MANUAL DO CIDADÃO 2025

EDITORA IMPÉRIO

APOIO:


HACK3R_
RANGER5


privacy tools


OAB
PERNAMBUCO


nv
seguros
digitais


EDITORA
IMPÉRIO


ABCCRIM
ACADEMIA BRASILEIRA DE CIÊNCIAS CRIMINAIS

MANUAL DO CIDADÃO 2025

Ana Paula Canto de Lima
Camilla Pinheiro Cianga
Carolina Margonari
Débora Gomes Galvão Basílio
Débora Leal Soares de Castro
Dionice de Almeida
Guilherme Peara Pereira Araújo
Louana Costa
Marison Souza
Rafael A. Carneiro de Castilho
Raniery Almeida
Vinícius Perallis

EDITORA IMPÉRIO

Direção Executiva: Eduardo Cavalcante de Almeida Costa
Direção Editorial: Ana Paula Moraes Canto de Lima
Conselho Editorial: Ana Paula Moraes Canto de Lima
Anne Cristine Silva Cabral
Cristiano Carrilho Silveira Medeiros
Ingrid Zanella Andrade Campos
Isabela Lessa de Azevedo Pinto Ribeiro
Maria Emília Miranda de Oliveira Queiroz

Capa: Coordenação

Projeto Gráfico e Diagramação: Editora Império

Revisão: Dos autores

Relacionamento com o cliente via WhatsApp: (81) 3203-6469

ISBN 978-65-89291-46-6

PREFÁCIO

Vivemos em um mundo cada vez mais digital e vimos iniciar uma revolução na maneira como a sociedade interage, consome e vive nesse ambiente. Nossas compras, conversas, pesquisas e até mesmo os trajetos que fazemos diariamente estão conectados a tecnologias que coletam e processam dados e informações sobre todos nós.

Com os avanços de novas tecnologias, que surgem quase todos os dias, a coleta, o armazenamento e qualquer outra operação feita com os dados pessoais se tornaram parte integrante das nossas rotinas. A cada clique na internet, a cada cadastro em uma rede social, a cada compra on-line, deixamos rastros digitais que podem ser utilizados para inúmeras finalidades. Enquanto navegamos por esse novo mundo virtual, surgem algumas dúvidas: quem usa e quem controla esses dados? E como podemos garantir que eles sejam utilizados de maneira correta?

Esses dados, conhecidos como dados pessoais, dizem respeito à nossa identidade, como nome, CPF, endereço, localização, hábitos de consumo, e também a dados mais sensíveis, como histórico de saúde, preferências políticas e aspectos da intimidade.

Você já parou para pensar sobre quem tem acesso a esses dados e que informações sobre nossas vidas obtém a partir deles?

Foi para proteger esses dados que foi aprovada a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil. A LGPD é uma conquista dos cidadãos brasileiros, elaborada para garantir que o uso dos nossos dados seja feito de forma válida, segura e com responsabilidade. Mais do que uma lei técnica para empresas e outras organizações públicas e privadas, a LGPD é um direito de todos nós, titulares de dados pessoais.

Por isso, este Manual do Cidadão foi pensado para você. Não importa se você entende pouco ou muito sobre Tecnologia ou Direito, o objetivo deste guia é explicar, de forma simples e prática, como

a LGPD funciona e, principalmente, como ela protege você no dia a dia.

Apesar de sua importância, a LGPD ainda é pouco compreendida por grande parte da população. Muitas pessoas não sabem quais são os seus direitos, como os seus dados e informações podem ser utilizados, ou mesmo a quem recorrer em caso de abuso ou de danos causados ao titular.

Por que a LGPD é importante para você?

Você já deve ter percebido que, nos últimos anos, muitas empresas começaram a pedir, além do cadastro de alguns dados pessoais, o seu consentimento para o tratamento de dados ao visitar os sites (na concordância ou não com os cookies, que coletam os seus dados), comprar seus produtos ou utilizar os serviços (inclusive o download de um aplicativo gratuito).

Isso acontece porque a LGPD exige que toda atividade feita com ou sobre os dados pessoais deve ocorrer de forma transparente, para finalidades específicas. Mas, afinal, o que são dados pessoais?

Dados pessoais são os dados que podem identificar você, pessoa natural ou física, ou possibilitar a sua identificação, direta ou indiretamente. Por exemplo, o seu nome, número de CPF, endereço, número de telefone ou de aplicativo de mensagens, endereço de e-mail, entre diversos outros, são considerados dados pessoais. A LGPD estabelece que você tem o direito de saber como esses dados são coletados, armazenados, utilizados e compartilhados por qualquer outra pessoa.

Para que isso ocorra, os chamados "agentes de tratamento" precisam ter o seu consentimento ou indicar alguma outra regra legal que os autorize a tratar os seus dados pessoais. Não bastasse isso, para assegurar o cumprimento dos seus direitos, todas as atividades feitas com seus dados pessoais precisam ser registradas. Como diria o "carimbador maluco" Raul Seixas: "Tem que ser selado, registrado, carimbado, avaliado, rotulado se quiser voar" (ou, para os dados pessoais, se quiser tratar).

Portanto, a proteção dos seus dados não é apenas um detalhe técnico, mas é um direito fundamental, previsto na Constituição brasileira desde fevereiro de 2022. Trata-se de garantir que ninguém use dados sobre você de maneira inadequada, discriminatória, ou de qualquer outra forma que não seja autorizada pela LGPD, que foi criada para que você possa ter mais segurança ao navegar na internet, realizar transações bancárias e até mesmo ao lidar com serviços presenciais que precisam de seus dados.

Conheça os seus direitos

Um dos principais objetivos da LGPD é assegurar que você tenha controle sobre os seus dados pessoais (o que é conhecido como "autodeterminação informativa"). Para isso, a lei contém uma série de direitos para proteger você.

Entre eles, estão os seguintes direitos:

- Direito de acesso: você tem o direito de saber quais dados pessoais são tratados por empresas, órgãos públicos e outras pessoas;

- Direito de retificação: se os seus dados estiverem incorretos em alguma base de dados, você pode solicitar que sejam corrigidos;

- Direito à exclusão: em algumas situações (salvo nos casos em que a LGPD prevê o dever de guarda), você pode exigir que seus dados pessoais sejam apagados ou excluídos de uma base de dados;

- Direito à portabilidade: permite que você transfira seus dados de uma empresa ou ente público para outro, mantendo o seu histórico e sem perder informações relevantes;

- Direito à informação: você tem o direito de ser informado sobre as finalidades específicas para as quais seus dados estão sendo utilizados;

- Direito de não ser submetido a decisões automatizadas: você pode contestar decisões que sejam tomadas exclusivamente com base em tratamento automatizado de dados pessoais, como as avaliações de crédito.

Esses direitos garantem que você tenha mais controle sobre quem pode acessar os seus dados e como eles podem ser utilizados (ou tratados, nos termos da lei).

Como a LGPD impacta o dia a dia das pessoas?

A LGPD não é uma lei restrita ao ambiente digital, que se aplica também ao meio físico e afeta diversas áreas do cotidiano.

Imagine que você precise fazer um exame médico e informar os seus dados em um laboratório, ou que contrate um serviço de internet e forneça alguns dados para o cadastro. Nesses casos, a LGPD assegura que seus dados sejam tratados de acordo com a lei e apenas para os fins previamente estabelecidos.

Além disso, você já deve ter ouvido falar em vazamentos de dados, casos em que os dados pessoais de milhares ou de milhões de pessoas foram expostos ou tratados indevidamente. A LGPD busca minimizar esses riscos, ao estabelecer regras claras sobre como os dados devem ser protegidos e ao exigir que as organizações adotem medidas de segurança eficazes e registrem as atividades que realizarem com os dados.

Outro aspecto importante é a transparência. A partir da LGPD, os agentes de tratamento precisam explicar de maneira clara e acessível como estão utilizando os dados pessoais que coletam. Isso significa que você pode exigir que as organizações sejam mais transparentes na prestação de informações sobre os seus dados pessoais.

Como ler este Manual do Cidadão?

O Manual do Cidadão foi pensado para ser um guia prático e de fácil consulta, com textos escritos por especialistas na área.

Ao abordar os conceitos básicos da LGPD, explicar os seus direitos e trazer exemplos práticos de como a lei pode ser aplicada em diferentes situações, você pode pesquisar diretamente o tema que lhe interessa, para se informar sobre os seus direitos e tomar as medidas cabíveis sempre que verificar que eles estão sendo desrespeitados.

O manual também inclui informações sobre a Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar e regulamentar o cumprimento da LGPD no Brasil. Saber a quem recorrer é um passo essencial para proteger seus direitos e garantir que as regras sejam cumpridas.

Porém, quando tiver dúvidas e precisar tomar alguma medida (administrativa ou judicial) contra um agente de tratamento de dados pessoais, consulte um advogado especialista no assunto, para ser orientado de forma específica para a sua situação.

Mensagem Final

A proteção de dados pessoais é um direito que afeta diretamente a qualidade da nossa vida, a segurança dos nossos dados e a liberdade que temos para navegar, consumir e interagir em ambientes físicos e digitais.

Com o avanço tecnológico, vários aspectos das nossas vidas se tornam cada vez mais digitais, tornando a LGPD ainda mais relevante. Por isso, conhecer a lei é um passo essencial para que possamos exercer nossa cidadania de maneira plena e consciente.

Espero que este Manual sirva como um ponto de partida para que você entenda melhor a importância da proteção dos seus dados e saiba como se proteger em um mundo cada vez mais conectado.

Oscar Valente Cardoso

Doutor em Direito (UFRGS), Mestre em Direito e Relações Internacionais (UFSC), Especialista em Direito Processual Civil, em Inteligência Artificial e em Ciência de Dados e Big Data Analytics, Coordenador do Comitê Gestor de Proteção de Dados do TRF4, Professor no Mestrado da Universidade Europeia de Lisboa, Juiz Federal.

SUMÁRIO

INTRODUÇÃO À LGPD: A IMPORTÂNCIA DA PRIVACIDADE E PROTEÇÃO DE DADOS NO MUNDO DIGITAL

Rafael A. Carneiro de Castilho[1]

1. INTRODUÇÃO

Imagine acordar em uma manhã e perceber diversas notificações de compras feitas no seu cartão, além da informação de novas contas bancárias abertas em seu nome com instituições que você nunca teve contato. Esse seria um longo dia, e tudo pode ter começado com um cadastro online aparentemente inofensivo. Parece distante? Não é.

Tudo isso ocorre quando pessoas mal-intencionadas tem acesso a informações pessoais relevantes sobre você, que pode ser apenas o CPF. Por esse motivo, a proteção de dados pessoais não é um tema fora da realidade ou distante da sua vida, está no seu dia a dia, e pode lhe trazer sérias consequências.

O conteúdo dessa cartilha serve exatamente para você compreender o que está em jogo, e não serve apenas para você, mas para todas as pessoas que fazem parte da sua convivência, pois conhecimento é poder.

2. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Para entendermos melhor o tema, é importante diferenciar os conceitos de privacidade e proteção de dados pessoais. A privacidade está relacionada à nossa intimidade, como aquilo que vivemos

1 Graduado pela Universidade para o Desenvolvimento do Estado e da Região do Pantanal (UNIDERP). Pós- Graduado em Direito Digital e Proteção de Dados pela Escola Brasileira de Direito (EBRADI). Extensão em Direito Imobiliário pela Fundação Getúlio Vargas (FGV). Extensão em Direito Processual Civil, pela Faculdade IBMEC São Paulo e o Instituto Damásio de Direito. Pós-Graduado LLM em Proteção de Dados, Brasil e Portugal, pela Fundação Escola Superior do Ministério Público (FMP) e Faculdade de Direito Universidade de Lisboa (CIDP). Advogado com atuação no Direito Imobiliário, Registral, Digital e Proteção de Dados.

dentro de casa e que é compartilhado apenas com pessoas do nosso círculo mais próximo, como familiares e amigos que frequentam nosso lar. Por outro lado, a proteção de dados pessoais refere-se às informações que identificam uma pessoa, como nome, RG e CPF. Embora esses dados possam ser de conhecimento público e não estejam diretamente vinculados à privacidade, eles, assim como a privacidade, devem ser protegidos e respeitados por lei. A privacidade é um conceito antigo e histórico, que vem sofrendo mudanças desde a Grécia Antiga, enquanto que a ideia de dados pessoais e a sua proteção, é mais recente, se desenvolvendo com a computação.

Agora você pode pensar o seguinte: tudo bem, mas como os dados pessoais se relacionam com a computação?

Os computadores são ferramentas excepcionais para o processamento de informações. Eles têm a capacidade de analisar e calcular milhões de dados em uma velocidade e com uma eficiência que seriam impossíveis de alcançar, mesmo com o esforço conjunto das mais de oito bilhões de pessoas que vivem na Terra hoje.

Essa capacidade foi se desenvolvendo ao longo das décadas, até chegarmos aos dias de hoje, em que contamos com ferramentas avançadas de inteligência artificial, capazes de criar praticamente qualquer coisa que se possa imaginar.

O ponto central aqui é o enorme poder de processamento de informações, no qual os dados pessoais desempenham um papel fundamental.

Nos Estados Unidos, entre as décadas de 60 e 70, grandes corporações começaram a usar computadores para processar grandes bases de dados pessoais para poder conhecer os seus consumidores de forma individual, isto é, criar um perfil de cada pessoa para saber mais da sua vida e seus hábitos para então oferecer produtos, ou então negá-los, como nos casos de crédito.

O uso indiscriminado de dados pessoais pelas corporações alcançou tamanha proporção que os legisladores norte-americanos decidiram criar leis para regulamentar o uso dessas informações e proteger a população, o que resultou em legislações como o *Fair*

Credit Reporting Act[2].

É importante destacar que essa questão já vem sendo tratada de forma específica em outros países há mais de 50 anos. No Brasil, porém, uma legislação dedicada ao tema só foi implementada em 2018, ou seja, há apenas sete anos, o que evidencia o atraso do país nesse aspecto.

Por isso, a proteção de dados pessoais é tão relevante nos dias de hoje. O poder computacional e as tecnologias de inteligência artificial permitem realizar uma infinidade de operações com poucas informações, sendo suficiente, em muitos casos, apenas o nome e o CPF.

3. A LEGISLAÇÃO E A PROTEÇÃO DO CIDADÃO

A legislação brasileira que regula o tratamento de dados pessoais é a Lei Geral de Proteção de Dados Pessoais (LGPD)[3]. Ela garante a todos os cidadãos o direito de que seus dados pessoais sejam tratados com responsabilidade e segurança.

Mas o que isso significa na prática? Significa que qualquer atividade realizada no Brasil envolvendo o tratamento de dados pessoais, desde profissionais autônomos que coletam informações de clientes para prestar serviços até grandes corporações, deve adotar medidas de segurança para proteger esses dados. Além disso, é fundamental que essas informações não sejam utilizadas de forma contrária à lei ou às expectativas do cidadão.

No caso de profissionais autônomos, as informações pessoais coletadas, como cópias de documentos em formato físico, devem ser armazenadas em locais seguros, com acesso restrito, como armários trancados, para evitar que terceiros não autorizados te-

2 Lei de Relatórios de Crédito Justos, em tradução livre: A legislação foi criada para regular o uso e a disseminação de crédito dos consumidores, de modo que os relatórios oriundos das informações processadas sejam precisas, justas e que respeitem os direitos dos consumidores.

