótica do vazamento de dados e do golpe, consequente, foram violados os seguintes fundamentos: o respeito à privacidade; a inviolabilidade da intimidade, da honra e da imagem; e a dignidade.

O vazamento de dados pessoais expõe informações do indivíduo como identificação pessoal, costumes, dados financeiros e de saúde, cuja exposição afeta aspectos de sua vida privada, da sua honra e da sua imagem podendo ter impactos irreversíveis à pessoa afetada. Por sua vez, a ocorrência de golpes, concretizados ou não, causa uma insegurança psicológica ao indivíduo, tendo impacto em sua dignidade, outro fundamento amparado na LGPD.

A legislação brasileira de proteção de dados garante a titularidade de seus dados pessoais ao indivíduo, conforme Artigo 17. Entretanto, o vazamento de dados pessoais torna inviável e impraticável ao indivíduo ter controle sobre os seus dados, haja vista, a divulgação incontrolada nos meios digitais. O direito à titularidade do dado pessoal também é comprometido no uso malicioso e ilícito dos dados pelos golpistas para benefícios próprios.

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Indo além do caráter ilícito do ato, o tratamento dos dados pessoais vazados na realização do golpe não possui nenhuma previsão jurídica na LGPD para sua legitimidade. Assim sendo, caberia unicamente a hipótese de consentimento pelo titular, conforme Artigo 7º, inciso I, a qual é facilmente descartada no contexto de golpe, pois não se trata de uma manifestação livre, informada e inequívoca do titular de dados, atributos requeridos ao consentimento pela lei.

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

Se por um lado há o indivíduo com seus direitos violados, no outro, pode haver a responsabilização da empresa controladora dos dados pessoais que facilitou esse fato.

Primeiramente, o Controlador pode não ter atendido aos princípios de segurança e de prevenção descritos no Artigo 6º, incisos VII e VIII:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

Muito provavelmente a empresa deve ter implementado medidas técnicas e administrativas para a segurança da informação, porém observa-se que as elas não foram "aptas" para a adequada e efetiva proteção dos dados pessoais, o que acabou resultando em um vazamento das informações de seus clientes. É importante, além de implementar medidas, verificar continuamente a sua eficácia em processos de monitoramento e auditoria, conforme orienta às boas práticas sobre o tema como a ISO 27001 (ABNT, 2013). A mesma norma também orienta que os riscos de segurança da informação sejam avaliados e tratados adequadamente, reduzindo a níveis aceitáveis pela organização e, consequentemente, as possibilidades de ocorrência de vazamento e outros incidentes de segurança.

A responsabilidade com a segurança da informação pelos agentes de tratamento, conceito que abrange os papéis de controlador e operador, é explicitamente citada no Artigo 46 da LGPD:

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

A violação do princípio da prevenção pode ser observada na concretização de danos aos titulares afetados, seja através dos impactos dos golpes decorrentes ou da desobediência aos fundamentos legais de proteção de dados mencionados anteriormente.

Outra implicação da LGPD ao Controlador (ou Operador, quando aplicável) é a obrigação de reparar danos patrimonial, moral, individual ou coletivo decorrentes de violação à privacidade e proteção de dados, o que poderia ser relacionado às consequências dos golpes ora apresentados.

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Esse conjunto de violação aos requisitos da LGPD implica em sanções diversas previstas no dispositivo legal, que inclui desde advertência até a aplicação de multas, que podem chegar a 2% do faturamento anual, limitada a R$ 50 milhões.

Ainda na hipótese de desrespeito aos direitos dos titulares pela empresa controladora de dados, a LGPD não exclui a possibilidade de responsabilização por outros dispositivos legais, como o Código Civil e o Código de Defesa ao Consumidor, o que acentua as possibilidades de aplicações de medidas cíveis.

Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

É importante observar que a legislação de proteção de dados pessoais ainda está em processo de amadurecimento no país e sua jurisdição está em construção. De toda forma, é possível concluir que tanto o ato do vazamento de dados quanto do golpe financeiro, afeta os direitos dos indivíduos preconizados na LGPD, assim como apresenta um cenário de risco jurídico para as entidades envolvidas. No caso dos golpes financeiros, em particular, ainda prevalecem as disposições e sanções penais previstas em outros dispositivos legais brasileiro.

O surgimento de legislações de proteção de dados, como a LGPD e a lei europeia General Data Protection Regulation (GDPR), tem contribuído para um aumento da consciência dos indivíduos com relação à sua privacidade e proteção de dados pessoais. Um exemplo é o caso recente do WhatsApp, cuja atualização da política de privacidade ocasionou uma forte migração de usuários para aplicativos concorrentes. Dessa forma, reforça-se também a preocupação em observar os requisitos da LGPD para evitar violações e consequentemente impactos na imagem e reputação de empresas.

Como exposto anteriormente, o vazamento de dados pessoais pode ser um facilitador de golpes financeiros. A conformidade com a LGPD requer também uma diligência das empresas com a segurança da informação, o que consequentemente, fomenta um ambiente mais seguro para seus negócios. Isso significa que os riscos de vazamento de dados são reduzidos, dificultando a ocorrência de golpes financeiros, pois o golpista precisará buscar outras fontes de dados ou trabalhar com suposições que aumentam a chance de falhas na execução do golpe.

**4. Considerações finais**

Este trabalho se justifica por debater o fenômeno sociotécnico dos golpes digitais de engenharia social que ameaçam a privacidade dos dados pessoais, unindo em colaboração tanto disciplinas da comunicação, quanto da computação.

Independente do termo utilizado – segurança da informação, segurança digital, cuidados digitais - é certo que a adoção de medidas de proteção em meios digitais se faz urgente e, provavelmente, passarão a fazer, ou no mínimo, devem fazer parte do futuro online e pós-pandêmico.

Os impactos financeiros dos golpes são claramente reconhecidos pela sociedade, além de ter uma previsão legal mais antiga no ecossistema jurídico brasileiro. Entretanto, a análise sob o ponto de vista de impactos a privacidade ainda apresenta um longo caminho a ser percorrido para seu amadurecimento. Espera-se que esse artigo apoie na construção desta visão.

**Referências**

ABNT, Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002:2013 In: A**BNT Catálogo**. Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=306582>. Acesso em 26 out. 2020.

A GAZETA. **Golpe do falso motoboy: dona de casa desconfia e ajuda polícia a prender suspeito no ES**. Disponível em: <https://www.agazeta.com.br/es/policia/golpe-do-falso-motoboy-dona-de-casa-desconfia-e-ajuda-policia-a-prender-suspeito-no-es-0920>. Acesso em: 29 nov. 2020.

APURA CYBERINTELLIGENCE. **Coronawave**: ameaças digitais em tempo de pandemia, 2020.

BIONI, Bruno; ZANATTA, Rafael; MONTEIRO, Renato; RIELLI, Mariana. **Privacidade e pandemia**: recomendações para o uso legítimo de dados no combate à COVID-19. Conciliando o combate à COVID-19 com o uso legítimo de dados pessoais e o respeito aos direitos fundamentais. São Paulo: Data Privacy Brasil, 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 26 out. 2020.

ESKIVE; THE HACK. **COVID-19**: uma análise de fraudes e golpes explorando a pandemia abril 2020.

FANTÁSTICO. **Golpe do motoboy causa prejuízos de até R$ 8 mil; entenda como funciona e como evitar**. Disponível em: <https://g1.globo.com/fantastico/noticia/2020/06/21/golpe-do-motoboy-causa-prejuizos-de-ate-r-8-mil-entenda-como-funciona-e-como-evitar.ghtml>. Acesso em 29 nov. 2020.

