Ilícitos de dados, fraudes e responsabilidade civil

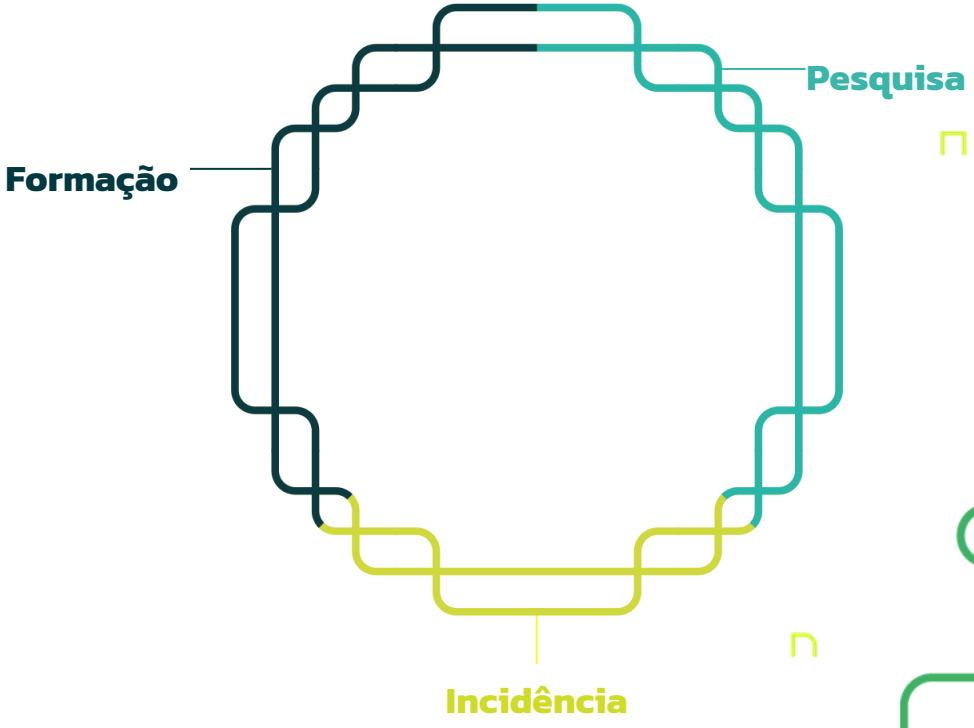
Rafael A. F. Zanatta
17.03.2026

DataPrivacyBR Research

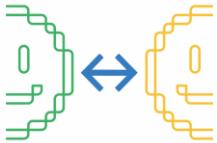
A missão da Data

Nossa missão é promover **direitos fundamentais e valores enraizados na justiça social diante de tecnologias emergentes e processos de datificação**. Navegando a dinâmica global-local e ancorada em uma estratégia em rede, a Data busca formar e disseminar conhecimento para um **ecossistema informacional justo**.

O que é a Data Privacy Brasil?



Princípios basilares

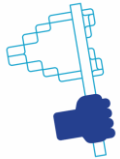


Colaboração: entre times e equipes, e entre atores do campo

Diversidade: de pessoas e modelos de pensamento e cultura

Transparência: na abertura dos nossos dados, pesquisas, referências

Dialogicidade: nas tomadas de decisão, na escuta e fala, na construção em conjunto



Pioneirismo: na identificação de tendências e empreendedorismo do campo

Impacto da formação

- Proteção de dados pessoais para **Defensores Públicos do Rio de Janeiro, São Paulo e Bahia** (2021, 2022 e 2023)

- Privacidade e Proteção de Dados Pessoais para servidores da **Agência Nacional de Proteção de Dados Pessoais** (2025)

- Proteção de dados e direitos dos consumidores para membros do **Sistema Nacional de Defesa do Consumidor** (2025)

- Governança de dados e proteção de dados para **Ministério da Gestão e Inovação** (2026)

Rafael Zanatta

Codiretor da Data Privacy Brasil. Pesquisador de pós-doutorado do Departamento de Filosofia e Teoria Geral do Direito da Faculdade de Direito da Universidade de São Paulo. Doutor pelo Instituto de Energia e Ambiente da Universidade de São Paulo, com formação no Instituto de Direito da Informação da Universidade de Amsterdam.
Mestre pela Faculdade de Direito da Universidade de São Paulo e mestre em direito e economia pela Universidade de Turim (LLM). Participou da elaboração da lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) e tem atuado nos debates sobre a Lei de Inteligência Artificial (PL 2338/2023).

Coordenou o programa de direitos digitais do Idec (2015-2018) e participou do Grupo de Trabalho de Tecnologia e Consumo do Ministério da Justiça (2015-2016)

O quão grave é o problema das fraudes?

DEFENSORIA PÚBLICA
DE MATO GROSSO DO SUL

PRENSA INTRANET CONCURSOS

PLANTÃO

o Institucional

nstância

Instância

es

a Digital

Atenção - Inf

Senhores Forn a solicitação do Informe de Rendimentos
2025) deverá s nte pelo e-mail: **financeiro-dpge@defen**

Campo Grande,

ATENÇÃO!

CUIDADO COM O Ggolpe NO WHAT'S!

A Defensoria Pública **NÃO COBRA NENHUM VALOR** para te atender.

NOSSOS SERVIÇOS SÃO TOTALMENTE GRATUITOS!