3 Lei 13.709/18, Lei Geral de Proteção de Dados Pessoais (LGPD). Acessível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>.

nham acesso a elas. Quando os dados forem digitais, como fotos de documentos, é necessário armazená-los em computadores protegidos por antivírus, softwares atualizados e senhas de acesso.

Para empresas, os cuidados são semelhantes, mas incluem também o treinamento das equipes, garantindo que todos os colaboradores compreendam e sigam as práticas necessárias para proteger as informações no dia a dia.

Em ambos os casos, faz parte da proteção de dados pessoais garantir que esses agentes não compartilhem suas informações com terceiros desconhecidos, com os quais você nunca teve qualquer contato.

Antes da legislação, esse cenário era comum, especialmente com a venda de bases de dados. Funciona da seguinte forma: alguém obtinha uma planilha com nomes, números de contato, endereços e outras informações pessoais e as vendia para terceiros, que então utilizavam esses dados para oferecer produtos ou serviços diretamente a você. Já passou por essa situação? Pois bem, esse era o cenário, e infelizmente, ainda ocorre.

Essa legislação, contudo, não se aplica apenas a prestadores de serviços privados, mas também aos órgãos públicos, que têm um dever ainda maior de proteger os dados pessoais. Isso se deve ao fato de que muitas informações coletadas por órgãos públicos são feitas de forma compulsória, sem que o cidadão tenha opção de recusar.

Um exemplo claro de falha na proteção de dados por instituições públicas é o assédio a beneficiários previdenciários por parte de instituições financeiras, que oferecem crédito consignado logo após a liberação do benefício. O próprio INSS foi alvo de uma operação da Polícia Federal que desarticulou uma organização criminosa especializada em obter e revender dados de beneficiários[4],

4 Polícia Federal. PF deflagra operação contra organização criminosa especializada em obtenção e venda de dados sigilosos do INSS. 2024. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2024/09/pf-deflagra-operacao-contra-organizacao-criminosa-especializada-em-obtencao-e-venda-de-dados-sigilosos-do-inss. Acesso em: 25 jan. 2025.

demonstrando a vulnerabilidade dessas informações.

Dados como nome, RG, CPF, endereço, telefone e informações sobre benefícios são extremamente valiosos para pessoas mal-intencionadas. Essas informações podem ser usadas não apenas para assédio, como no caso da oferta de crédito, mas também para fins criminosos, como fraudes e golpes.

É importante mencionar que a obtenção de dados pessoais por criminosos não ocorre apenas por meio de vazamentos ou venda ilegal por prestadores de serviços, mas também por meio de ações realizadas pelos próprios indivíduos.

Durante a navegação na internet, é comum encontrarmos serviços que oferecem promoções, materiais gratuitos, acessos exclusivos e outros benefícios em troca de um cadastro com algumas informações. É justamente nesses cadastros aparentemente inofensivos que reside o risco de exposição de dados, tornando os usuários vulneráveis a ações criminosas.

É nesse contexto que a Lei Geral de Proteção de Dados Pessoais se mostra essencial, ao impor a empresas, prestadores de serviços e órgãos públicos o dever de informar aos cidadãos sobre o tratamento de seus dados e como exercer seus direitos perante essas instituições.

Um exemplo prático dessa obrigatoriedade são os avisos de cookies, geralmente exibidos na parte inferior da tela ao acessar um site pela primeira vez, questionando o usuário sobre a aceitação ou rejeição da coleta de dados.

Essa prática, antes inexistente ou pouco transparente, garante que os cidadãos sejam informados sobre a possível coleta de seus dados pessoais apenas pelo acesso ao site.

Assim, o cidadão que desejar obter informações mais detalhadas sobre as práticas de privacidade de um site, deve procurar por seções como “Política de Privacidade”, “Aviso de Privacidade” ou “LGPD”, cuja nomenclatura pode variar entre os diferentes websites.

Nessas seções, devem ser descritas as informações relevantes sobre o tratamento dos dados pessoais que serão fornecidos,

abrangendo a finalidade do tratamento, os direitos do titular, os prazos de conservação dos dados e o contato do encarregado de dados (DPO), responsável por atender às solicitações de exercício de direitos.

É nesse contexto que a legislação se torna crucial, pois estabelece regras claras para o tratamento de dados pessoais no Brasil e confere aos cidadãos o controle sobre suas informações em um mundo cada vez mais digital.

4. CONSIDERAÇÕES FINAIS

Em um mundo altamente digitalizado, impulsionado por potentes sistemas de inteligência artificial que dependem de dados pessoais para seu funcionamento, torna-se essencial termos consciência sobre a importância de proteger nossas próprias informações pessoais.

Embora empresas e órgãos públicos tenham a obrigação legal de garantir a segurança dos dados sob sua responsabilidade, nós, como titulares, também desempenhamos um papel crucial nessa proteção. Devemos evitar expor nossos dados de forma desnecessária na internet ou fornecê-los indiscriminadamente a serviços que prometem benefícios em troca de cadastros.

Se uma planilha contendo nomes e CPFs já era comercializada por valores significativos, por que você forneceria essas informações gratuitamente e sem cautela?

A legislação nos garante o direito de questionar qualquer empresa, prestador de serviços ou órgão público sobre os motivos da coleta de nossos dados e o uso que será feito dessas informações. É obrigatório que essas entidades apresentem uma justificativa legítima para o tratamento dos dados; caso contrário, não estão autorizadas a utilizá-los.

Em resumo, a questão não é apenas sobre levar uma vida que alguns chamam de 'livro aberto', nem sobre ser uma pessoa honesta ou transparente. Trata-se, sobretudo, da necessidade de proteger seus dados pessoais. Essas informações devem ser compartilhadas apenas em situações em que você compreenda plenamente

o uso que será feito delas e concorde explicitamente com isso.

Dados pessoais são recursos de grande valor. Como será abordado em um tópico específico desta cartilha, evite disponibilizar informações sensíveis, como a sua íris, ou qualquer outra informação pessoal de forma indiscriminada ou por qualquer valor que seja, pois no futuro, o preço a ser pago pela exposição dessas informações pode ser muito maior do que qualquer valor que tenha sido recebido.

CONCEITOS BÁSICOS: O QUE SÃO DADOS PESSOAIS E DADOS SENSÍVEIS

Camilla Pinheiro Cianga

A sociedade já percebeu o quanto a privacidade e a proteção de dados têm ganhado destaque nos últimos anos, principalmente com o avanço das tecnologias e o uso crescente de informações pessoais no dia a dia. No entanto, você sabia que existem dados pessoais que devem ser protegidos de forma especial? Para entender como proteger seus dados, é essencial conhecer dois conceitos básicos: o conceito de dados pessoais e o conceito de dados pessoais sensíveis.

O que são Dados Pessoais?

Dados pessoais são todas as informações que identificam diretamente uma pessoa ou que têm o potencial de identificar um indivíduo. Vamos aos exemplos!

O nome completo ou o CPF de alguém, seu documento de identificação, sua foto, são dados pessoais a partir dos quais nós conseguimos identificar diretamente essa pessoa, também chamada de titular de dados. Todos nós somos titulares dos nossos dados pessoais, ou seja, somos os "donos" dos nossos dados.

Acontece que existem outras informações sobre você que não vão possibilitar que eu identifique imediatamente quem você é, mas podem contribuir na identificação como, por exemplo, a placa do seu carro. A placa de um veículo é única e vinculada diretamente ao proprietário do automóvel. Com esse dado, é possível identificar quem é o dono do veículo por meio de registros em sistemas de trânsito ou bases de dados oficiais. Mesmo sem ter outras informações, a placa permite rastrear o titular responsável, tornando-a um dado pessoal.

Justamente porque qualquer dado, dependendo do contexto, pode acabar revelando quem é seu titular, ou seja, qualquer dado pode ser um dado pessoal em situações determinadas, é que

a Lei Geral de Proteção de Dados não traz uma lista de quais dados podem ser considerados dados pessoais. Não é um conceito fechado, tudo vai depender da possibilidade que o dado oferece, no caso concreto, de identificar alguém.

Alguns exemplos que conseguimos identificar mais claramente de dados pessos são:

- Nome completo;
- Número de CPF ou RG;
- Endereço residencial;
- Número de telefone;
- E-mail pessoal;
- Placa de veículo;
- Localização (como dados de GPS).

Alguns outros exemplos que não parecem dados pessoais, mas também podem ser considerados dados pessoais dependendo do contexto:

- Apelido: quando uma pessoa tem um apelido muito conhecido, muitas vezes mais conhecido que o nome, esse apelido é um dado pessoal. Exemplo: Pelé, Xuxa. E se for um apelido comum, como Zé? Mesmo que várias pessoas possam atender pelo apelido de Zé, se essa informação é falada dentro de um contexto, por exemplo, na cantina da empresa onde determinado funcionário só é conhecido por Zé, todos saberão de quem se trata.
- Título/profissão: um título ou uma profissão também pode ser considerado dado pessoal dependendo do contexto. Se você está em uma roda de amigos da igreja e no meio de uma conversa menciona o "Pastor", mesmo sem falar o nome desse pastor, todos vão saber de quem você está falando. Quando se combina a profissão com mais alguma informação, também pode ser fácil identificar alguém. Por exemplo: se eu me referir ao "professor de matemática" essa informação é genérica. Porém, se eu falo do "professor de matemática" que leciona para o quinto ano

B da escola XYZ em determinada cidade, então será muito mais fácil identificar quem é esse indivíduo, ainda que eu não tenha mencionado o nome dele.

Basicamente, qualquer informação poderá ser considerada dado pessoal se ajudar na identificação de um indivíduo! Por isso é tão importante tomar cuidado com todas as informações que compartilhamos nas nossas redes sociais, por exemplo. Ou, se você é dono de uma empresa, tomar cuidado com todas as informações que você coleta dos seus clientes, funcionários, etc.

O que são Dados Sensíveis?

Os dados sensíveis são um tipo especial de dado pessoal que exige maior proteção. Eles revelam informações íntimas ou que, se mal utilizadas, podem levar a discriminação ou danos à pessoa.

No caso dos dados pessoais sensíveis, a Lei Geral de Proteção de Dados apresenta uma lista de todos os eles, que são:

- Dados sobre origem racial ou étnica: indicam a identidade ou pertencimento de uma pessoa a determinado grupo étnico ou racial (como branco, negro indígena, asiático, etc);
- Dados sobre convicção religiosa: indicam crenças e práticas religiosas ou informações sobre a espiritualidade de um indivíduo;
- Dados sobre opinião política: revelam posicionamentos e preferências políticas;
- Dados sobre filiação a sindicato: indicam a associação de uma pessoa a uma organização sindical ou a participação em atividades relacionadas a sindicato;
- Dados sobre filiação a organização de caráter religioso, filosófico ou político: informações que indicam a associação de uma pessoa a entidades, grupos ou movimentos relacionados a crenças filosóficas, políticas ou religiosas;
- Dado referente à saúde: como histórico médico ou resultados de exames;
- Dados referentes à vida sexual: informações que dizem

respeito às preferências, comportamentos, prática, histórico ou orientação sexual de uma pessoa;
- Dados genético ou biométrico: como impressões digitais ou reconhecimento facial;

Esses dados são considerados sensíveis porque podem expor vulnerabilidades ou aspectos delicados da vida de alguém. Por isso, as leis de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD), estabelecem regras mais rigorosas para o uso dessas informações.

Diferenças entre dados pessoais e dados pessoais sensíveis

A principal diferença entre dados pessoais e dados pessoais sensíveis está no nível de proteção necessário. Enquanto os dados pessoais são informações gerais que identificam uma pessoa, os dados sensíveis envolvem aspectos mais íntimos ou que podem gerar discriminação.

Vamos a alguns exemplos práticos!

Um número de telefone é um dado pessoal porque identifica diretamente o titular. Já um laudo médico, além de ser um dado pessoal, é considerado sensível porque revela informações sobre a saúde da pessoa. Se esse laudo médico atesta que o cidadão é portador de HIV, por exemplo, e as pessoas na empresa onde ele trabalha ou na escola onde ele estuda têm acesso à essa informação, isso pode acarretar em discriminação, pois essa é uma condição de saúde ainda muito estigmatizada.

A utilização indevida de dados sobre a opinião política, por sua vez, pode levar a discriminação, retaliação ou até mesmo exclusão social. O mesmo acontece com dados sobre convicção religiosa, que se usados de forma indevida, podem levar a perseguições (como a perseguição dos judeus na Segunda Guerra Mundial).

Já as informações sobre filiação a sindicatos podem gerar processos discriminatórios em ambientes de trabalho, como a empresa não querer sequer contratar um novo funcionário que seja engajado em questões sindicais, ou não promover esse funcionário.

Por fim, sua digital, que é considerada um dado biométrico, merece proteção especial porque são únicos e permanentes, ou seja – não tem mais ninguém com a mesma digital que você e você nunca vai conseguir alterá-la. Se esses dados forem capturados ou armazenados sem proteção segura, podem ser usados para práticas ilícitas.

Saber diferenciar esses conceitos ajuda você a entender seus direitos e a proteger melhor suas informações. Dados sensíveis exigem maior cuidado, tanto por parte de quem os coleta quanto de quem os compartilha.

Para finalizar, veja como saber diferenciar dados pessoais e dados pessoais sensíveis pode fazer a diferença no seu dia a dia:

- Cadastro em uma loja virtual: se você vai fazer um cadastro em uma loja virtual, é natural fornecer seu nome, endereço e e-mail, que são dados pessoais. Mas se há necessidade de você fornecer dados sobre sua saúde como alergias ou restrições alimentares para encomendar produtos, você estará fornecendo dados pessoais, sensíveis. Nesse caso, é necessário tomar mais cuidado, conferir se o site é seguro, se a empresa é confiável e fornecer somente o mínimo de informações necessárias.

- Redes sociais: fotos, vídeos e comentários que você publica podem ser considerados dados pessoais, certo? Agora, se você compartilha informações sobre sua religião ou orientação sexual, esses dados são sensíveis. Será que vale a pena mesmo compartilhar isso a todo momento? É preciso refletir sempre! Você não sabe quem está do outro lado da tela tendo acesso às suas informações.

DIREITO DOS TITULARES DE DADOS

Débora Leal Soares de Castro

A **proteção da privacidade** é um direito fundamental assegurado pela Constituição Federal de 1988 (art. 5º, inciso X), e a Lei Geral de Proteção de Dados (LGPD) foi criada para reforçar esse direito. A lei estabelece um conjunto de direitos e garantias que buscam **proteger os titulares de tratamentos inadequados ou não autorizados de seus dados**. Sem essas garantias, os titulares estariam vulneráveis a situações como o compartilhamento de informações sem consentimento ou a discriminação baseada em dados sensíveis, por exemplo.

No contexto de uma sociedade cada vez mais digital e interconectada, as informações pessoais são utilizadas em diversos setores, como comércio eletrônico, serviços financeiros, marketing digital, saúde e redes sociais, entre outros. Isso confere aos dados um valor estratégico, mas também os torna vulneráveis a usos inadequados, abusivos ou não autorizados, daí a importância dos titulares estarem cientes de seus direitos e garantias legais existentes para proteção de seus dados e privacidade.