FEBRABAN, 1. **Conheça as tentativas de golpes financeiros mais comuns na pandemia e saiba como evitá-los**. 2020a .Disponível em: <https://portal.febraban.org.br/noticia/3522/pt-br/>. Acesso em 29 nov. 2020.

FEBRABAN, Federação Brasileira de Bancos. **FEBRABAN alerta para sites fraudulentos usando nome da instituição**. 2020b. Disponível em: <https://portal.febraban.org.br/pagina/3185/52/pt-br/alerta-site-fraudulentos>. Acesso em 29 nov. 2020.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 2. ed. SP: Atlas, 1991.

GZH. **Polícia Civil do RS lança aplicativo que mostra os 15 principais golpes e ensina como se protege**. Disponível em: <https://gauchazh.clicrbs.com.br/seguranca/noticia/2020/11/policia-civil-do-rs-lanca-aplicativo-que-mostra-os-15-principais-golpes-e-ensina-como-se-proteger-ckhvyj5930012014lghq0m5vv.html>. Acesso em 29 nov. 2020.

HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. Brasport: 2018, Tradução: Alan de Sá.

KASPERSKY. **Spam and phishing in Q2 2020**. Disponível em https://securelist.com/spam-and-phishing-in-q2-2020/97987/ . Acesso em 25 out. 2020.

MANN, Ian. **Engenharia Social**. Série Prevenção de Fraudes. Editora Edgar Blucher, 2018.

MODESTO, Jéssica Andrade; EHRHARDT JUNIOR, Marcos. **Danos colaterais em tempos de pandemia**: preocupações quanto ao uso dos dados pessoais no combate a COVID-19. In: Redes: Revista Eletrônica Direito e Sociedade, Canoas, v. 8, n. 2, 2020.

KSHETRI, Nir. **The Economics of Cyberattacks on Brazil**. In: **IEEE Computer Society**, 2020 DOI 10.1109/MC.20202997322

PROCON SP. **Procon-SP alerta para golpe da troca de cartão**. 2020. Disponível em: https://www.procon.sp.gov.br/procon-sp-alerta-para-golpe-da-troca-de-cartao/. Acesso em: 15 jan. 2021.

PROCON SP. **PROCON-SP alerta para golpe do delivery**. Disponível em: https://www.procon.sp.gov.br/procon-sp-alerta-para-golpe-do-delivery/. Acesso em: 15 jan. 2021.

RC, Rádio Cidade. **Polícia Militar de Brusque alerta para golpe do falso funcionário**. Disponível em: <https://rc.am.br/homes/page_noticia/id_62961/titulo_pol-iacute-cia-militar-de-brusque-alerta-para-golpe-do-falso-funcion-aacute-rio/>. Acesso em: 29 nov. 2020.

REVISTAPEGN, Revista. Pequenas Empresas Grandes Negócios. **Golpes virtuais disparam com pandemia**. 2020. Disponível em: https://revistapegn.globo.com/Banco-de-ideias/Mundo-digital/noticia/2020/06/golpes-virtuais-disparam-com-pandemia-coronavirus.html. Acesso em: 15 jan. 2021.

RNP, Rede Nacional de Ensino e Pesquisa. **Catálogo de Fraudes**. Disponível em:<https://catalogodefraudes.rnp.br/>. Acesso em 29 maio 2020.

SILVEIRA, Sergio Amadeu da. **Tudo sobre tod@s**: Redes digitais, privacidade e venda de dados pessoais. São Paulo: Edições SESC São Paulo, 2017.