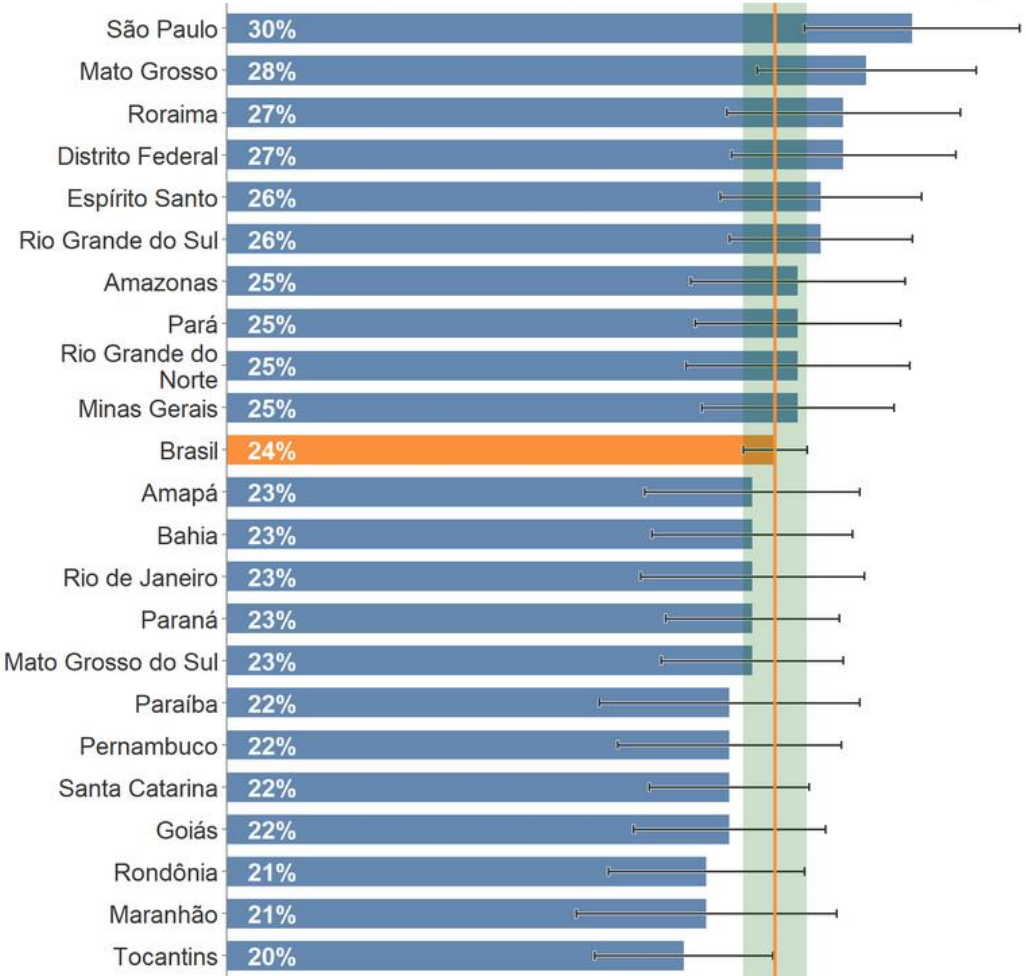
DEFENSORIA PÚBLICA
DE MATO GROSSO DO SUL

O tamanho do problema

- O quadro geral é de forte expansão dos golpes e fraudes, especialmente os digitais. O melhor indicador sintético é o estelionato: o Brasil registrou 1.819.409 casos em 2022; 1.965.353 em 2023; e **2.166.552 em 2024**. No dado mais recente, isso equivale a cerca de quatro golpes por minuto no país.

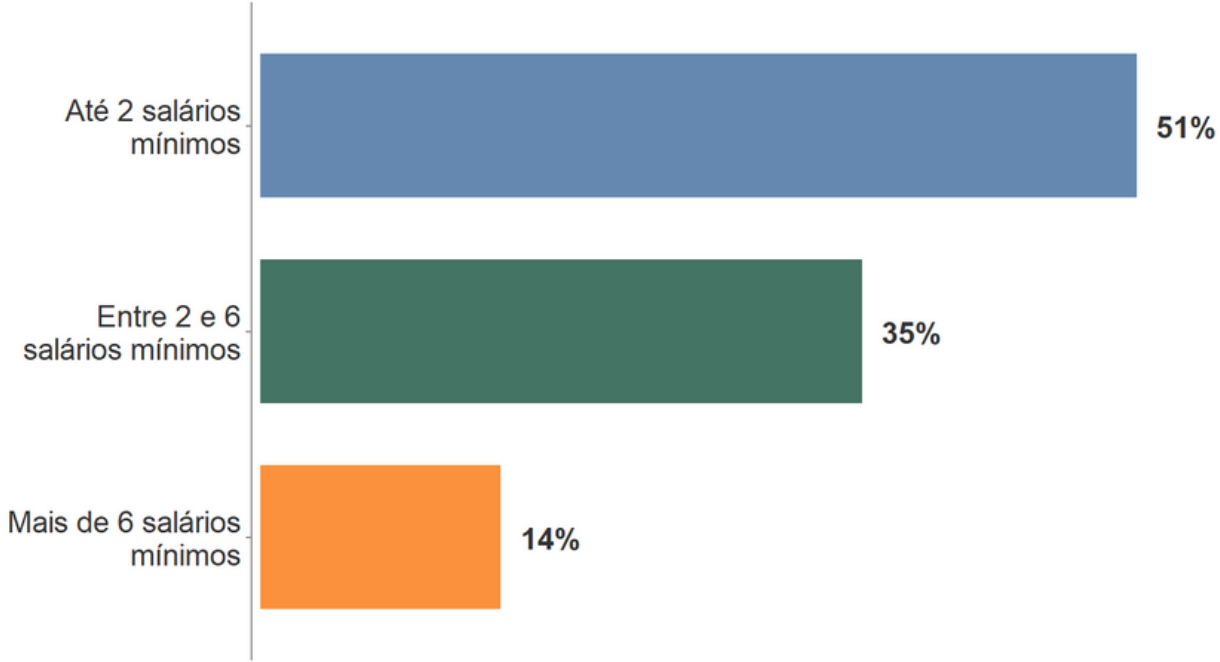
- O DataSenado apurou que 24% dos brasileiros com 16 anos ou mais relataram ter perdido dinheiro em golpes digitais no último ano, o que foi estimado em mais **de 40 milhões de pessoas**.