A LGPD também busca restabelecer o **equilíbrio de poder** nas relações entre titulares de dados e organizações. Empresas e instituições possuem tecnologias sofisticadas para coletar, armazenar e analisar dados pessoais, colocando os indivíduos em posição de desvantagem. Ao conferir direitos aos titulares, a lei permite que eles questionem, monitorem e controlem o uso de suas informações, promovendo uma relação mais justa.

Além disso, a legislação é essencial para a **redução de riscos** relacionados ao tratamento de dados. Entre os principais riscos estão o roubo de identidade, as fraudes financeiras, a discriminação algorítmica e a exposição de dados sensíveis, como informações médicas ou financeiras. Esses riscos podem ser reduzidos significativamente com o exercício dos direitos assegurados pela LGPD.

Por fim, a LGPD promove a **transparência e a confiança** nas relações entre titulares de dados e organizações. Quando as empresas atuam de forma ética e clara no tratamento de informações pessoais, criam um ambiente de maior segurança, essencial para o compartilhamento responsável de dados, especialmente no contexto digital.

Por que devo conhecer meus direitos como titular de dados?

Embora a LGPD assegure direitos fundamentais aos titulares de dados, **sua eficácia depende do conhecimento que a população** tem sobre essas prerrogativas. Compreender os próprios direitos é essencial para que os indivíduos possam proteger suas informações pessoais e agir de forma consciente e responsável.

O **conhecimento dos direitos** proporciona aos titulares mais autonomia e controle sobre o uso de seus dados. Isso permite que avaliem de forma crítica as situações em que compartilham suas informações e, quando necessário, imponham limites ao tratamento.

Além disso, entender as garantias oferecidas pela LGPD possibilita o **exercício efetivo de direitos** como o acesso, a correção ou a exclusão de dados pessoais. Com esse conhecimento, os titulares podem interagir diretamente com as organizações responsáveis pelo tratamento de dados ou recorrer à Autoridade Nacional de Proteção de Dados (ANPD) em casos de violação.

O conhecimento também ajuda a **prevenir abusos**. Indivíduos que conhecem seus direitos conseguem identificar práticas inadequadas, como a coleta excessiva de informações, a falta de consentimento ou o uso discriminatório de dados pessoais, exigindo que as organizações se adequem às normas legais.

Além disso, a conscientização dos titulares contribui para a **formação de uma cultura de proteção de dados no Brasil**. Quando os indivíduos exercem seus direitos de forma ativa, incentivam empresas e instituições a adotarem práticas mais éticas e transparentes, beneficiando toda a sociedade.

Por fim, estar informado sobre os direitos previstos na LGPD é essencial para a **defesa em situações de conflito**. Os titulares podem buscar a proteção de seus dados junto à ANPD ou aos órgãos de defesa do consumidor sempre que perceberem violações ou abusos relacionados ao uso de suas informações pessoais.

Compreender e exercer esses direitos é uma forma de garantir que os titulares mantenham o controle sobre suas informações pessoais, protegendo sua privacidade e contribuindo para uma relação mais equilibrada e transparente no tratamento de dados.

A seguir, detalharemos alguns dos direitos previstos pela legislação brasileira para os titulares de dados.

Direito de acesso, correção e exclusão de dados

A LGPD prevê, nos art. 18 e 20, uma ampla gama de direitos dos titulares de dados, dentre os quais podem ser destacados os seguintes:

- acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva;
- confirmação da existência de tratamento;
- acesso aos dados;
- correção de dados incompletos, inexatos ou desatualizados;
- anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
- portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD;
- informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

- informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- revogação do consentimento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado;
- peticionamento em relação aos seus dados contra o controlador, perante a ANPD e perante os organismos de defesa do consumidor;
- oposição a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na LGPD;
- solicitação de revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade; e
- fornecimento, mediante solicitação, de informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão
- automatizada, observados os segredos comercial e industrial.

Trataremos aqui de alguns desses direitos.

O **direito de acesso**, permite que o titular saiba quais dados pessoais uma empresa ou organização possui sobre ele, como foram obtidos, qual a finalidade do uso, a forma e a duração do processo, a identificação e os dados de contato do controlador, informações sobre o compartilhamento dos dados pelo controlador, e a responsabilidade dos agentes que realizarão o tratamento.

Segundo a LGPD o titular tem ainda o direito de solicitar informações sobre as entidades com as quais seus dados pessoais foram compartilhados, bem como sobre as consequências de não fornecer o consentimento para o tratamento de seus dados pessoais quando solicitado.

Exemplo:

Se o titular contratou um serviço de streaming e deseja saber quais dados pessoais ele armazena, como histórico de visualizações ou dados de pagamento, este pode solicitar essas informações diretamente à empresa. A resposta deve ser clara e conter detalhes, como:

- A origem dos dados (se o titular os forneceu ou se foram obtidos por terceiros);
- Os motivos pelos quais estão sendo tratados;
- O período de armazenamento.

A empresa deve fornecer essas informações em formato acessível, como um relatório digital.

Nos termos da LGPD, o titular tem o direito de corrigir informações pessoais que estejam incorretas, incompletas ou desatualizadas.

Exemplo:

Imagine que o titular alterou seu endereço residencial, mas continua recebendo correspondências em um endereço antigo. Nesse caso, o titular pode solicitar à empresa que atualize seu cadastro.

A organização tem a obrigação de corrigir os dados rapidamente e informar eventuais terceiros com quem esses dados tenham sido compartilhados sobre as alterações realizadas.

O direito de exclusão, também conhecido como direito de eliminação, garante que o titular possa pedir a exclusão de seus dados pessoais nos seguintes casos:

- Quando o tratamento dos dados não é mais necessário para o objetivo original;
- Quando há a revogação de sua autorização para uso de seus dados;
- Quando há tratamento de dados em desconformidade com a LGPD.

Exemplo:

Se o titular encerrou sua conta em um aplicativo de compras online e não deseja mais que seus dados sejam mantidos, pode solicitar que a empresa elimine as informações associadas ao seu cadastro, como histórico de compras e dados de pagamento.

Porém, em situações específicas, a exclusão pode não ser possível. Dados relacionados a obrigações fiscais, como notas fiscais emitidas, devem ser mantidos pelo prazo exigido pela legislação tributária, por exemplo. Ainda assim, no caso de impossibilidade de exclusão a empresa deve fornecer uma justificativa para a manutenção dos dados.

O **direito de revisão das decisões automatizadas** é uma garantia essencial da LGPD, assegurando que os titulares possam questionar e compreender decisões que impactem seus interesses, como aquelas baseadas exclusivamente no uso de algoritmos para definir perfis de consumo, crédito ou comportamento.

Exemplo:

Se um sistema automatizado negar a concessão de um empréstimo com base em critérios que não estejam claros, o titular tem o direito de solicitar explicações claras sobre os parâmetros utilizados e exigir a revisão dessa decisão, incluindo a possibilidade de intervenção humana. Este direito é fundamental para prevenir discriminações, corrigir possíveis erros e assegurar maior transparência no uso de dados pessoais em processos automatizados.

O exercício dos direitos previstos pela LGPD é garantido de forma gratuita aos titulares e os prazos para atendimento das solicitações variam conforme a complexidade do pedido e devem seguir as regulamentações estabelecidas pela Autoridade Nacional de Proteção de Dados (ANPD).

Como exercer seus direitos junto às empresas?

A requisição dos direitos pelo titular dos dados deve ser, primeiramente, direcionada ao controlador responsável pelo tratamento dos dados, ou seja, à empresa que está realizando o uso dos dados do titular.

Para iniciar o processo, é necessário **identificar o canal de comunicação da empresa**. A consulta à Política de Privacidade é uma medida eficaz, uma vez que geralmente esta contém informações sobre o contato do Encarregado de Proteção de Dados (DPO) ou outro canal específico destinado a solicitações.

Após identificar o canal, a **solicitação deve ser formalizada** de maneira clara e objetiva. O titular deve apresentar sua demanda, indicando especificamente o direito que deseja exercer, como, por exemplo, acesso, correção ou exclusão de dados. Para que a solicitação seja processada adequadamente, é essencial incluir informações que possibilitem a identificação do titular, como nome completo, CPF e e-mail cadastrado na empresa.

A depender da solicitação, pode ser necessário confirmar a identidade de quem está fazendo o pedido e verificar se os dados fornecidos correspondem aos registros da empresa. Esse procedimento visa garantir que a solicitação esteja sendo feita pelo titular dos dados ou por seu representante legal.

O prazo para a resposta completa ou detalhada à solicitação, conforme estabelecido pela Lei Geral de Proteção de Dados (LGPD), é de 15 dias úteis, sendo esse o período considerado razoável para que a empresa forneça um retorno. Durante esse período, é importante que o titular aguarde a resposta da empresa.

Como exemplo prático de formulário para solicitação de exclusão, o titular pode utilizar a seguinte mensagem:

"Eu, [nome completo], portador do CPF [número do CPF], solicito, com base no artigo 18 da Lei Geral de Proteção de Dados, a exclusão de meus dados pessoais tratados por esta empresa. Estou à disposição para eventuais dúvidas e aguardo retorno dentro do prazo estabelecido por lei."

Como exercer seus direitos junto à ANPD?

Em caso de violação de direitos do titular ou infração à LGPD, é possível registrar reclamações junto aos **órgãos de defesa do consumidor**, especialmente quando o tratamento de dados ocorrer no âmbito de uma relação de consumo e ainda levar a ques-

tão até a **Autoridade Nacional de Proteção de Dados – ANPD**, órgão responsável por zelar pela proteção dos dados pessoais dos brasileiros. A infração pode ser informada à ANPD por meio de petição do titular ou denúncia.

A petição do titular é a comunicação dirigida à ANPD pelo próprio titular dos dados pessoais, relatando a violação de seus direitos por um controlador específico.

Essa petição deve ser acompanhada de prova de que a questão foi previamente submetida ao controlador e não solucionada dentro do prazo estabelecido pela regulamentação. Caso não seja possível apresentar outro meio de prova, é permitida a autodeclaração do titular.

Exemplo de situação que pode ser objeto de petição do titular é o não atendimento, pelo controlador, de uma solicitação do titular para correção ou eliminação de dados pessoais ou para revogação do consentimento.

Por outro lado, as denúncias são comunicações feitas à ANPD por qualquer pessoa, física ou jurídica, sobre supostas infrações à legislação de proteção de dados pessoais, desde que não se trate de uma petição do titular.

Dessa forma, as denúncias de descumprimento da LGPD não se referem necessariamente a uma situação específica de um determinado titular de dados pessoais.

Exemplos de situações passíveis de denúncia incluem o repasse indevido de dados pessoais de clientes a terceiros, acessos não autorizados a dados pessoais ou a ausência de comunicação à ANPD, por parte do controlador, de incidentes de segurança envolvendo dados pessoais que possam causar riscos ou danos relevantes aos titulares.

Para enviar requerimentos à ANPD em casos como os mencionados, deve-se utilizar o Peticionamento Eletrônico do Sistema SEI, conforme as orientações disponíveis no site da entidade.

RISCOS E CONSEQUÊNCIAS DE NÃO PROTEGER SEUS DADOS

Débora Gomes Galvão Basílio

Com o crescimento exponencial da tecnologia e o aumento do uso de dados pessoais, a proteção dessas informações tornou-se um dos principais desafios da atualidade. O compartilhamento indiscriminado e a falta de cuidados podem levar a graves impactos financeiros, emocionais e sociais. Este capítulo busca conscientizar o cidadão sobre os riscos de não proteger adequadamente seus dados, especialmente biométricos, por meio de informações claras e exemplos reais.

1. IMPACTOS FINANCEIROS, EMOCIONAIS E SOCIAIS

1.1. Impactos Financeiros

Os dados biométricos, como impressões digitais e reconhecimento facial, são únicos e permanentes. Quando expostos, podem ser usados para fraudes financeiras, como abertura de contas bancárias ou contratos em nome do titular. Diferentemente de senhas que podem ser alteradas, uma vez vazados, esses dados não podem ser substituídos, aumentando os riscos para a vítima.

Além disso, sistemas que utilizam biometria em vez de senhas estão se tornando cada vez mais comuns, especialmente no setor financeiro. Isso aumenta a dependência desses dados para atividades cotidianas, o que, por sua vez, amplia os riscos em caso de vazamento. É fundamental que as empresas que armazenam essas informações adotem medidas rigorosas de segurança para minimizar os impactos potenciais.

Exemplo real: Em 2019, no Brasil, dados biométricos de eleitores foram expostos em uma brecha de segurança, possibilitando que criminosos usassem essas informações para aplicação de golpes em instituições financeiras. Essa situação mostrou a necessidade de maior fiscalização e penalização para empresas e instituições que tratam dados sensíveis de forma inadequada.

1.2. Impactos Emocionais

Ser vítima de roubo de identidade pode gerar sentimentos de insegurança, impotência e ansiedade. Além disso, lidar com as consequências, como limpar seu nome ou provar que não foi o autor de certas transações, pode ser extremamente estressante e desgastante. O impacto emocional também afeta a confiança nas instituições que coletam e armazenam esses dados.

Cenário frequente: Muitas vítimas relatam dificuldade em reaver prejuízos financeiros e a sensação de invasão em sua vida privada. Casos de uso indevido de dados biométricos também resultam em medo constante de novos golpes, levando algumas pessoas a evitarem serviços digitais.

1.3. Impactos Sociais

A exposição de dados pode resultar em discriminação ou estigmatização. Informações sensíveis, como dados de saúde ou origem étnica, se compartilhadas indevidamente, podem causar exclusão social ou prejuízos à reputação da pessoa.

Exemplo: Empresas que vazaram dados de currículos, incluindo informações sobre deficiências ou histórico médico, geraram constrangimento e dificultaram a contratação dos titulares. Casos como esses evidenciam a importância de políticas claras e eficazes para o tratamento de dados sensíveis no mercado de trabalho.

2. CASOS REAIS DE VAZAMENTOS E SUAS CONSEQUÊNCIAS

- **Caso Facebook (2019):** Dados de mais de 500 milhões de usuários foram expostos, incluindo telefones, localização e datas de nascimento. As vítimas relataram aumento de fraudes e tentativas de phishing. Esse episódio reforça a necessidade de maior responsabilidade das empresas na segurança de informações.
- **Caso Serasa (2021):** Informes apontaram o vazamento

de dados de mais de 220 milhões de brasileiros, incluindo informações financeiras e de contato. Isso aumentou a vulnerabilidade dos titulares a golpes e roubos de identidade. Esse caso é um marco para a LGPD, que estabelece multas e penalizações severas para empresas que falham em proteger dados.

- **Vazamento de dados da Saúde (2020):** Informes revelaram que informações sensíveis de pacientes do SUS foram expostas. Esses dados incluíam históricos médicos, gerando preocupação quanto à discriminação no mercado de trabalho ou em instituições educacionais.