1. Artigo apresentado ao Eixo Temático 24. Ciberataques, Cyberwar. [↑](#footnote-ref-1)
2. Doutora em Comunicação e Cultura Contemporâneas pela UFBA. Integrante do Grupo de Pesquisa em Gênero, Tecnologias Digitais e Cultura e pesquisadora em pós-doutoramento pelo PPGDC, ambos da UFBA. E-mail: profmonicapaz@gmail.com [↑](#footnote-ref-2)
3. Consultora e especialista em Segurança da Informação. E-mail: carla.elaine@gmail.com [↑](#footnote-ref-3)
4. Disponível em: <https://support.google.com/googleplay/answer/9057338>. Acesso em 15 Dez. 2020. [↑](#footnote-ref-4)
5. Notícias mais relevantes coletadas na ferramenta Google, na categoria Notícias, em 20 nov. 2020, para as palavras-chave “golpe do falso motoboy” e “golpe do funcionário falso”. [↑](#footnote-ref-5)
6. Mensagens recebidas pelas autoras. [↑](#footnote-ref-6)
7. Disponível em: <https://www.itau.com.br/seguranca/privacidade>. Acesso em 06 dez. 2020. [↑](#footnote-ref-7)
8. Disponível em: <https://www.itau.com.br/seguranca/itoken/>. Acesso em 06 Dez 2020. [↑](#footnote-ref-8)
9. Disponível em: <https://www.itau.com.br/pix/>. Acesso em 06 dez. 2020. [↑](#footnote-ref-9)
10. Disponível em: <https://www.youtube.com/channel/UC0yw39DOcCOwyUj2uY8vbuA>. Acesso em 06 Dez 2020. [↑](#footnote-ref-10)
11. Dados coletados em 06 dez. 2020. [↑](#footnote-ref-11)
12. Disponível em <http://jornaldamanhamarilia.com.br/exibe.php?id=24219> e em <https://www.tudocelular.com/seguranca/noticias/n164754/nova-onda-golpes-boleto-atinge-clientes-claro.html>. Acesso em 09. Dez. 2020. [↑](#footnote-ref-12)
13. Acesso em: <https://olhardigital.com.br/2019/11/14/noticias/exclusivo-falha-de-seguranca-da-claro-expoe-dados-de-8-milhoes-de-usuarios/>. Disponível em 15 jan. 2020. [↑](#footnote-ref-13)
14. Acesso em: <https://www.istoedinheiro.com.br/hackers-podem-ter-roubado-dados-de-278-milhoes-de-clientes-claro-net-no-brasil/> . Disponível em 15 dez. 2020. [↑](#footnote-ref-14)
15. Disponível em: <https://www.reclameaqui.com.br/empresa/claro/>. Acesso em 15 Dez 2020. [↑](#footnote-ref-15)
16. Pesquisa realizada dia 15 Dez. 2020, às 15:15. Ressalta-se que esta ferramenta retorna os resultados considerados mais relevantes, segundo as suas políticas. Foram retornados 806 resultados. [↑](#footnote-ref-16)
17. Os extratos apresentados são públicos, não apresentam dados pessoais e não estão transcritos em sua integridade, embora sejam indicados os links dos mesmos. [↑](#footnote-ref-17)
18. Disponível em: <https://www.reclameaqui.com.br/claro-tv/boleto-falso-fatura-minha-net_LL-q5GIgu8TmOdSL/> . Acesso em 15 Dez 2020. [↑](#footnote-ref-18)
19. Disponível em: <https://www.reclameaqui.com.br/net-tv-banda-larga-e-telefone/boleto-da-net-claro-falso-mais-com-dados-verdadeiro-do-cliente_5Pn8wMZd_pbpAIVS/> . Acesso em 15 Dez 2020. [↑](#footnote-ref-19)
20. Disponível em: <https://www.reclameaqui.com.br/claro/boleto-claro-net-falso-com-desconto_GrPmDiXwLpWidDqO/> . Acesso em: 15 dez. 2020. [↑](#footnote-ref-20)
21. Disponível em: <https://www.reclameaqui.com.br/net-tv-banda-larga-e-telefone/boleto-falso-net_To4-ZYOF6EdFrQv7/> . Acesso em: 15 dez. 2020. [↑](#footnote-ref-21)