"Distribuição da população que, nos últimos 12 meses, perdeu dinheiro por algum crime digital como clonagem de cartão, fraude na internet ou invasão de contas bancárias em cada unidade da Federação" - Brasil - 2024



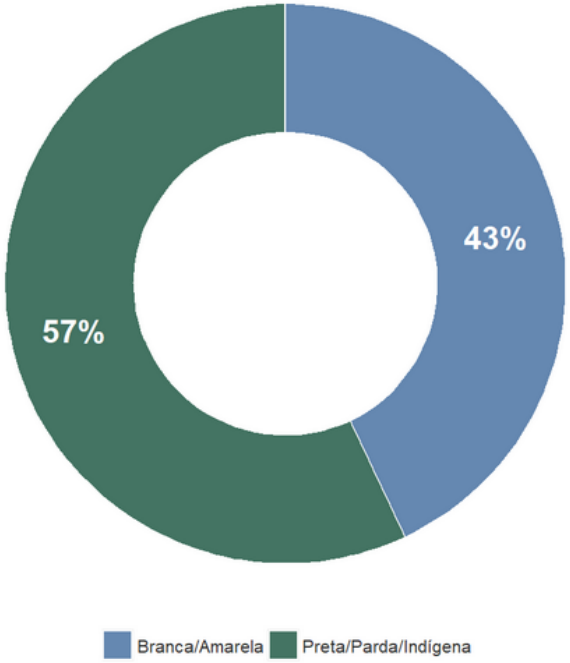
Fonte: Data Senado (2025)

"Distribuição da população que perdeu dinheiro por algum crime digital como clonagem de cartão, fraude na internet ou invasão de contas bancárias por Renda familiar em salários mínimos" - Brasil - 2024



Fonte: Instituto de Pesquisa DataSenado - coleta de 5 a 28.6.2024.
Nota: Distribuição referente aos 24% da população que declararam ter perdido dinheiro por algum crime digital como clonagem de cartão, fraude na internet ou invasão de contas bancárias.

"Distribuição da população que perdeu dinheiro por algum crime digital como clonagem de cartão, fraude na internet ou invasão de contas bancárias por Cor/raça" - Brasil - 2024



Fonte: Instituto de Pesquisa DataSenado - coleta de 5 a 28.6.2024.
Nota: Distribuição referente aos 24% da população que declararam ter perdido dinheiro por algum crime digital como clonagem de cartão, fraude na internet ou invasão de contas bancárias.

O tamanho do problema

- Relatório Febraban 2024: os três tipos mais frequentes foram golpe do WhatsApp, falsas vendas e falsa central/falso funcionário de banco

- Relatório Febraban 2025: quase **4 em cada 10 brasileiros** já sofreram golpe, e que esse é o maior patamar da série

- Lançamento da Aliança Nacional Contra a Fraude (2025) pelo MJSP/Febraban e pouca articulação com o campo da proteção de dados pessoais (ANPD) e sistema de justiça

Estelionatos no Brasil mais que quadruplicam em cinco anos, e golpes virtuais disparam após pandemia, revela Anuário

De acordo com dados do Anuário Brasileiro de Segurança Pública 2023, em 2022, foram 151,6 mil casos por mês ou 208 golpes por hora.

Por Gustavo Honório, Arthur Stabile e Deslange Paiva, g1 SP — São Paulo
20/07/2023 10h00 · Atualizado há um ano

Tentativas de fraude no e-commerce brasileiro sobem 66% em agosto, diz pesquisa

Tíquete médio dos golpes caiu 59% em comparação com o mesmo período de 2023

Mateus Cerqueira, do Estadão Conteúdo
20/09/2024 às 15:02 | Atualizado 20/09/2024 às 15:02

Brasil projeta maior crescimento em fraudes no mundo e perdas com golpes do Pix podem chegar a R$ 11 bilhões até 2028, aponta relatório

Nova edição do Relatório Scamscope, desenvolvido pela ACI Worldwide em parceria com a GlobalData, volta a analisar os seis principais mercados de pagamentos em tempo real do mundo: Brasil, Estados Unidos, Reino Unido, Índia, Austrália e Emirados Árabes Unidos