3. RECOMENDAÇÕES PARA O CIDADÃO

- **Limitar o compartilhamento de dados:** Forneça apenas o essencial e para empresas confiáveis. Sempre verifique políticas de privacidade e termos de uso.
- **Monitorar ativamente suas informações:** Utilize ferramentas para acompanhar seu CPF ou dados biométricos em bases de dados. Isso inclui serviços que alertam sobre possíveis utilizações indevidas.
- **Educar-se sobre os riscos:** Conhecer seus direitos sob a Lei Geral de Proteção de Dados (LGPD) é fundamental para exigir segurança no tratamento de suas informações. Caso note falhas em empresas, é possível denunciar aos órgãos competentes.
- **Adotar boas práticas de segurança:** Use senhas fortes, autenticação em dois fatores e não reutilize credenciais. Evite ao máximo salvar senhas em dispositivos compartilhados ou públicos.
- **Cuidado redobrado com redes públicas:** Não utilize redes Wi-Fi abertas para realizar transações financeiras ou acessar informações sensíveis.

4. CONCLUSÃO

A proteção de dados não é apenas um dever das empresas, mas também uma responsabilidade individual. Ao compreender os riscos e consequências de não proteger seus dados, é possível adotar práticas mais seguras e reduzir vulnerabilidades. A LGPD é um marco importante nesse cenário, mas sua efetividade depende da conscientização coletiva e da aplicação rigorosa de suas disposições.

Estar atento e ser proativo na defesa de sua privacidade é essencial. Como cidadão, você tem o poder de exigir transparência e seguridade no uso de suas informações, contribuindo para um ambiente digital mais seguro para todos.

O PERIGO DE COMPARTILHAR DADOS SENSÍVEIS

Guilherme Peara Pereira Araújo

Os dados pessoais sensíveis, como saúde, religião, ideais políticos, questões genéticas, biométricas, origem racial ou étnica são um verdadeiro tesouro, então, se caírem nas mãos erradas, têm o potencial de prejudicar você de várias formas, como:

- Discriminação: você pode acabar sendo excluído de oportunidades devido à sua raça, religião, etc.;
- Preconceito: as pessoas podem lhe julgar e tratar mal apenas por quem você é;
- Manipulação: seus dados podem ser usados para lhe influenciar e, até mesmo, fazer tomar decisões que você não tomaria normalmente;
- Golpes: pessoas mal-intencionadas podem usar seus dados para lhe enganar e roubar;
- Assédio: você pode ser alvo de mensagens ofensivas, ameaças e coações.

Portanto, é exatamente por isso que você precisa protegê-los de quem quer que seja.

O que são dados sensíveis e por que são mais vulneráveis?

Imagine que os seus dados pessoais são como peças de um quebra-cabeça.

Algumas peças são mais "normais", como seu nome, endereço e telefone.

Porém, existem outras peças que são "especiais", porque mostram informações mais íntimas sobre você, como sua religião, suas opiniões políticas, sua saúde, entre outras.

A Lei Geral de Proteção de Dados (LGPD) define dados sensíveis como:

- Origem racial ou étnica: informações sobre sua raça ou cor da pele;
- Convicção religiosa: sua religião ou crença espiritual;
- Opinião política: suas ideias sobre política e partidos;
- Filiação a sindicato ou organização: se você faz parte de algum sindicato ou partido político;
- Dado referente à saúde ou à vida sexual: informações sobre sua saúde, doenças, vida sexual ou orientação sexual;
- Dado genético ou biométrico: seu DNA, impressões digitais ou reconhecimento facial.

Mas por que esses dados são considerados mais vulneráveis?

Porque, conforme comentei, eles podem ser usados para lhe discriminar!

Pense bem: se alguém descobre seu nome e endereço, já é ruim, não é mesmo?

Mas se essa pessoa descobre também que você tem uma doença crônica, as coisas ficam bem piores.

Isso porque seus dados sensíveis podem ser usados para lhe rotular, excluir ou manipular. Então é como se eles dessem um poder extra para quem quer lhe fazer mal.

Por exemplo, em razão de uma doença crônica, uma empresa poderia usar essa informação para lhe negar um emprego ou cobrar mais caro por um plano de saúde.

Isso não é nada justo, não é mesmo?

É por isso que a LGPD tem regras especiais para proteger os dados sensíveis.

Assim, as empresas só podem usar esses dados com o seu consentimento ou, ainda, em casos específicos, como para cumprir uma lei ou proteger sua saúde.

Lembre-se: seus dados sensíveis são parte importante da sua privacidade e intimidade, então devem ser bastante protegidos.

Exemplos de usos indevidos de dados sensíveis e graves consequências

Agora, você já entendeu que os dados sensíveis são informações que revelam aspectos íntimos da sua vida, como sua origem racial, religião, opiniões políticas, saúde, entre outros.

Então, quando esses dados são usados de forma errada, as consequências podem ser muito graves.

Veja alguns exemplos:

- Discriminação em ofertas de emprego: imagine que você se candidata a uma vaga e a empresa lhe exclui do processo seletivo devido à sua religião ou da sua origem racial.
- Negativa de serviços: um plano de saúde pode acabar negando sua cobertura ou aumentar o preço em razão de uma condição médica pré-existente. Isso é injusto e pode ter impactos sérios na sua saúde.
- Exclusão social: você pode ser excluído de grupos ou comunidades por causa das suas opiniões políticas ou da sua orientação sexual. Isso pode lhe isolar e lhe causar sofrimento emocional.
- Manipulação em eleições: seus dados podem ser usados por anunciantes para lhe influenciar a votar em determinado candidato ou partido. Isso fere a democracia e pode ter consequências desastrosas para o país.
- Assédio e perseguição: você pode ser alvo de mensagens ofensivas, ameaças e, até mesmo, perseguição por causa da sua religião, raça ou orientação sexual. Isso pode lhe causar medo e insegurança.

Esses são apenas alguns exemplos de como o uso indevido de dados sensíveis pode ter consequências devastadoras para você e toda a sociedade.

Mas o que acontece com quem usa esses dados de forma errada?

A LGPD prevê punições para quem descumpre a lei, como multas pesadas que podem chegar a milhões de reais.

Além disso, a empresa ou pessoa que cometeu o abuso pode ser processada e ter de pagar indenização por danos morais.

É importante lembrar que a LGPD lhe protege, então você tem o direito de controlar seus dados sensíveis e de tomar medidas para evitar que eles sejam usados de forma indevida.

Fique atento e proteja seus dados!

VENDA DE DADOS BIOMÉTRICOS: OS RISCOS DE VENDER SUA ÍRIS

Louana Costa[1]

A venda de dados biométricos, como a íris, tem se tornado um tema cada vez mais relevante em um mundo onde a tecnologia avança rapidamente e a coleta de informações pessoais é comum. A íris, com seus padrões únicos e inimitáveis, é uma das características biométricas mais seguras e precisas para identificação. Entretanto, a comercialização desses dados levanta sérias preocupações sobre privacidade, segurança e ética. Ao vender informações tão pessoais, os indivíduos podem se expor a riscos significativos, como roubo de identidade e uso indevido de suas características biométricas.

Neste breve texto, explicarei porque os dados biométricos são tão valiosos e quais os riscos associados a venda da sua íris.

1 Advogada e DPO (Data Protection Officer), com forte atuação na área de Direito Digital e Proteção de Dados, com foco na Implementação da Lei Geral de Proteção de Dados Pessoais - (LGPD) e Gestão do Programa de Privacidade e Proteção de Dados Pessoais. Experiência em jurídico interno em empresas de grande porte; Pós-graduada em Direito Corporativo pela IBMEC e Especialização em Proteção Dados - LGPD e GDPR pela Universidade de Lisboa. Certificada internacional pela EXIN como DPO (Data Protection Officer). Membro da Comissão de Proteção de Dados da OAB/RJ e membro da Comissão de Compliance da OAB/Méier-RJ. Coautora dos artigos "A Aplicação da Lei Geral de Proteção de Dados no E-Commerce", LGPD 2022, Debates e Temas Relevantes. [livro eletrônico]. Organização Ana Paula Canto de Lima e Eduardo Chacon Rosas. PE: Império Jurídico, 2022. e o "O Impacto da Lei Geral de Proteção de Dados Pessoais no E-commerce.", Ensaios sobre Direito Digital, Privacidade e Proteção de Dados. [livro eletrônico]. Organização Ana Paula Canto de Lima, Maria Beatriz Saboya. 1. Ed. Recife, PE: Império Jurídico, 2022 (Elas debatem). E-mail: louana.privacy@gmail.com. Linkedin: linkedin.com/in/louana-costa

1. AFINAL, O QUE SÃO DADOS BIOMÉTRICOS, E POR QUE SÃO TÃO VALIOSOS?

Dados biométricos são características físicas ou biológicas que identificam uma pessoa de forma individual e exclusiva, pois são informações únicas e específicas sobre características físicas ou comportamentais de um indivíduo, que podem ser usadas para identificá-la de maneira precisa, como por exemplo, impressões digitais, reconhecimento facial, características físicas ou comportamentais. Contudo, é importante esclarecer, que biometria não se resume à apenas impressão digital, abrangendo também a utilização de íris, face, voz e outras técnicas desde que sejam capazes de identificar as pessoas de forma única.

Abaixo, cito alguns exemplos de dados biométricos:

a) Impressões digitais;

b) Reconhecimento facial;

c) Verificação de retina;

d) Impressões da palma da mão;

e) Tipos sanguíneos;

f) Sequências genéticas;

A biometria é considerada uma das formas mais seguras de identificar pessoas e proteger dados, e podem ser utilizados para diversas finalidades, conforme alguns exemplos abaixo:

a) Passaporte biométrico

b) Controle de ponto;

c) Regulamentação de acesso;

d) Identificação criminal;

e) Controles de acesso em indústrias e condomínios;

f) Diagnóstico por imagem;

g) Acesso digital a instituições financeiras e governamentais.

Devido a essas características, os dados biométricos são considerados um ativo valioso, mas também levantam preocupações sobre privacidade e segurança, especialmente quando são coletados, armazenados e utilizados sem o consentimento adequado.

Venda de Dados Biométricos: Os riscos e os impactos de Vender Sua Íris

Recentemente, diversos vídeos viralizaram nas redes sociais ao relatar o processo de venda de íris no Brasil. Nos conteúdos, é possível ver dezenas de pessoas formando filas para terem seus olhos escaneados e armazenados em bancos de dados, em troca, recebem uma quantia monetária em criptomoeda. De acordo com empresas especializadas em compra de dados biométricos, o objetivo é criar uma rede de identificação global para diferenciar humanos de robôs e inteligências artificiais (IAs), através de um passaporte para "certificação de humanidade", utilizando dados biométricos retirados da íris de pessoas cadastradas.

A venda de dados biométricos, especialmente a íris, levanta uma série de preocupações em relação a privacidade e segurança. Quando informações tão pessoais são comercializadas, há o risco que elas sejam utilizadas de maneira inadequada, como fraudes ou roubo de identidade, ou utilizados sem o consentimento do usuário. Além disso uma vez que os dados biométricos são coletados e vendidos, é difícil controlá-los, o que pode levar a vazamento e uso não autorizado de dados.

Existem alguns riscos que devemos considerar, como por exemplo vazamentos de informações que podem ter consequências irreversíveis, como vazamento de dados biométricos, a segurança no armazenamento desses dados, o uso que as empresas poderão fazer com esses dados. Os impactos vão além do indivíduo, afetando a sociedade como um todo, ao criar um ambiente onde a vigilância e o controle podem se intensificar. E nesse sentido, é crucial entender os riscos associados à venda da íris e as implicações que isso pode ter para a segurança pessoal e a proteção da privacidade em um mundo cada vez mais digital.

Por isso, é importante entender, que ao vender dados biométricos, a pessoa pode estar abrindo mão de um aspecto único de sua identidade, tornando-se vulnerável a ataques que exploram essas informações. Portando, é essencial considerar cuidadosamente os riscos associados a venda de dados biométricos, como a íris, e estar ciente das implicações a logo prazo para a privacidade e segurança pessoal.

DICAS DE COMO SE PROTEGER NO AMBIENTE DIGITAL

Ana Paula Canto de Lima[1]

Dionice de Almeida[2]

A tecnologia inquestionavelmente promove muitos benefícios para a sociedade, tanto para pessoas quanto para as empresas, no entanto, ocasionou também ameaças que surgem de diversas maneiras, situações envolvendo vazamento de dados, invasões hackers e extorsões ganharam muito espaço, gerando preocupação e prejuízos financeiros para os cidadãos.

A internet é uma página em branco e o que cada um insere é que vai dando o tom que ela vai tomando, é indispensável compreender que assim como no cotidiano, estamos passivos de sofrer riscos e ameaças, não seria diferente na rede, por isso é essencial para evitar problemas como fraudes, roubos de identidade e prejuízos financeiros proteger seus dados pessoais. Aqui estão orientações e dicas práticas para manter você e seus dados seguros na internet.

---

1 Advogada, mestre, professora, cursou LLM em proteção de dados com dupla certificação (LGPD RGPD); Conselheira no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD); Membro do Observatório Nacional de Cibersegurança, Inteligência Artificial e Proteção de Dados – ONCiber; Membro da Comissão de Proteção de Dados da OAB Nacional; Diretora de Direito e Tecnologia da Escola Superior da Advocacia de Pernambuco (ESA/PE); Presidente Nacional da Comissão de Crimes Cibernéticos da ABCCRIM (Academia Brasileira de Ciências Criminais); possui artigos e livros indicados nas bibliografias selecionadas pelo STJ.

2 Empresária, escritora e palestrante, é CEO da NV Seguros Digitais, especialista em gestão de riscos, seguros Liability e seguros cibernéticos. Certificada EXIN, possui formação em DPO, é membro do comitê de Governança da ANPPD. Autora do 1º curso EAD de vendas de Seguros Cibernéticos do Brasil, possui autorias relevantes como sua principal obra em coautoria, o livro "LGPD Sua Empresa está Pronta? Legislação - Tecnologia - Mitigação de Riscos", publicada em 2020 e já vendeu mais de 2000 cópias. Iniciou a carreira como Policial Civil, empreende desde 1997 na área de seguros, acredita que o diferencial de um bom profissional está atrelado ao nível de seu conhecimento.

1. RECONHEÇA TENTATIVAS DE ENGENHARIA SOCIAL

Engenharia social é uma técnica em que criminosos manipulam pessoas para obter informações confidenciais. Esteja atento a e-mails, mensagens ou ligações que solicitem dados pessoais ou financeiros. Sempre questione a legitimidade da solicitação antes de compartilhar qualquer informação.

2. EVITE COMPARTILHAR INFORMAÇÕES SENSÍVEIS

- Não divulgue dados pessoais sensíveis, não compartilhe e nem venda seus dados biométricos.
- Desconfie de links e anexos recebidos por e-mail ou mensagem, especialmente se pedirem informações confidenciais ou sensíveis.

3. USE SENHAS FORTES E SEGURAS

- Crie senhas únicas e complexas para cada conta, utilizando uma combinação de letras maiúsculas, minúsculas, números e caracteres especiais.
- Altere suas senhas regularmente e nunca as reutilize em diferentes serviços.
- Habilite a autenticação em duas etapas sempre que possível.
- Use um e-mail apenas para a autenticação em duas etapas, assim você evita problemas se perder acesso ao seu celular, além do próprio golpe aplicado com essa finalidade.
- Acompanhe se seus dados estão seguros, sites como o "Cadê meu Dado" permite que você avalie se seu e-mail se envolveu em algum vazamento/incidente.
- O Serasa e o SPC oferecem serviços como o Serasa Antifraude ou SPC Monitora, que alertam o consumidor sobre o uso de seus dados, incluindo consultas de crédito e tentativas de abertura de contas ou financiamentos.