Somando os seis países, prejuízo com fraudes de pagamentos em tempo real é estimado em mais de US$ 7,6 bilhões (mais de R$ 44 bilhões) até 2028

Uma em cada quatro vítimas de golpe afirma que abandonará a sua instituição financeira atual, expondo a necessidade de as organizações protegerem os clientes e preservarem a confiança

January 22, 2025 10:01 PM Eastern Standard Time

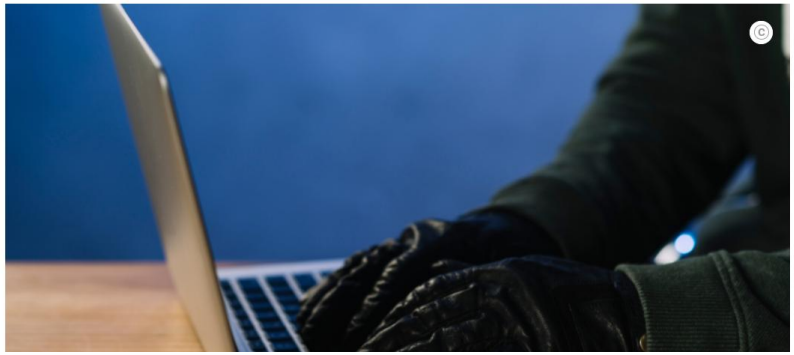
SÃO PAULO--(BUSINESS WIRE)--Com um ecossistema de pagamentos em tempo real acelerado pela adoção do Pix, o Brasil projeta o maior crescimento em fraudes de pagamentos em tempo real no mundo. Assim, as perdas com o golpe do Pix, termo adotado no país, podem chegar a US$ 1,937 bilhão (cerca de R$ 11 bilhões) até 2028. Os dados são do mais recente relatório Scamscope, desenvolvido pela ACI Worldwide (NASDAQ: ACIW), empresa de inovação em pagamentos globais, em parceria com a GlobalData, companhia especializada em análise e dados mundiais.

poder brasil

PODER 360

Golpes digitais crescem 45% em 2024, diz associação

Crescimento de fraudes digitais em 2024 é impulsionado pela evolução de técnicas criminosas, incluindo o uso de IA



e | investidor
ESTADÃO

Notícias | Mercado | Investimentos | Negócios | Educação Financeira | Criptor

Uma das principais ameaças atuais são as fraudes baseadas em deepfakes. Este tipo de golpe utiliza **tecnologias de Inteligência Artificial** para manipular rostos e vozes, criando vídeos ou áudios convincentes que podem enganar até mesmo profissionais experientes. Em 2023, o número de **deepfakes relacionados a fraudes** aumentou 31 vezes, segundo a Onfido – empresa especialista em verificação de identidade. O Brasil ocupa o topo do pódio dos casos na América Latina, com 49,6% das ocorrências.

Esse tipo de tecnologia é usada não apenas para fraudes em massa, mas também em golpes altamente direcionados. Um exemplo famoso é o de um CEO britânico que foi enganado por um áudio deepfake, acreditando estar em uma ligação com seu chefe. O resultado foi a transferência de mais de €200 mil para a conta de fraudadores.

A relação entre ilícitos de dados e fraudes

Os ilícitos de dados estão na raiz do problema

- Nos últimos anos, o Brasil tem enfrentado uma **explosão de golpes e megavazamentos de dados pessoais**, muitos deles sem solução, como o “vazamento do fim do mundo” denunciado pela Tecmundo em 2021

- A Agência Nacional de Proteção de Dados tem fiscalizado casos envolvendo Ministério da Saúde e DataPrev. Há vazamentos de grandes proporções que afetam os brasileiros e violação sistemática do direito fundamental à proteção de dados pessoais

MAIORES VAZAMENTOS DE DADOS NO BRASIL

CONSEQÜÊNCIAS

- Golpes Financeiros
- Fraudes e Estelionato
- Assédio a Idosos

PANORAMA GERAL

- **2,8 Bilhões** de Registros Vazados
- **Alta Incidência** no Brasil

A relação entre ilícitos de dados e fraudes

- Hoje, golpes não dependem mais de força ou acesso físico, mas de **dados pessoais, perfis de comportamento e informações financeiras**

- Quando há vazamentos massivos (como CPF, renda, benefícios do INSS), criminosos passam a ter: (i) identidade completa da vítima, (ii) **capacidade de simular confiança**, (iii) base para automatizar golpes

Infraestrutura dos Ilícitos de Dados e Automação da Engenharia Social

Metadados e fraudes

- Há, também, uma quantidade gigantesca de dados que são **retirados de nós (dados retirados dos dispositivos)**
- **Metadados** são dados sobre dados. Eles não são o conteúdo principal da informação, mas descrevem características dela, como:
  - Quem criou ou enviou (autor, emissor, receptor);
  - Quando (data e hora);
  - Onde (localização, endereço IP, coordenadas de GPS);
  - Como (tipo de dispositivo, sistema operacional, formato do arquivo)

O quanto produzimos de metadados?