4. VERIFIQUE A CONFIABILIDADE DOS SITES

- Antes de fornecer qualquer informação em um site, confira se ele utiliza um protocolo seguro (HTTPS) e possui um certificado digital válido.
- Evite acessar sites a partir de links enviados por terceiros; prefira digitar o endereço diretamente no navegador.

5. PROTEJA SEUS DISPOSITIVOS

- Mantenha seu sistema operacional, aplicativos e antivírus atualizados.
- Utilize firewalls e softwares antimalware para proteger seus dispositivos contra invasões.
- Evite usar redes Wi-Fi públicas para acessar serviços sensíveis, como bancos online.

6. TENHA CAUTELA NAS REDES SOCIAIS

- Limite o que você compartilha em redes sociais; informações pessoais podem ser usadas por criminosos para criar golpes personalizados.
- Configure suas contas para que apenas pessoas de confiança possam visualizar suas publicações.

7. EDUQUE-SE E CAPACITE-SE

- Esteja sempre informado sobre as últimas técnicas de fraude e medidas de segurança.
- Participe de treinamentos e palestras sobre segurança digital, especialmente no ambiente corporativo.
- Oriente familiares e amigos, principalmente crianças e idosos, sobre os cuidados na internet.

8. VERIFIQUE A ORIGEM DE SOLICITAÇÕES E OFERTAS

- Desconfie de promoções e ofertas que parecem boas demais para serem verdade.
- Confirme a autenticidade de e-mails ou mensagens rece-

bidas, ligando diretamente para a empresa ou pessoa que supostamente enviou a comunicação.

9. CUIDADO COM APLICATIVOS E DOWNLOADS

- Baixe aplicativos somente de fontes confiáveis, como lojas oficiais, crie o hábito de pesquisar sobre o aplicativo antes.
- Leia as permissões solicitadas pelos aplicativos antes de instalá-los; desconfie se pedirem acesso a informações que não são necessárias para sua funcionalidade.
- Se acostume a ler os termos de uso de aplicativos e as políticas de privacidade, peça ajuda se não entender, ou mesmo peça ao Chat GPT para apontar os principais riscos se não tiver a quem pedir ajuda.

10. O FUTURO DAS FRAUDES DIGITAIS E ALGUMAS MEDIDAS NECESSÁRIAS

Com a evolução tecnológica, a evolução que a inteligência artificial (IA) trouxe para as ferramentas, também se sofisticam as técnicas de fraudes e golpes cibernéticos, na mesma velocidade. Em 2025, espera-se um aumento significativo no uso de (IA) para criar golpes mais elaborados. Um exemplo disso são os deepfakes, tecnologia que utiliza IA para gerar vídeos e áudios falsos de pessoas reais, criando situações de extorsão e desinformação. [3]Empresas e indivíduos devem estar atentos a esses riscos e buscar soluções que combinem tecnologia e educação digital, além de sempre garantir a fonte da informação, antes de tomar qualquer ação relacionada a compartilhar algum dado confidencial.

Outro desafio será o aumento de fraudes em sistemas financeiros, como transferências bancárias e carteiras digitais. De acordo com especialistas, os cibercriminosos devem explorar vulnerabilidades de novos sistemas baseados em blockchain, exigindo

3 DIÁRIO DO COMÉRCIO. Inteligência artificial: Campo fértil para crimes cibernéticos. Disponível em: https://diariodocomercio.com.br/economia/inteligencia-artificial-campo-fertil-para-crimes-ciberneticos/. Acesso em: 25 jan. 2025.

ferramentas mais robustas de autenticação e rastreamento.[4]

Além disso, a engenharia social gamificada promete ser uma tendência preocupante. Os criminosos podem criar experiências interativas para engajar as vítimas em golpes mais complexos, dificultando a identificação do risco.[5]

Para combater essas ameaças, é essencial:

- Implementar soluções de IA para monitoramento e análise preditiva de comportamentos maliciosos.
- Atualizar protocolos de segurança regularmente e investir em backup automatizado.
- Garantir que a legislação acompanhe as inovações tecnológicas, promovendo sanções eficazes contra fraudes, desta forma é extremamente necessário que qualquer empresa esteja sempre em conformidade legal com regras e leis, como a da LGPD, que visa a proteção dos dados pessoais.

Por isso, mais que nunca é preciso ficar atento aos avanços e atualizações da sociedade da informação, considerando a inteligência artificial e aparatos tecnológicos diversos procure desconfiar sempre, buscar a pesquisar, e só depois tome uma decisão ou ação, valide antes toda a procedência da informação. Mesmo que ela tenha sido enviada por alguém de confiança.

11. IMPACTO DOS GOLPES CIBERNÉTICOS

Os golpes cibernéticos têm impacto significativo tanto para indivíduos quanto para organizações. Dados recentes indicam que o Brasil é um dos países com maior índice de ataques de phishing, representando 65% dos golpes relacionados à engenharia social[6] Esses ataques resultam em prejuízos financeiros, danos à reputa-

4 FOLHA DE PERNAMBUCO. Fraudes em 2025: Como equilibrar segurança digital e experiência. Disponível em: https://www.folhape.com.br/noticias/opiniao/fraudes-em-2025-como-equilibrar-seguranca-digital-e-experiencia-do/386851/. Acesso em: 25 jan. 2025.

5 MPMT. Tendências em fraudes para 2025 e o futuro dos golpes digitais. Disponível em: https://mpmt.mp.br/portalcao/news/1217/153221/tendencias-em-fraudes-para-2025-e-o-futuro-dos-golpes-digitais. Acesso em: 25 jan. 2025.

6 (ALMEIDA, 2023).

ção e perda de dados sigilosos, inclusive podendo comprometer as organizações com multas e sanções da própria LGPD.

Casos como o vazamento de 110 milhões de registros na Target (2013) e o ataque à campanha presidencial de Hillary Clinton em 2016 demonstram como ataques cibernéticos podem comprometer grandes organizações e processos políticos.[7]

12. REVISE E CONTROLE SEUS DADOS

- Monitore suas contas bancárias e cartões de crédito regularmente para identificar movimentações suspeitas.
- Solicite relatórios de crédito para verificar se há contas abertas em seu nome sem sua autorização.
- Exercite seus direitos previstos pela Lei Geral de Proteção de Dados (LGPD), como acesso, correção e exclusão de dados pessoais mantidos por empresas.

Campanhas promocionais recebidas através de WhatsApp muitas vezes de parentes e amigos também são muito utilizadas, por ser recebida por alguém conhecido, há uma imensa probabilidade de a pessoa confiar na "promoção" e fazer o cadastro e enviar para outras pessoas[8].

Eles são criativos, inventam listas vip, palestras relevantes, assim eles conseguem cometer crimes e ganhar muito dinheiro, que é o objetivo de toda essa manobra.

Abrir portas através de *Phishing* é uma maneira muito fácil e encurta caminhos de entradas, principalmente para os criminosos que tem como principal objetivo invadir ambientes dos mais variados tipos em quaisquer empresas. Afinal, é muito mais fácil ludibriar pessoas do que as ferramentas de segurança.

Por este motivo, envolver a capacitação de colaboradores quanto aos métodos de Engenharia Social, é essencial e, inclusive, é a orientação de vários profissionais que atuam na área de ade-

7 (ALMEIDA, 2023).

8 LIMA, Ana Paula Canto de. Um manual para nunca mais cair em golpes na Internet. Recife: Editora Império, 2023.

quação à LGPD - Lei Geral de Proteção de Dados, nas empresas. Essa capacitação deve ser de ponta a ponta para que, ao expandir o conhecimento dos usuários, as empresas fiquem mais seguras de possíveis invasores.

> Em aplicativos de comunicação também é possível receber golpes, promoções, contato para um evento, para uma lista VIP, ou mesmo pessoas se passando por pais, filhos, parentes pedindo dinheiro. Procure sempre conferir através de ligação se de fato é a pessoa que acredita ser. Se o contato diz que a pessoa mudou de número de celular, atenção redobrada, ligue imediatamente para o número antigo para confirmar a história.
>
> Um golpe crescente é em 2ª via de boletos, onde o golpista disponibiliza um site com um nome muito idêntico ao da empresa e ao pesquisar no Google ele está entre os primeiros, pois os golpistas pagam para estar no topo das pesquisas, a pessoa acessa e não consegue gerar o boleto no site, pois se trata de um site fake, nesse caso, a pessoa vai ser encaminhada para o WhatsApp dos criminosos, onde conseguirá o boleto com as mesmas características e valores do original, por isso a pessoa cai no golpe.[9]

Evite migrar de sites que encontrou nas pesquisas do Google para o WhatsApp, não pague boletos sem antes confirmar diretamente com a empresa que deveria emiti-lo, ligue sempre de um aparelho diferente daquele que falou com o golpista.[10]

Os criminosos estão cada vez mais astuciosos, precisamos cada vez ter muita atenção para realizar qualquer tarefa na internet.

RISCOS E DANOS

A probabilidade de pessoas continuarem caindo em ataques provocados através de *Phishing* é enorme. E a tendência é aumentar ainda mais, tendo em vista que pesquisas trazem um aumento em 2022 de 226%[11] de ataques comparando apenas o último semestre de 2021.

9 Idem.

10 Idem.

11 **ESET**. Insegurança digital no Brasil: Quais são as maiores preocupações das empresas? Disponível em <https://www.eset.com/br/security-report/>. Acesso em: 20 dez. 2024.

Isto faz com que pensemos que, embora seja uma forma muito antiga para quem é do mundo do cibercrime, é também ainda uma maneira muito fácil e de bons resultados para os criminosos, pois continua sendo eficiente e trazendo sucesso na abertura de brechas para estes invasores digitais.

É importante salientar que a evolução do crime digital tem sido proporcionalmente tão eficiente quanto a evolução da própria tecnologia. Enquanto os hackers éticos se dedicam para a solução das vulnerabilidades nos ambientes digitais, os crackers estão descobrindo formas de invadi-los ou de levar vantagem financeira das pessoas.

Portanto, é importante que os titulares de dados tenham consciência dos danos e prejuízos os quais possam ser vítimas de ataques com *Phishing,* para que evitem clicar em links sem ter certeza da procedência.

CUIDADOS E PRECAUÇÕES

Existem alguns cuidados que os cidadãos podem tomar para evitarem cair em golpes através de *Phishing*. Diversas ferramentas podem auxiliar na prevenção desse tipo de golpe como firewalls, antivírus e antimalwares, mas o principal é a capacitação das pessoas. Afinal, todas as atitudes se referem à conscientização dos usuários.

Não importa o sistema operacional do dispositivo, a Engenharia Social foca na vulnerabilidade das pessoas, como já mencionamos.

O primeiro passo é sempre desconfiar do que você recebe. Nos e-mails avalie o remetente e se o endereço de e-mail está de acordo com o site da empresa de onde ele supostamente está sendo enviado. Mas, não confie plenamente em e-mails estranhos com nota fiscal em anexo, ou mesmo que venha de um conhecido ou parente, sempre verifique antes de baixar e clicar. Verifique se há erros de português ou ofertas que são muito boas para serem verdade, mesmo que o e-mail contenha imagens ou logotipos que pareçam confiáveis não clique, nem baixe arquivos antes de confirmar.

Leve em consideração o senso de urgência da mensagem, alegando uma consequência negativa se você não clicar naquele momento. Dificilmente empresas ou bancos farão esse tipo de ameaça.

Não clique em links desconhecidos e a tática de passar o mouse por cima da mensagem sempre funcionou, pois é possível conferir se o endereço é o correto (o endereço do link irá aparecer no canto inferior esquerdo da sua tela), contudo, surgiu um vírus que infecta a máquina ao passar o mouse em cima do link. Se ficou na dúvida, pesquise a notícia, a promoção, o site ao invés de entrar pelo link recebido.

Nunca forneça informações pessoais. Raramente elas são solicitadas por e-mail ou telefone. O melhor é entrar em contato com a empresa e verificar se eles realmente estão fazendo essa solicitação.

Altere suas senhas regularmente, utilize senhas fortes com letras maiúsculas, minúsculas, números e caracteres, opte pela verificação em duas etapas e perguntas personalizadas, quando possível. Evite utilizar redes abertas de wi-fi.

Outra atitude é proteger os seus meios de comunicação através de softwares de segurança de e-mail que podem identificar e filtrar certos tipos de mensagens.

CONSIDERANDO TUDO ISSO...

A segurança na internet começa com a mudança de hábitos simples e atenção às práticas recomendadas. Manter-se informado e cauteloso é a melhor forma de proteger suas informações pessoais e evitar prejuízos.

Lembre-se: a proteção de seus dados é uma responsabilidade compartilhada entre você, as empresas e o Estado, cada um deve fazer sua parte no cuidado e zelo pelos dados pessoais. Seja proativo na adoção de medidas de segurança e contribua para manter ao máximo a sua segurança no ambiente digital.

A LGPD vem melhorando o cenário, mas ainda há muito o que evoluir, e você é indispensável para a mudança de cultura que

desejamos ter, entender seus direitos e fazer com que eles sejam respeitados faz toda diferença.

Os golpes continuam cada vez mais envolventes, e são aplicados em todos sem distinção, porém os mais vulneráveis como os idosos, são um alvo frequente, conversar com seus pais e tios, e com quem você puder, é uma postura que você pode fazer, ajudando de forma ativa a promover um ambiente seguro na internet, mas lembre-se, os golpes e a coleta de dados para fins ilícitos não ocorre apenas através da internet, há inúmeras versões que podem ocorrer no mundo offline, através de ligação telefônica, promoções e rifas, por exemplo.

Além disso, em datas comemorativas como Natal, Dia dos Namorados, Black Friday, entre outros, os criminosos abusam da criatividade para aplicar golpes e obter vantagens indevidas, agindo solitariamente ou com uma organização criminosa.

Sendo assim, fica um grande alerta de que o cidadão se empenhe, tanto a aprender quanto a disseminar a cultura da segurança e da proteção dos dados, além de cobrar das empresas, é indispensável ficar atentos ao que fazemos com nossos dados pessoais, onde inserimos, com quem compartilhamos e qual a finalidade.

Por fim, a conscientização e a mudança de cultura são as melhores respostas para que o cidadão se mantenha seguro em relação aos seus dados pessoais.

REFERÊNCIAS

ALMEIDA, Dionice.

DIÁRIO DO COMÉRCIO. Inteligência artificial: Campo fértil para crimes cibernéticos. Disponível em: https://diariodocomercio.com.br/economia/inteligencia-artificial-campo-fertil-para-crimes-ciberneticos/. Acesso em: 25 jan. 2025.

ESET. Insegurança digital no Brasil: Quais são as maiores preocupações das empresas? Disponível em <https://www.eset.com/br/security-report/>. Acesso em: 20 dez. 2024.

FOLHA DE PERNAMBUCO. Fraudes em 2025: Como equilibrar segurança digital e experiência. Disponível em: https://www.folhape.

com.br/noticias/opiniao/fraudes-em-2025-como-equilibrar-seguranca-digital-e-experiencia-do/386851/. Acesso em: 25 jan. 2025.