- Uma pessoa produz, em média, **10 megabytes de metadados (dados pessoais passivos) por dia**
- Em um mês, essa quantia é de 300 megabytes
- Em um ano, são 3,65 gigabytes
- Em cinco anos, são 18 gigabytes de metadados
    - Em um modelo simplificado de 2 kb por página de texto puro (“plain text” - codificado em UTF-8), esse armazenamento representa 9 milhões de páginas de texto puro
        - É três vezes mais que o acervo de livros da Biblioteca Nacional
        - Empilhadas, essas páginas teriam 957 metros de altura

O que são dados pessoais?

Tipo de dado	*O que é*	*Exemplos*	*Controle do titular*	*Valor para negócios*
Fornecidos	Informações entregues **diretamente** pela pessoa	Nome, CPF, e-mail, telefone, foto de perfil	Alto: a pessoa decide o que informar	Básico: necessários para cadastro e autenticação
Observados	Dados **registrados automaticamente** pelo uso de serviços ou dispositivos	Localização via GPS, histórico de navegação, tempo de uso de apps, endereço IP	Médio: a coleta ocorre em segundo plano, com pouca consciência do usuário	Alto: revelam hábitos e rotinas
Inferidos	Informações **criadas a partir da análise** dos dados fornecidos e observados	Perfil de consumo, preferências políticas, saúde provável, risco de crédito, orientação sexual	Baixíssimo: o usuário não sabe o que é inferido nem pode revisar ou corrigir	Muito alto: permitem personalização, segmentação e previsão de comportamento

Uma distinção: fraudes com base em anúncios

Dados inferidos

- Além de dados pessoais cadastrais e dados de aplicações (metadados), uma categoria de dado pessoal que pode ser usada em fraudes é a de **dados inferidos**
  - São informações deduzidas ou criadas a partir de outros dados coletados.
  - Diferem dos dados fornecidos diretamente (ex.: nome, e-mail) ou observados automaticamente (ex.: geolocalização, histórico de navegação).
  - Nos dados inferidos, **algoritmos e análises estatísticas produzem novas informações sobre a pessoa**.

Dados inferidos

- Personalização e segmentação:
  - Empresas usam inferências para criar perfis detalhados e oferecer anúncios, produtos e serviços sob medida.
  - Exemplo: **anúncios direcionados no Instagram** ou YouTube

- Previsão de comportamento:
  - Modelos de negócio baseados em dados **buscam prever o que o usuário vai querer, comprar ou fazer**

Perfilamento e golpes

Como as redes sociais da Meta se tornaram uma plataforma para golpes de investimento

Vídeos deepfake, perfis falsos no Instagram e Facebook, conversas privadas no WhatsAp como as plataformas de mídia social de Mark Zuckerberg se tornaram o principal meio utilizado para golpistas de investimentos.

Alanna Titterington

Características da fraude com perfilamento

- A fraude depende de:

🎯 segmentação comportamental

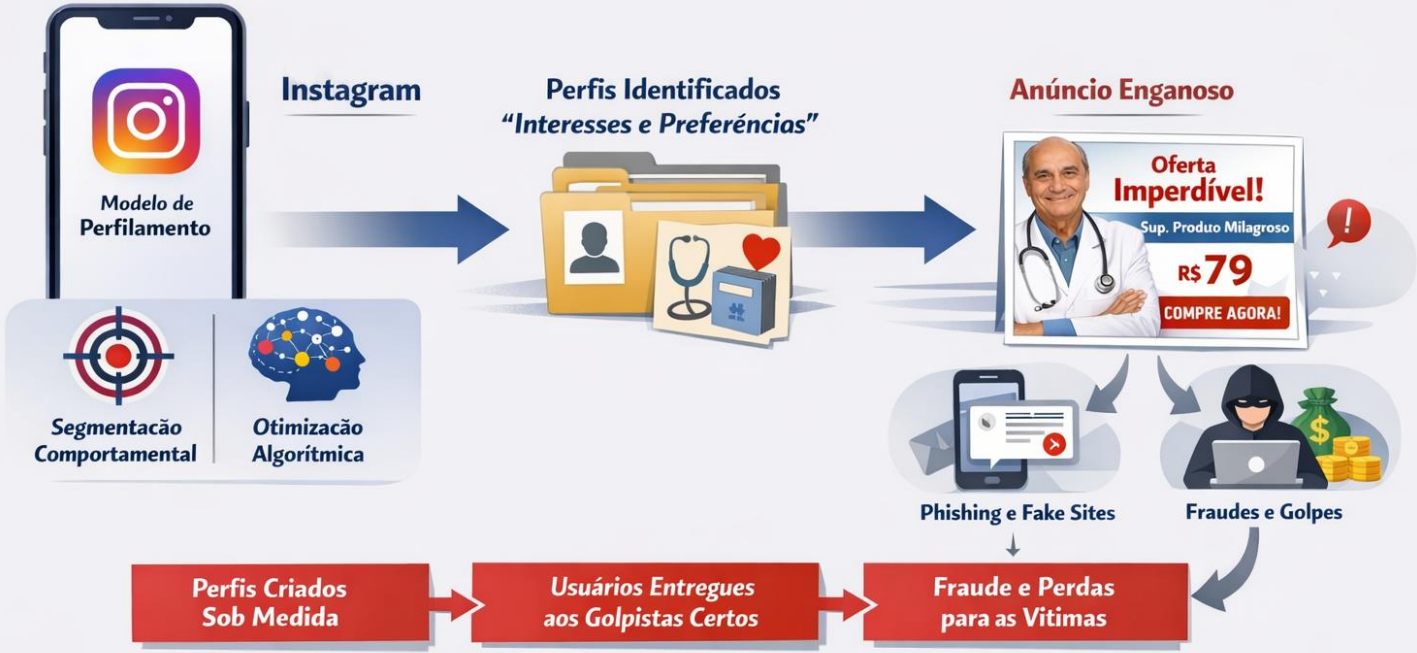
📊 inferências sobre preferências

⚙️ otimização algorítmica

- Isso transforma o modelo da plataforma em condição estrutural do dano? O perfilamento viabiliza economicamente o golpe? O sistema de anúncios é defeituoso porque potencializa fraudes previsíveis sem mitigação adequada?

O **Nexo Causal** Entre o **Modelo** de **Perfilamento** do **Instagram** e os **Golpes** de **Anúncios**

*De como os **fraudadores** chegam até as vítimas certas*



Do **Algoritmo** ao **Golpe:** *O Perfilamento como Instrumento da **Fraude***

A violação sistemática da Lei Geral de Proteção de Dados

Três premissas básicas

- A proteção de dados pessoais é um **direito fundamental** assegurado na Constituição Federal e em legislação federal (**Lei Geral de Proteção de Dados Pessoais - Lei 13.709/2018**)

- Todo brasileiro **possui titularidade sobre seus dados pessoais** (art. 17, LGPD) e todo tratamento deve respeitar a boa-fé e os princípios para tratamento de dados pessoais

- Os controladores devem se empenhar para tratar os dados pessoais de forma **lícita, leal e justa**

Para quê serve a LGPD?

- Define os conceitos fundamentais sobre o que é “dado pessoal”, o que é “tratamento”, quais são os “agentes de tratamento” e os princípios e regras aplicáveis

- Estipula que todo controlador deve, **de antemão**, demonstrar que está amparado por lei para realizar o tratamento (o que chamamos de “base legal”)
    - É como o regramento ambiental e a aviação civil
    - **Cultura preventiva** (prevenção e redução de danos)

Lei 13.709/2018

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;

Lei 13.709/2018

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.

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, **acerca dos instrumentos de tutela individual e coletiva**.

Lei 13.709/2018

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação **ou quando não fornecer a segurança que o titular dele pode esperar**, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, **der causa ao dano**.

Tratamento irregular e segurança esperada

- O Superior Tribunal de Justiça tem decidido diversos casos sobre fraudes e interpretação sistemática do art. 44 da LGPD. Afinal, o que é a segurança que o titular pode esperar? No que consiste essa obrigação jurídica? E o que ocorre quando dados que estavam sob custódia de uma organização passam a ser utilizados para golpes e fraudes?

- Relação intrínseca com o direito do consumidor e os princípios que regem o direito do consumidor com relação à máxima proteção dos consumidores e garantia da segurança

A responsabilidade civil pelo uso de dados pessoais em fraudes

Responsabilidade civil e LGPD no STJ

- **Tema Repetitivo 466/STJ** e **Súmula 479/STJ**: “As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias”

- "Se comprovada a hipótese de vazamento de dados da instituição financeira, será dela, em regra, **a responsabilidade pela reparação integral de eventuais danos**. Do contrário, inexistindo **elementos objetivos que comprovem esse nexo causal**, não há que se falar em responsabilidade das instituições financeiras pelo vazamento de dados utilizados por estelionatários para a aplicação de golpes de engenharia social (REsp 2.015.732/SP, julgado em 20/6/2023, DJe de 26/6/2023).

Responsabilidade civil e LGPD no STJ

- **Tese firmada por Nancy Andrighi** (RESP nº. 2.077.278-SP, Caso Daniela Ramos vs BV Financeira)**:** Para sustentar o nexo causal entre a atuação dos estelionatários e o vazamento de dados pessoais pelo responsável por seu tratamento, é imprescindível perquirir, com exatidão, quais dados estavam em poder dos criminosos, **a fim de examinar a origem de eventual vazamento e, consequentemente, a responsabilidade dos agentes respectivos**. Os nexos de causalidade e imputação, portanto, dependem da hipótese concretamente analisada.

Caso Daniela Ramos vs BV Financeira

boleto", limitando-se a defesa apresentada a tentar excluir a responsabilidade das instituições bancárias pelo ocorrido.

As alegações não merecem guarida.

Não é razoável esperar que a autora saiba os códigos correspondentes a cada banco para perceber a divergência entre o nome do banco emitente e do banco indicado no código de barras. [...]

A ré não aponta qualquer aspecto na conduta do autor que estivesse em desacordo com as regras e orientações fornecidas para utilização do sistema, limitando-se a levantar hipótese de culpa de terceiro, sem trazer qualquer elemento que fundamentasse o legado.

Ora, utilizando-se a ré de meios eletrônicos para prestação de serviços aos seus clientes, deve adotar todas as medidas cabíveis para garantir a segurança do sistema e dos serviços prestados, respondendo em caso de falha na prestação de serviços.