LIMA, Ana Paula Canto de. Um manual para nunca mais cair em golpes na Internet. Recife: Editora Império, 2023.

MPMT. Tendências em fraudes para 2025 e o futuro dos golpes digitais. Disponível em: https://mpmt.mp.br/portalcao/news/1217/153221/tendencias-em-fraudes-para-2025-e-o-futuro-dos-golpes-digitais. Acesso em: 25 jan. 2025.

ATIVE SEU MODO SEGURANÇA

Vinícius Perallis[1]

Caro(a) leitor(a),

Se está lendo este capítulo, meus parabéns! Você acaba de dar mais um passo importante rumo ao aprimoramento dos seus conhecimentos e ao fortalecimento dos seus hábitos em cibersegurança. Infelizmente, é bastante provável que você, ou alguém que conheça, já tenha sido alvo de uma tentativa de golpe, ou até mesmo tenha caído em um. O impacto nas finanças, no emocional e na privacidade podem ser devastadores. Por isso, este capítulo foi especialmente elaborado para ajudá-lo a reduzir consideravelmente as chances de algo assim acontecer — seja com você ou com alguém que você ama.

No Brasil, a grande maioria dos golpes ocorre por meio de uma técnica conhecida como **engenharia social**, que nada mais é do que a prática de manipular as emoções de uma pessoa para que ela tome decisões que, em condições normais, não tomaria. Imagine, por exemplo, que alguém muito próximo entre em contato com você pelo WhatsApp, dizendo que trocou de número e precisa urgentemente de ajuda para pagar uma conta. Uma situação como essa pode desestabilizá-lo, certo? Se você não parar para refletir ou para confirmar que a pessoa é realmente quem diz ser, há uma grande chance de acabar transferindo dinheiro para um golpista. É assim que funciona a engenharia social. O principal intuito dos criminosos cibernéticos é te forçar a tomar uma ação por impulso.

---

1 Especialista em cibersegurança e fundador da Hacker Rangers. Com mais de 15 anos de experiência na área, é referência na criação de soluções inovadoras que combinam tecnologia e gamificação para criar um ambiente digital mais seguro e colaborativo. Mentor nos cursos de Security Awareness Office e Contra Engenharia Social, Vinícius já ajudou 1 milhão de pessoas a se tornarem mais ciberseguras por meio da mudança de comportamento e do fortalecimento da cultura de segurança em mais de 500 empresas no Brasil e no mundo. LinkedIn: https://www.linkedin.com/in/vperallis/

Uma pesquisa de 2024 do Datafolha em parceria com o Fórum Brasileiro de Segurança Pública demonstrou que, em um período de um ano, cerca de 17,3 milhões de brasileiros foram vítimas de golpes causados por falsas solicitações de pagamento com Pix ou boleto. Assustador, não é mesmo? Um número como esse reforça que adotar boas práticas de proteção digital não é apenas um capricho, mas, sim, uma necessidade.

Pensando nisso, ao longo deste capítulo, apresentaremos dez boas práticas de segurança que, quando aplicadas corretamente, podem dificultar — e muito — a vida dos golpistas. E, para tornar essa jornada mais interativa, aqui vai um desafio:

- Atribua **0 pontos** para cada prática que você não conhece e não aplica;
- Atribua **1 ponto** para cada prática que você conhece, mas ainda não aplica;
- Atribua **2 pontos** para cada prática que você já aplica.

No final, some seus pontos, compare com um amigo ou familiar e descubra em qual perfil de segurança você se encaixa. O objetivo? Que você adote essas dicas, monitore seu progresso e ative de vez o seu **modo segurança**!

1. ATIVE A VERIFICAÇÃO EM DUAS ETAPAS NO WHATSAPP

Perigo: Sem essa proteção, golpistas podem clonar sua conta e usá-la para enganar seus contatos, solicitando dinheiro ou informações pessoais em seu nome. Esse é um golpe bastante comum no Brasil e, muitas vezes, as vítimas só percebem o problema quando já sofreram prejuízos.

Por que é importante?

A verificação em duas etapas adiciona uma camada extra de segurança à sua conta, exigindo um código PIN, configurado por você, sempre que o WhatsApp for ativado em um novo dispositivo. Isso significa que, mesmo que alguém tenha acesso ao seu número

de telefone, não conseguirá usar sua conta sem o código.

Passo a passo para ativar:

1. Abra o WhatsApp e vá em **Configurações**.
2. Toque em **Conta** > **Confirmação em Duas Etapas**.
3. Selecione **Ativar** e configure um código PIN de 6 dígitos.
4. Adicione um endereço de e-mail de recuperação para garantir que você possa redefinir o PIN caso o esqueça.

Dica extra:

Crie um código PIN que não seja óbvio. Evite datas de nascimento ou sequências simples, e nunca compartilhe esse código com outras pessoas. Essa camada de segurança pode fazer toda a diferença para proteger você e os seus contatos contra golpes.

2. USE UM COFRE DE SENHAS

Perigo: Usar a mesma senha em várias contas facilita o trabalho dos golpistas. Eles sabem que essa é uma prática comum entre as pessoas. Por isso, quando uma das combinações é descoberta em um vazamento de dados, o primeiro passo é tentar acessar outras contas que potencialmente usem essa mesma senha. Com isso, informações pessoais, financeiras e qualquer outro dado presente em seus perfis podem ficar vulneráveis.

Por que é importante?

Um cofre de senhas é uma ferramenta essencial para proteger suas contas. Ele permite que você guarde todas as suas senhas de forma segura e criptografada, eliminando a necessidade de ter que lembrar por conta própria qual é a combinação de cada perfil. Assim, fica muito mais fácil usar senhas fortes e únicas para cada serviço, não é mesmo? Além disso, muitos cofres podem te ajudar a criar senhas aleatórias e extremamente robustas, tornando tudo ainda mais prático.

Dicas práticas:

1. Escolha um gerenciador de senhas confiável, como **LastPass**, **1Password**, ou **Kaspersky Password Manager**. Todos eles oferecem versões gratuitas ou premium, com excelentes recursos de segurança. No caso de usuários de iOS, aproveite o aplicativo **Senhas**, que nada mais é do que um cofre nativo do sistema.

2. Configure uma **senha-mestre segura** para o cofre de senhas. Essa é a única senha que você precisará se lembrar, então, escolha uma combinação única e difícil de adivinhar.

3. Permita que o aplicativo **gere senhas fortes automaticamente** ao criar novas contas. Assim, você reduz significativamente o risco de usar combinações fracas.

4. Ative o fator de autenticação em duas etapas no aplicativo do cofre de senhas para proteger ainda mais as suas informações.

Dica extra:

Não crie senhas com informações que os cibercriminosos podem descobrir facilmente, como nomes, datas de aniversário ou sequências simples. Além disso, não anote suas combinações em lugares de fácil acesso, como papel ou blocos de notas digitais. Prefira sempre usar o cofre de senhas para se manter protegido!

3. EVITE CARREGADORES USB PÚBLICOS

Perigo: Estações de carregamento USB públicas, como as encontradas em aeroportos, shopping centers e hotéis, podem ser usadas por criminosos para roubar dados do seu celular ou instalar malwares sem que você perceba. Essa prática, conhecida como *juice jacking*, tem se tornado cada vez mais comum e pode comprometer informações sensíveis, como senhas, fotos ou até dados bancários.

Por que é importante?

Carregar seu celular em um USB público parece inofensivo, não é? Mas o que você possivelmente não sabe é que um criminoso pode manipular esses pontos de carregamento para roubar informações ou infectar dispositivos. Usar uma porta USB desconhecida é como confiar em uma fonte de energia não verificada: os riscos são altos e as consequências podem ser graves.

Dicas práticas:

1. Sempre que precisar de bateria fora de casa, leve e use **seu próprio carregador,** conectando-o diretamente a uma tomada elétrica comum.

2. Invista em um **carregador portátil** (também conhecido como *power bank*) para carregar seu aparelho de forma prática e segura em situações de emergência, especialmente durante viagens ou eventos.

3. Considere usar um **cabo USB com bloqueio de dados**. Esse item é projetado para permitir apenas o carregamento, impedindo a transferência de informações entre o dispositivo e a fonte de energia.

Dica extra:

Crie o hábito de carregar totalmente seus dispositivos antes de sair de casa e sempre leve um power bank com você. Essas medidas simples podem evitar que você precise recorrer a portas USB públicas e ajuda a reduzir significativamente o risco de ataques cibernéticos.

4. AJUSTE A PRIVACIDADE NAS REDES SOCIAIS

Perigo: Perfis públicos ou com configurações fracas de privacidade podem abrir portas para diferentes fraudes, da criação de perfis falsos ao roubo de identidade. Criminosos podem usar informações aparentemente inofensivas — como fotos, localização, status e outros dados que você costuma compartilhar — para construir golpes altamente personalizados, aumentando as chances de

que você ou alguém que você conheça caia na armadilha.

Por que é importante?

Ao ajustar as configurações de privacidade nas redes sociais, você torna suas informações menos acessíveis para desconhecidos e dificulta o trabalho de golpistas que usam dados públicos para aplicar fraudes. Limitar o acesso de quem pode ver suas publicações, fotos e informações pessoais é uma forma simples e eficaz de proteger a sua identidade e garantir a sua segurança.

Passo a passo para proteger suas contas:

1. No Instagram:

- Acesse **Configurações > Privacidade** e defina sua conta como privada, garantindo que apenas pessoas que façam parte da sua rede de seguidores possam ver suas publicações.

2. No WhatsApp:

- Vá em **Configurações > Privacidade** e ajuste quem pode ver sua **foto de perfil**, **status** e **"visto por** último**"**. Além disso, escolha bem quem pode te adicionar a **grupos**. Recomenda-se limitar essas informações para **apenas contatos**.

3. No geral:

- Configure a visibilidade das suas publicações para somente amigos ou contatos de confiança. Evite compartilhar informações sensíveis, como localização, viagens ou rotina diária em tempo real.

Dica extra:

De tempos em tempos, dê uma olhada na sua lista de contatos e seguidores e remova aqueles usuários que você não conhece

ou em quem não confia. Assim, você garante que apenas pessoas de confiança tenham acesso às suas informações. Além disso, desconfie de mensagens ou solicitações de pessoas que você não conhece, mesmo que pareçam legítimas.

5. USE UMA VPN EM REDES PÚBLICAS

Perigo: Redes Wi-Fi públicas, como as disponíveis em aeroportos, cafés e shoppings, são altamente vulneráveis ao roubo de dados. Criminosos podem interceptar sua conexão para capturar informações confidenciais, como senhas, números de cartões e mensagens pessoais. Isso ocorre porque, geralmente, essas redes geralmente não possuem os níveis adequados de segurança e criptografia.

O que é VPN e por que é importante?

VPN é a sigla para *virtual private network*, que significa **rede virtual privada** em português. Essa ferramenta cria um "túnel" seguro entre o seu dispositivo e a internet, criptografando todos os dados que você envia e recebe. Isso torna a interceptação de informações muito mais difícil, mesmo em redes Wi-Fi sem senha. Usar uma VPN é como colocar um cadeado em suas informações enquanto elas transitam pela internet, garantindo que ninguém além de você e o serviço ao qual está conectado possam acessá-las.

Dicas práticas:

1. Invista em um aplicativo de VPN confiável, como **NordVPN**, **Proton VPN**, ou **Kaspersky VPN**. Esses serviços são conhecidos por sua facilidade de uso e proteção robusta.

2. Sempre use VPN quando se conectar a redes públicas. Antes de se conectar a uma rede Wi-Fi pública, ative sua VPN. Isso é especialmente importante ao acessar aplicativos de banco, e-mails ou qualquer site que exija login.

Dica extra:

O fato de uma rede Wi-Fi de um estabelecimento público ter senha não significa que ela seja segura. Afinal, a combinação geralmente fica visível e acessível para qualquer pessoa que frequente o local. Por isso, mesmo que a rede seja protegida por senha, sempre habilite a VPN antes de se conectar.

6. MONITORE SEUS DADOS NO REGISTRATO

Perigo: Seus dados pessoais, como seu CPF, podem ser usados por golpistas para abrir contas bancárias fraudulentas ou conseguir empréstimos em seu nome. Muitas vezes, essas fraudes passam despercebidas até que você enfrente problemas financeiros e judiciais ou descubra dívidas que nunca fez.

O que é o Registrato e por que é importante?

O **Registrato** é um sistema gratuito que te permite consultar uma série de informações financeiras vinculadas ao seu CPF, como contas bancárias, cartões de crédito, empréstimos e financiamentos. Desenvolvido pelo Banco Central, ele permite que você monitore sua vida financeira e identifique rapidamente atividades suspeitas. É como revisar o extrato de todas as suas contas ao mesmo tempo, garantindo que não haja nada fora do normal ou feito sem sua autorização.

Passo a passo para proteger seus dados:

1. Acesse **www.bcb.gov.br/meubc/registrato** e entre no Registrato usando sua conta **gov.br**. Caso ainda não tenha uma conta, siga as instruções de cadastro.

2. Consulte regularmente suas informações financeiras no sistema. Monitore todas as contas e créditos vinculados ao seu CPF para verificar se são legítimos.

3. Caso identifique alguma irregularidade, entre em contato imediatamente com o banco responsável e, se

necessário, registre um boletim de ocorrência para formalizar a denúncia.

Dica extra:

Assim como você se consulta regularmente com médicos para garantir que tudo esteja bem, consulte periodicamente o Registrato para garantir que sua saúde financeira esteja em dia. Combine essa prática com o monitoramento de alertas de crédito em serviços de proteção ao consumidor para reforçar ainda mais a sua segurança.

7. DESATIVE O PAGAMENTO POR APROXIMAÇÃO DO CARTÃO OU CONFIGURE SENHA

Perigo: Os cartões com tecnologia de pagamento por aproximação (NFC) tornam as compras mais práticas, mas, em caso de perda ou roubo, qualquer pessoa pode usá-los para efetuar transações de valores baixos, sem precisar de senha. Isso transforma seu cartão em um alvo fácil para gastos não autorizados, especialmente em locais com pouca fiscalização.

Por que é importante?

Manter o pagamento por aproximação ativado sem exigir senha é como deixar uma porta destrancada, facilitando o acesso para pessoas mal-intencionadas. Desativar essa função ou configurar o cartão para exigir senha em todas as transações aumenta a segurança e reduz significativamente os riscos.

Dicas práticas:

1. No aplicativo do seu banco, acesse as configurações do seu cartão e desative a funcionalidade de pagamento por aproximação (NFC). Essa opção geralmente está disponível em seções como “Segurança” ou “Configurações do cartão”.

2. Configure o uso de senha caso prefira manter o NFC habilitado. Ajuste as configurações para exigir que

uma senha seja inserida em todas as transações, independentemente do valor. Assim, em caso de perda ou roubo do cartão, mesmo que um criminoso tente usar o pagamento por aproximação, não conseguirá concluir a compra.

3. Bloqueie o cartão imediatamente em caso de perda. Se você perder o cartão ou detectar compras não reconhecidas, bloqueie-o o quanto antes usando o app do banco ou entrando em contato com a central de atendimento.

Dica extra:

Para garantir ainda mais segurança, revise regularmente o histórico de transações do seu cartão e esteja atento a qualquer movimentação suspeita. Além disso, ative as notificações em tempo real para ser alertado sempre que uma compra for realizada.