Não é de se esperar que o consumidor memorize todos os números identificadores dos diversos bancos a fim de perceber eventual discrepância entre o logo e o código do banco emissor do documento." (e-STJ fls. 136-137)

26. O Tribunal de Justiça do Estado de São Paulo, por maioria, reformou a sentença, afastando a responsabilidade da instituição financeira ante a culpa exclusiva da vítima, *in verbis*:

> "Trata-se de hipótese de culpa exclusiva do terceiro estelionatário e da própria parte autora apelante, o que afasta a responsabilidade do fornecedor de serviços, nos termos do artigo 14, §3º, II, do Código de Defesa do Consumidor.
>
> Verifica-se inicialmente que a conversa por *whatsapp* que ela diz ter mantido com o canal oficial da BV Financeira foi, na verdade, mantida com a "VB Financeira Fit Financiamento", conforme se vê a fls.49/50, em que a autora forneceu seus dados pessoais. Nessa conversa, a requerente inclusive questionou o motivo do pagamento ser feito à "Zap Pay" e não à credora BV, o que lhe permitia saber tratar-se de golpe.
>
> Por outro lado, o boleto de fls.54, recebido pela autora, era do Banco Bradesco, e não do Banco Votarantim, como as parcelas previamente pagas. Ademais, esse boleto indica um número errado de contrato (12**********), quando, na verdade, o contrato tinha número 511321854 (fls.36).
>
> Por fim, o pagamento foi feito em favor de ZapPay, e não à BV, conforme demonstrado pelo comprovante de pagamento de fls.55.
>
> Todos esses fatos tornavam muito suspeita a operação e, como dito, permitia que a autora, se tivesse agido com a cautela que se espera do homem médio, percebesse o golpe, o qual só foi possível por sua própria incúria,

Caso Daniela Ramos vs BV Financeira

- **STJ, RESP nº. 2.077.278-SP:** A prestação do serviço de qualidade pelos **fornecedores abrange o dever de segurança**, que, por sua vez, engloba tanto a integridade psicofísica do consumidor, quanto sua integridade patrimonial. Note-se que o art. 8º do CDC admite que se coloquem no mercado **apenas produtos e serviços que ofereçam riscos razoáveis e previsíveis,** isto é, que não sejam excessivos ou potencializados por falhas na atividade econômica desenvolvida pelo fornecedor

- Especificamente nos casos de golpes de engenharia social, não se pode olvidar que os **criminosos são conhecedores de dados pessoais das vítimas**, valendo-se dessas informações para convencê-las, por meio de técnicas psicológicas de persuasão – como a semelhança com o atendimento bancário verdadeiro –, a fim de atingir seu objetivo ilícito

Caso Daniela Ramos vs BV Financeira

- **STJ, RESP nº. 2.077.278-SP:** Os dados sobre operações bancárias são, em regra, de tratamento exclusivo pelas instituições financeiras. No ponto, a Lei Complementar 105/2001 estabelece que as instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados (artigo 1º), **constituindo dever jurídico dessas entidades não revelar informações que venham a obter em razão de sua atividade profissional**, salvo em situações excepcionais. Desse modo, seu armazenamento de maneira inadequada, a possibilitar que terceiros tenham conhecimento de informações sigilosas e causem prejuízos ao consumidor, **configura defeito na prestação do serviço** (artigo 14 do CDC e artigo 44 da LGPD)

RESP nº. 2.077.278–SP

- **STJ, RESP nº. 2.077.278-SP:** O tratamento indevido de dados pessoais bancários **configura defeito na prestação de serviço**, notadamente quando tais informações são utilizadas por estelionatário para facilitar a aplicação de golpe em desfavor do consumidor.

- Será possível utilizar o precedente “Daniela Ramos vs BV Financeira” (STJ, 2023) em outros casos semelhantes, que não envolvem instituições financeiras, em casos de ilícitos de dados e fraudes?

- Tese forte sobre **fortuito interno**: evento danoso que ocorre dentro do risco da atividade e está ligado ao funcionamento do serviço. Não exclui a responsabilidade civil. A fraude com uso de dados não é evento externo. O tratamento é interno e a proteção é obrigação da instituição

Caso Ananda Martins vs Facebook (2024)

- **Invasão de rede social – fortuito interno – responsabilidade civil**: A invasão da rede social do usuário do serviço configura fortuito interno, inerente ao risco da atividade desenvolvida pelo seu provedor, de modo que está configurada a falha na prestação do serviço ao não dotar seus sistemas com a segurança tecnológica necessária a impedir sua violação por fraudadores, além de ter ficado inerte na solução administrativa do problema, com o fim obstar as ações do estelionatário. Inaplicável, portanto, a excludente prevista no art. 14, § 3º, CDC."

- TJDFT, Acórdão 1890017, 0774228-79.2023.8.07.0016, Relator(a): RITA DE CÁSSIA DE CERQUEIRA LIMA ROCHA, PRIMEIRA TURMA RECURSAL, data de julgamento: 12/07/2024, publicado no DJe: 25/07/2024.

Caso Ananda Martins vs Facebook (2024)

- Verifica-se que o perfil do Instagram de um amigo próximo da recorrida foi invadido, ocasião em que o **estelionatário se passou pelo titular da conta e aplicou um golpe contra a recorrida**, a qual realizou transferências bancárias acreditando que se tratava de um investimento financeiro. (...) Por outro lado, **faltou à recorrida a diligência necessária para desconfiar da oferta de investimento com ganho bem superior ao usualmente praticado**, sobretudo porque a recorrida é pessoa instruída, e, assim, teria maior discernimento para identificar tais fraudes. Configurada a culpa concorrente para consolidação da fraude, o prejuízo deverá ser repartido entre partes (art. 945 do Código Civil). Precedente desta Turma Recursal: Acórdão 1825223 (TJDFT, Acórdão 1890017, 0774228-79.2023.8.07.0016)

Caso Pedro Camiloti vs Prudential (2025)

- **STJ, RESP nº. 2.121.904-SP**: Em contrato de seguro de vida, deve-se empreender um rigoroso esforço para a proteção dos dados pessoais, já que, para sua celebração, a seguradora, para a avaliação dos riscos**, recebe dados sensíveis sobre aspectos pessoais, familiares, financeiros e de saúde do segurado**.

- O vazamento de dados pessoais sensíveis fornecidos para a contratação de seguro de vida, por si só, **submete o consumidor a riscos em diversos aspectos de sua vida**, como em sua honra, imagem, intimidade, patrimônio, integridade física e segurança pessoal.

Caso Pedro Camiloti vs Prudential (2025)

- **STJ, RESP nº. 2.121.904-SP**: O art. 44 da LGPD, à semelhança do art. 14, § 1º, do CDC, estabelece que o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, considerados o modo pelo qual é realizado, o resultado e os riscos que razoavelmente dele se esperam, as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado, entre outras circunstâncias.

- "A disponibilização indevida de dados pessoais pelos bancos de dados para terceiros caracteriza dano moral presumido (in re ipsa) ao cadastrado titular dos dados, diante, sobretudo, da **forte sensação de insegurança por ele experimentada**" (REsp 2.115.461/SP, Terceira Turma, DJe 14/10/2024).

Caso Pedro Camiloti vs Prudential (2025)

- **STJ, RESP nº. 2.121.904-SP:** Nesse contexto, o quadro fático-probatório delineado pelas instâncias ordinárias indica que, no contexto de um contrato de seguro de vida: i) houve vazamento de dados pessoais do consumidor; ii) tais dados são classificados como sensíveis, de modo a abranger informações fiscais, bancárias e sobre a saúde do consumidor; iii) há nexo de causalidade entre o vazamento de dados sensíveis do consumidor e falhas na prestação do serviço pela recorrente, que não atendeu a seu dever de garantir a proteção dos dados sensíveis do consumido. O vazamento de dados pessoais sensíveis fornecidos para a contratação de seguro de vida, **por si só, submete o consumidor a riscos de diversas ordens**.

Conclusões e questões em aberto

CDC e LGPD

- Em diversos precedentes do STJ, há um diálogo frutífero entre o Código de Defesa do Consumidor e a Lei Geral de Proteção de Dados Pessoais, com relação ao regime de responsabilidade civil e as falhas no dever de segurança, combinando os artigos 42, 44 e 46 da LGPD com os artigos 4º e 14 do CDC

- A explosão de golpes e fraudes tem atacado pessoas de baixa renda, produzindo uma relação de aprofundamento das assimetrias e desigualdades no Brasil, o que merece atenção das Defensorias Públicas no Brasil

CDC e LGPD

- Golpes que envolvem dados pessoais de pessoas naturais que estão sob custódia de instituições financeiras já possuem uma definição jurídica clara, no sentido de reconhecimento de dever de indenização em razão da falha no dever de segurança e a existência do fortuito interno (Tema 466, STJ e STJ, RESP nº. 2.077.278-SP)

- Golpes de envolvem a invasão de dispositivos e contas de redes sociais (Instagram) para aplicação de fraudes de investimentos são mais complexos, porém as Cortes já reconhecem culpa concorrente e violação dos deveres de segurança nas relações de consumo

- Golpes e fraudes que envolvem a obtenção de vantagem a partir do perfilamento feito pelas redes sociais ainda não foram analisados pelas Cortes, mas podem ser vistos de um ponto de vista estrutural na produção do dano

Recomendações para Defensores Públicos

Recomendações

- Narrativas iniciais (petições) devem: (i) descrever o ecossistema do golpe, e (ii) demonstrar previsibilidade e repetição. Usar linguagem de: risco da atividade, defeito do serviço e cadeia de tratamento de dados

- Sempre estruturar a peça com dupla fundamentação. **CDC**: art. 14 → responsabilidade objetiva, art. 4º → vulnerabilidade. **LGPD**: art. 44 → tratamento irregular, art. 46 → dever de segurança

- Usar o conceito de fortuito interno de forma ofensiva. Não só como defesa, mas como tese estruturante. Explorar a tese do **risco inerente na atividade econômica** baseada em dados

Recomendações

- Consolidar precedentes em fraudes bancárias como “porta de entrada”. Usar os casos bancários como âncora jurisprudencial e como modelo de raciocínio jurídico. Priorizar as populações vulneráveis e transformar isso em **estratégia institucional**. Enfoque em idosos, beneficiários do INSS e população de baixa renda!

- No caso de golpes via anúncios, as teses mais promissoras sobre defeito na prestação do serviço dizem respeito a ausência de controle de anunciantes e falha de verificação. O sistema de perfilamento atua como mecanismo de identificação e entrega de vítimas, produzindo nexo estrutural.

- Os golpes não são eventos isolados, são sintomas de **uma falha sistêmica na proteção de dados.** E enfrentar essa falha é uma tarefa central das Defensorias Públicas.

Contatos

zanatta@dataprivacybr.org