8. FAÇA BACKUP DOS SEUS DADOS CRÍTICOS

Perigo: A perda de dados sensíveis, seja por falha no dispositivo, roubo ou ataques cibernéticos, pode causar sérios prejuízos. Imagine perder suas fotos, documentos importantes ou conversas essenciais. Muitas vezes, essas informações são impossíveis de se recuperar sem um backup.

Por que é importante?

Fazer o backup regular dos seus dados garante que você tenha uma uma cópia de segurança para situações imprevistas. Assim, mesmo que algo dê errado, suas informações estarão protegidas e acessíveis por outros meios. É como ter um seguro para suas memórias e documentos — algo que você só percebe o valor quando precisa. Backups automáticos tornam esse processo prático e confiável, reduzindo o risco de perda de dados em momentos críticos.

Dicas práticas:

1. **Ative backups automáticos no Android ou iOS:**
   - No Android, configure o backup em **Configurações > Google > Backup**.[2]
   - No iOS, configure o backup em **iCloud** em **Ajustes > [Seu Nome] > iCloud > Backup do iCloud**.
   - Certifique-se de incluir contatos, fotos, documentos e outros arquivos importantes.
2. **Backup das conversas do WhatsApp:**
   - Acesse **Configurações > Conversas > Backup de Conversas** no WhatsApp.
   - Configure backups diários ou semanais e certifique-se de incluir vídeos se eles forem importantes para você.
3. **Lembre-se de salvar dados críticos.** Inclua no backup arquivos importantes, como contratos, registros médicos e dados financeiros.

Dica extra:

Armazenar informações online usando a nuvem é fundamental, mas também é importante manter uma cópia offline de documentos sensíveis. Para isso, utilize um HD externo ou um pen drive. Assim, você terá acesso às informações mesmo sem conexão à internet.

9. CONFIRME SOLICITAÇÕES SUSPEITAS

Perigo: Para tentar te enganar, golpistas frequentemente se passam por pessoas conhecidas, atendentes de banco ou mesmo autoridades. No Brasil, é muito comum receber mensagens de

2 Lembre-se de que cada fabricante que usa o sistema operacional Android pode personalizar a interface e as configurações de seus dispositivos. Portanto, os caminhos para acessar determinadas funções podem variar entre diferentes marcas e modelos.

“amigos” pedindo transferências urgentes via PIX, com desculpas como emergências médicas ou contas atrasadas. Só depois de fazer a transferência a pessoa percebe que o perfil do contato foi clonado ou falsificado, e o dinheiro foi parar nas mãos dos golpistas. Essas fraudes têm causado grandes prejuízos e se tornado cada vez mais sofisticadas.

Por que é importante?

Confirmar solicitações suspeitas é como verificar a identidade de alguém antes de abrir a porta de casa. É uma prática simples, mas fundamental para não cair em fraudes que tentam se aproveitar da sua confiança ou te desestabilizar com gatilhos de urgência.

Dicas práticas:

1. Sempre confirme a identidade da pessoa antes de tomar qualquer ação. Ligue para o número oficial do contato em questão e confirme diretamente se a solicitação é verdadeira. Nunca confie apenas na mensagem recebida, mesmo que o tom pareça familiar.

2. Faça perguntas específicas. Se suspeitar de algo, faça uma pergunta cuja resposta seja algo que apenas você e a pessoa saberiam, como o nome de um animal de estimação, uma memória compartilhada ou alguma piada interna.

3. Desconfie de urgência extrema. Golpistas costumam te pressionar para agir rapidamente, de modo que você fique sem tempo para pensar de maneira racional. Pare, respire e confirme todas as informações antes de tomar qualquer decisão.

Dica extra:

Oriente seus amigos e familiares a também adotarem essas práticas — e habilitarem as configurações de segurança anteriores!

Essa rede de cuidado mútuo pode dificultar a vida dos golpistas e ajudar a proteger as pessoas importantes para você.

10. ESTEJA INFORMADO SOBRE OS GOLPES MAIS RECENTES

Perigo: Você não navegaria em águas desconhecidas sem um mapa para te orientar, correto? Do mesmo modo, manter-se informado sobre os golpes mais recentes é fundamental para se proteger contra fraudes que, a cada dia, se tornam mais frequentes e sofisticadas. Um alvo fácil é aquele que desconhece os perigos à sua volta. Conhecimento é poder.

Por que é importante?

Para se manter atualizado sobre os golpes mais recentes de forma prática, siga portais de notícias e perfis especializados que te alertam sobre essas fraudes. É como ter um radar que detecta ameaças antes que elas cheguem até você. Esses perfis compartilham informações atualizadas, exemplos reais de golpes em circulação e dicas práticas para se proteger. Estar bem-informado é sua melhor defesa contra armadilhas digitais.

Dicas práticas:

1. Siga perfis especializados. Procure páginas de redes sociais que focam em conscientização sobre cibersegurança, como o **Hacker Rangers** no Instagram. Essas contas oferecem alertas em tempo real e instruções claras para evitar fraudes.

2. Leia, compartilhe e espalhe conhecimento. Dedique alguns minutos para ler as publicações e compartilhar com amigos e familiares. Muitas vezes, o alerta certo no momento certo pode evitar que alguém próximo caia em um golpe.

3. Coloque as sugestões em prática: Apenas ler não basta. É crucial colocar em prática as dicas recebidas,

de modo que elas se tornem parte do seu dia a dia.

Dica extra:

Transforme o hábito de acompanhar perfis de cibersegurança em uma atividade de rotina. Assim como você verifica o clima para planejar seu dia, consulte essas páginas para se preparar contra novos golpes. Estar em dia com as notícias é a melhor maneira de manter você e sua rede de contatos mais protegidos.

11. PONTUAÇÃO E PERFIS:

- **0-6 pontos: Recruta Digital** – Você está apenas começando sua jornada na luta contra os perigos digitais. É hora de vestir sua capa de herói e agir! Cada pequena mudança pode fazer uma grande diferença para proteger você e aqueles ao seu redor.
- **7-14 pontos: Mago Cibernético** – Você já domina alguns poderes, mas ainda precisa ajustar alguns detalhes da sua armadura para enfrentar os vilões cibernéticos. Continue aprimorando suas habilidades para alcançar níveis ainda maiores de defesa digital!
- **15-20 pontos: Super-herói da Cibersegurança** – Parabéns, você é um verdadeiro herói da segurança cibernética! Seu nível de proteção é sólido e você está pronto para combater qualquer ameaça que apareça no caminho.

A missão continua

Lembre-se: a segurança digital não é apenas individual, é uma missão coletiva. Compartilhe essas dicas com sua família e amigos, inspire outros a reforçarem suas defesas e ajude a criar um mundo digital mais seguro. Juntos, formamos uma verdadeira liga de heróis da cibersegurança, prontos para enfrentar os desafios e manter nosso ambiente online protegido.

Ative seu modo herói, e que a segurança esteja sempre com você!

O PAPEL DAS EMPRESAS E DAS AUTORIDADES NA PROTEÇÃO DE DADOS

Marison Souza[1]

No mundo de hoje, cada vez mais digital, dificilmente existe uma atividade que realizamos na internet ou mesmo fora dela que não envolva a coleta e uso de nossos dados pessoais por alguma empresa.

Sempre que compramos algo no celular, usamos um aplicativo de transporte ou acessamos serviços públicos nossos dados são coletados e processados por empresas privadas ou órgãos públicos. Mas você já pensou em como esses dados pessoais são tratados, quem garante seu uso seguro e responsável?

A proteção de dados pessoais é um assunto muito discutido nos últimos anos, principalmente após a criação da Lei Geral de Proteção de Dados (LGPD) aqui no Brasil. Essa lei foi feita para que as empresas tratem os dados pessoais com transparência, segurança e respeito à sua privacidade como cidadão, cliente e funcionário, ou seja, respeitando você como ser humano.

Por exemplo, quando você chega em um estabelecimento e na hora do pagamento o vendedor lhe pede o seu endereço, CEP, telefone, onde trabalha... você nunca parou e pensou: "porque a loja precisaria dessas informações?" Na maioria das vezes, fornecemos esses dados sem questionar, mas a verdade é que muitas empresas coletam dados sobre nós que vão além do necessário.

A LGPD veio justamente para mudar isso, exigindo que as empresas tenham uma finalidade clara e específica para pedir esses dados pessoais. Se a empresa não puder explicar o motivo pelo qual ela precisa dos seus dados pessoais e como eles serão usados, ela não deveria solicitá-los. Isso é um exemplo de como a lei busca proteger os cidadãos, garantindo que seus dados não sejam coletados ou utilizados de maneira abusiva ou desnecessária.

1 Marison Souza é sócio-fundador da Privacy Tools, engenheiro de software, perito judicial, especialista em Privacidade e Proteção de Dados pela Harvard University e ECPC pela Maastricht University.

Imagine que você precisa entrar em um hospital para visitar um parente ou amigo. Para garantir a segurança de todos, é razoável que o hospital peça um documento de identificação e pergunte quem você irá visitar. Esse tipo de procedimento é comum e justificado, pois protege tanto os visitantes quanto os pacientes e a própria instituição. No entanto, seria aceitável que esses dados fossem compartilhados com uma rede de farmácias e, logo depois, você começasse a receber propagandas de medicamentos que coincidem com o tratamento da pessoa que você foi visitar? Claro que não. Esse tipo de prática viola a privacidade e a confiança, além de ir contra as regras da LGPD, que proíbe o uso de dados pessoais para finalidades diferentes daquelas que foram informadas para você. A lei existe justamente para evitar que dados pessoais sejam usados de forma inadequada, protegendo os cidadãos de situações como essa.

Mas, você compreendeu o que são dados pessoais? Dados pessoais são qualquer informação que possa identificar uma pessoa, como nome, CPF, endereço, e-mail, número de telefone, ou até mesmo dados mais sensíveis, como informações sobre saúde, religião ou orientação sexual.

Além desses, existem outros tipos de dados que também são considerados pessoais e exigem cuidado redobrado, como os dados biométricos. Por exemplo, imagine que você usa a digital ou a leitura da íris para acessar seu local de trabalho ou desbloquear seu celular. Esses dados são únicos e, se vazados, podem ser usados para fraudes ou até mesmo para rastrear suas atividades sem seu conhecimento. Da mesma forma, dados financeiros, como extratos bancários ou cartões de crédito, também são críticos e se caírem em mãos erradas, podem resultar em prejuízos financeiros e até mesmo em roubo de identidade, fraudes, invasão de privacidade e até discriminação.

Por exemplo, sabe quando o seu pai ou avó recebe uma ligação ou mensagem no WhatsApp se passando por você e pedindo um dinheiro emprestado? Esse golpista conhece muitos dados sobre a pessoa, como o nome, o número de telefone, a relação familiar

e até detalhes pessoais que podem ter sido obtidos de forma ilícita. Essas informações, aparentemente simples e que qualquer um acaba compartilhando nas redes sociais, são suficientes para explorar a confiança de quem recebe a mensagem. Esse tipo de golpe, conhecido como "fraude do falso sequestro" ou "golpe do parente", só é possível porque os criminosos têm acesso a dados pessoais que foram vazados ou compartilhados de forma inadequada.

As empresas têm um papel muito importante na prevenção de golpes e fraudes, especialmente quando o assunto é proteger os dados pessoais dos clientes. Com o aumento de crimes digitais, como pessoas se passando por outras pessoas para enganar ou roubar dados, as empresas precisam tomar medidas para garantir que os dados estejam seguros. Isso inclui usar sistemas que protejam a guarda dos dados dos clientes, como códigos que dificultam o acesso de pessoas não autorizadas, e fazer verificações para encontrar possíveis falhas de segurança. Além disso, é fundamental que os funcionários sejam treinados para identificar situações suspeitas, como e-mails ou mensagens falsas que tentam enganar as pessoas para obter dados pessoais.

Outra ação importante é avisar os clientes sobre os riscos de golpes e ensiná-los a se proteger. Por exemplo, as empresas podem orientar os clientes a não compartilhar senhas ou dados pessoais por telefone ou e-mail, a não clicar em links suspeitos e a sempre verificar a identidade de quem está entrando em contato. Essas práticas parecem simples mas a grande maioria das empresas ignora e delega ao cidadão a responsabilidade pela segurança dos dados enquanto que atuar de maneira proativa pode inclusive aumentar a fidelidade do cliente que se sentirá em um ambiente seguro para troca de dados pessoais.

Imagine que seus dados de saúde foram vazados e usados por uma empresa para negar um seguro ou um emprego. Isso não é apenas uma hipótese, mas uma realidade que já aconteceu em diversos lugares. Um caso emblemático envolveu a Amazon[2], que foi

2 https://www.reuters.com/legal/new-details-ftc-antitrust-lawsuit-against-amazon-made-public-2023-11-02/

alvo de um processo movido pela *Federal Trade Commission* (FTC) nos Estados Unidos (como se fosse o Procon no Brasil, com algumas diferenças). De acordo com a denúncia, a empresa teria usado algoritmos para aumentar ilegalmente os preços em sua plataforma, explorando dados dos consumidores para aumentar seus lucros. Esses algoritmos analisam registros como histórico de compras, comportamento de navegação e até a localização dos usuários, ajustando os preços de forma discriminatória. Isso significa que duas pessoas buscando o mesmo produto poderiam ver valores diferentes, simplesmente porque a Amazon usou seus dados pessoais para praticar o que foi chamado de "discriminação de preços". Esse tipo de prática, além de injusta, viola a privacidade e a confiança dos consumidores, mostrando como o uso inadequado de dados pode levar a situações de abuso e desigualdade.

A LGPD exige que as empresas adotem uma série de medidas para garantir a proteção dos dados pessoais. Em primeiro lugar, as empresas precisam ser transparentes sobre como e por que estão coletando os dados. Isso significa que elas devem informar de forma clara e acessível para que estão pedindo esses dados e como eles serão usados. Além disso, em alguns casos, é necessário obter o seu consentimento antes de pedir seus dados. Isso significa que você deve autorizar o uso dos seus dados de forma livre, informada e inequívoca, ou seja, você não pode ser obrigado ou coagido a dar um consentimento, pois quem decide sobre como os dados serão tratados é você, dono dos dados.

Mas cuidado, nem sempre vão lhe pedir autorização livre para coletar seus dados, e isso não significa que a coleta seja ilegal. Em várias situações, a lei permite que empresas e instituições coletem dados sem o seu consentimento explícito, desde que haja uma justificativa legítima. Por exemplo, imagine que você está comprando um carro em uma concessionária e o vendedor solicita uma cópia do seu imposto de renda para avaliar a liberação de um financiamento junto ao banco. Nesse caso, você não tem muita liberdade para negar, a menos que desista do financiamento. No entanto, isso não significa que você deva abrir mão do controle sobre seus dados.

Você pode e deve exigir que os dados do seu imposto de renda sejam usados exclusivamente para o cálculo da sua renda e capacidade de pagamento, conforme a finalidade informada. Além disso, é importante garantir que o banco não compartilhe esses dados com empresas de cartão de crédito, que poderiam usar seu histórico para enviar ofertas de empréstimos e crédito de forma insistente. Portanto, fique atento à finalidade para a qual seus dados estão sendo coletados e usados. A LGPD existe justamente para garantir que as organizações respeitem esses limites e não utilizem seus dados de maneira abusiva ou desproporcional.

Os dados pessoais são coletados por empresas privadas mas também pelo governo, e todos possuem um papel importante nesse ecossistema de proteção de dados. Digamos que você precisa abrir um protocolo na prefeitura para solicitar um serviço, como a poda de uma árvore na sua rua. Para isso, o atendente vai pedir alguns dados pessoais, como seu nome, CPF, endereço e número de telefone. Esse pedido é necessário para que a prefeitura possa identificar quem está fazendo a solicitação, entrar em contato com você caso precise de mais detalhes e garantir que o serviço seja realizado no local correto. Nesse caso, a prefeitura está coletando seus dados de forma legítima, pois há uma finalidade clara e justificada: atender sua solicitação e prestar um serviço público. Além disso, a prefeitura é obrigada a proteger esses dados, garantindo que eles não sejam usados para outros fins, como enviar propagandas ou compartilhar com terceiros sem sua autorização, portanto, não encare a LGPD como uma lei que proíbe o compartilhamento de dados, pois é exatamente o oposto, ele apenas cria responsabilidade para as empresas que irão coletar os dados pessoais e garante maior segurança e controle para você, cidadão.

Outro ponto importante é que os dados só podem ser coletados para uma ou mais finalidades específicas e legítimas de forma separada. Isso significa que as empresas não podem usar o que você fornece para qualquer propósito que desejarem. Por exemplo, se uma loja online pede seu email para enviar uma nota fiscal, ela não pode usar esse mesmo email para enviar propagandas sem a

sua autorização, como se fosse uma "venda casada". A emissão da nota fiscal é uma obrigação legal, e existem regulamentações que exigem que a empresa identifique você para cumprir essa finalidade. No entanto, isso não dá à empresa o direito de usar seu CPF e email para cadastrá-lo em uma base de dados de marketing e enviar promoções sem o seu consentimento.

Entendeu? Mesmo que a coleta do dado seja feita no mesmo momento, como durante o pagamento de um produto ou serviço, isso não significa que, uma vez coletado, o dado possa ser usado sem controle. A LGPD exige que as empresas sejam transparentes sobre a finalidade do uso dos dados e respeitem os limites estabelecidos. Se uma informação foi coletada para emitir uma nota fiscal, ela não pode ser desviada para outras finalidades, como marketing, sem a sua autorização explícita, onde nesse exemplo, o seu consentimento seria necessário. Portanto, é essencial que você esteja atento e questione sempre que perceber que seus dados estão sendo usados de forma inadequada.

Além disso, as empresas devem adotar medidas técnicas e administrativas para proteger os dados contra acessos não autorizados, vazamentos ou perdas. Isso inclui o uso de sistemas de criptografia, que transformam os seus dados pessoais em códigos indecifráveis para quem não tem autorização, e firewalls, que funcionam como barreiras digitais para bloquear invasões de sistemas e computadores. Mas a segurança dos dados não se resume apenas à tecnologia; também envolve a conscientização e o treinamento dos funcionários.

Muitos vazamentos de dados ocorrem devido a falhas humanas, por isso, as empresas precisam investir em programas de capacitação para que seus funcionários entendam a importância da proteção de dados e saibam como agir para evitar riscos. Isso inclui desde práticas simples, como não compartilhar senhas, até procedimentos mais complexos, como identificar tentativas de golpes ou garantir que os dados sejam armazenados apenas em sistemas seguros.

A LGPD exige que as organizações adotem essas medidas para garantir que os dados pessoais sejam tratados com o máximo de segurança, minimizando os riscos de violações que podem causar prejuízos tanto para os cidadãos quanto para as próprias empresas. Afinal, um vazamento de dados não só coloca a privacidade das pessoas em risco, mas também pode gerar multas e danos à reputação de uma empresa, e claro que ninguém quer isso, certo?

A lei de proteção de dados também garante uma série de direitos aos titulares dos dados, ou seja, aos cidadãos a quem os dados se referem. Entre esses direitos estão o acesso aos dados, a correção de dados incorretos ou desatualizados, a eliminação dos dados quando não forem mais necessários e a portabilidade dos dados para outra empresa, desde que isso seja tecnicamente viável.

Imagine que você suspeita que uma rede de supermercados está usando seus dados pessoais de forma inadequada. Você decide exercer seu direito de acesso aos dados e entra em contato com a empresa para solicitar uma cópia de tudo o que eles têm sobre você. A empresa é obrigada a fornecer esses dados de forma clara e acessível, mostrando, por exemplo, seu histórico de compras, endereço de e-mail cadastrado e até mesmo se seus dados pessoais foram compartilhados com terceiros. Esse tipo de solicitação permite que você entenda como seus dados estão sendo usados e, se necessário, tome medidas para corrigir ou limitar esse uso.

Agora, pense em uma situação em que você se cadastrou em um site de compras online, mas depois de um tempo decidiu que não quer mais receber e-mails promocionais ou ter seus dados armazenados na plataforma. Nesse caso, você pode exercer seu direito de eliminação de dados, solicitando que a empresa apague do sistema os dados que foram gravados sobre você. A empresa é obrigada a atender sua solicitação, desde que não haja uma obrigação legal ou outra justificativa legítima para manter esses dados. Isso garante que os registros sobre você não fiquem armazenados indefinidamente, reduzindo o risco de vazamentos ou usos indevidos no futuro.

O papel da empresa na proteção de dados vai além de apenas coletar e armazenar informações de forma segura. Ela também precisa garantir que os cidadãos possam exercer seus direitos de forma fácil e transparente. Para isso, é fundamental que a empresa nomeie um Encarregado de Proteção de Dados (DPO).

A sigla DPO vem do inglês "Data Protection Officer", que em português significa Encarregado de Proteção de Dados, que é o profissional responsável por cuidar de todas as questões relacionadas à LGPD dentro da organização. O DPO é como um "guardião" dos dados, ajudando a empresa a cumprir a lei e servindo como ponto de contato para os cidadãos que desejam saber mais sobre como seus dados estão sendo usados ou que precisam corrigir, acessar ou até mesmo apagar dados que foram informados.

Além de nomear um DPO, a empresa deve disponibilizar um canal de atendimento específico para que os cidadãos possam entrar em contato de forma rápida e eficiente. Ter um canal de atendimento bem organizado e de fácil acesso é essencial para mostrar que a empresa leva a sério a privacidade dos cidadãos e está preparada para atender suas solicitações dentro dos prazos estabelecidos pela LGPD. Isso não só ajuda a empresa a cumprir a lei, mas também constrói confiança com os clientes, mostrando que seus dados estão em boas mãos.

No final de 2024, a ANPD fiscalizou[3] 20 empresas por não cumprirem as exigências da Lei Geral de Proteção de Dados (LGPD), especificamente a falta de indicação do DPO e a ausência de canais de comunicação adequados para os titulares de dados. As empresas, que atuam em diversos setores como tecnologia, saúde e varejo, foram notificadas por não disponibilizarem meios eficazes para que os usuários pudessem exercer seus direitos. A ANPD destacou que essa fiscalização é parte do ciclo de monitoramento e visa garantir a transparência e a responsabilização no tratamento de dados pessoais, podendo resultar em penalidades se as irregularidades não forem corrigidas.

3 https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-fiscaliza-20-empresas-por-falta-de-encarregado-e-canal-de-comunicacao

Para que o cidadão exerça seus direitos garantidos pela LGPD, como o acesso ou a eliminação de dados, é essencial que ele entre em contato com a empresa de forma correta. Isso significa que não basta enviar um e-mail genérico ou ligar para o atendimento ao cliente comum. O ideal é que o cidadão utilize um canal específico destinado a questões relacionadas à proteção de dados. Em muitos locais esse canal estará disponível no website da empresa em alguma área como "LGPD", "Fale com o DPO", "Converse com o Encarregado", "Exerça seus direitos" entre outros similares. Geralmente, essas áreas informam como entrar em contato com o DPO, seja por e-mail, formulário online ou até mesmo um número de telefone específico.

Caso o cidadão não encontre essas orientações, ele pode enviar uma solicitação formal à empresa, pedindo os dados de contato do DPO. Uma vez identificado o canal adequado, o cidadão deve fazer sua solicitação de forma clara e objetiva, informando qual direito deseja exercer (acesso, correção, eliminação, etc.) e fornecendo os dados necessários para que a empresa possa identificá-lo e processar o pedido. É importante que o cidadão guarde comprovantes da comunicação, como cópias de e-mails ou protocolos de atendimento, para garantir que sua solicitação seja tratada de forma adequada e dentro dos prazos estabelecidos pela LGPD.

Se mesmo após todas essas tentativas você não obtiver sucesso, saiba que existe no Brasil um órgão público responsável por lhe ajudar. A ANPD é o órgão responsável por fiscalizar e garantir o cumprimento da LGPD no Brasil. Ela foi criada para ser uma espécie de "guardiã" dos dados pessoais, protegendo os direitos dos cidadãos e orientando as empresas sobre como seguir a lei. A ANPD tem o poder de fiscalizar as empresas e órgãos públicos para verificar se estão cumprindo as regras da LGPD. Em caso de descumprimento, ela pode aplicar sanções, como multas, bloqueio ou eliminação dos dados, e até mesmo proibir parcial ou totalmente o tratamento de dados pela empresa.

Além de fiscalizar, a ANPD também tem um papel educativo. Ela publica guias e orientações para ajudar as empresas a se ade-

quarem à LGPD e promove campanhas de conscientização para que os cidadãos conheçam seus direitos. A ANPD também atua como um canal de comunicação entre os cidadãos e as empresas. Se você tiver dúvidas ou quiser denunciar um possível descumprimento da LGPD, pode entrar em contato com a ANPD para obter ajuda.

Além da ANPD, outras autoridades também têm um papel importante no cumprimento da LGPD. O Ministério Público, por exemplo, atua como um fiscal da lei, podendo investigar e tomar medidas legais contra empresas ou órgãos públicos que descumprirem as regras de proteção de dados. Ele pode, inclusive, mover ações judiciais para garantir que os direitos dos cidadãos sejam respeitados, especialmente em casos de vazamentos de dados ou uso indevido de dados pessoais. Já o Procon, conhecido por defender os direitos do consumidor, também pode atuar em casos onde empresas usam dados de forma abusiva, como no envio de propagandas não autorizadas ou na coleta excessiva de dados pessoais sem justificativa clara. Essas autoridades ajudam a complementar o trabalho da ANPD, ampliando a proteção dos cidadãos.

O Poder Judiciário também tem um papel importante na aplicação da LGPD. Em casos mais graves, como vazamentos de dados que causam prejuízos financeiros ou morais, os cidadãos podem recorrer à justiça para buscar reparação. Os juízes podem determinar que empresas paguem indenizações ou tomem medidas para corrigir falhas na proteção de dados. Além disso, o Judiciário pode interpretar e aplicar a LGPD em situações complexas, ajudando a definir como a lei deve ser entendida em casos específicos. Essas autoridades, juntas, formam uma rede de proteção que fortalece o cumprimento da LGPD e garante que os direitos dos cidadãos sejam respeitados em todas as esferas.

Em 2023, a LGPD foi citada[4] em mais de 14 mil decisões judiciais no Brasil, evidenciando um aumento significativo na aplicação da legislação em diversas esferas do Direito. Esse crescimento reflete uma maior conscientização sobre a importância da proteção

4 https://valor.globo.com/legislacao/noticia/2024/02/16/levantamento-aponta-que-lgpd-e-citada-em-mais-de-14-mil-decisoes-judiciais.ghtml

de dados pessoais e a responsabilização das empresas pelo tratamento inadequado dessas informações. O estudo, realizado pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), destaca que as áreas mais afetadas incluem o Direito do Consumidor, Direito Civil e Direito do Trabalho, com um número crescente de ações judiciais relacionadas a violações de privacidade e segurança de dados. Essa tendência indica que os tribunais estão se adaptando à nova realidade imposta pela LGPD, promovendo um ambiente jurídico mais seguro em relação à proteção de dados pessoais no Brasil.

A implementação da LGPD trouxe desafios para as empresas, especialmente para as pequenas e médias, que muitas vezes não têm recursos suficientes para se adequar às novas regras. No entanto, a proteção de dados também representa uma oportunidade para as organizações que desejam construir uma relação de confiança com seus clientes. Ao adotar boas práticas de privacidade e segurança, as empresas podem se destacar no mercado e garantir a fidelidade dos consumidores.

Por outro lado, os cidadãos também têm um papel importante nesse processo. É fundamental que as pessoas conheçam seus direitos e saibam como exercê-los. A LGPD não é apenas uma lei para empresas e órgãos públicos, mas também uma ferramenta para que os cidadãos tenham mais controle sobre como os seus dados pessoais influenciam diretamente em aspectos da sua vida.

A proteção de dados pessoais é um tema que afeta a todos nós. Com a entrada em vigor da LGPD, as empresas e órgãos públicos passaram a ter a responsabilidade de tratar os dados das pessoas com transparência, segurança e respeito à privacidade. A ANPD (Autoridade Nacional de Proteção de Dados) desempenha um papel fundamental nesse processo, fiscalizando o cumprimento da lei e orientando as organizações e os cidadãos.

No entanto, a proteção de dados não é apenas uma questão legal ou técnica. Ela é também uma questão de confiança e responsabilidade. As empresas que adotam boas práticas de privacidade e segurança demonstram respeito pelos seus clientes e contribuem

para a construção de um ambiente digital mais seguro e justo. Por sua vez, os cidadãos que conhecem e exercem seus direitos ajudam a fortalecer a cultura de proteção de dados no país.

Em um mundo cada vez mais conectado, a proteção de dados pessoais é essencial para garantir a privacidade, a liberdade e a dignidade das pessoas. A LGPD e a ANPD são ferramentas importantes nessa jornada, mas o sucesso depende da colaboração de todos: empresas, autoridades e cidadãos. Juntos, podemos construir um futuro onde os dados sejam tratados com o respeito e a segurança que todos merecemos.

COMO PROTEGER SEUS DADOS PESSOAIS NO DIA A DIA

Raniery Almeida

Em um mundo cada vez mais digital, os dados pessoais tornaram-se um ativo valioso, cobiçado tanto por empresas legítimas, muitas vezes para campanhas de marketing, quanto por cibercriminosos.

Com a rápida disseminação da tecnologia no Brasil, a população teve acesso às ferramentas digitais, mas, infelizmente, não foi educada na mesma velocidade para utilizá-las de forma consciente.

Apesar dos esforços regulatórios, como a Lei Geral de Proteção de Dados (LGPD) e outros regulamentos, a experiência demonstra que a educação é o meio mais eficaz para proteger a privacidade e os dados pessoais.

Embora seja praticamente impossível impedir completamente o acesso de terceiros aos seus dados — seja de forma lícita ou ilícita — é essencial que esse acesso seja limitado e que não gere prejuízos.

O primeiro passo para essa proteção é o usuário reconhecer o valor dos seus dados pessoais. É indispensável uma mudança de cultura. De que adianta não instalar o aplicativo do banco no celular por receio de segurança, se o usuário, ao receber uma mensagem alegando ser do banco, fornece seus dados sem questionar a origem do contato ou a necessidade de compartilhamento? Hoje, a maioria das fraudes ocorre por meio de **engenharia social** — situações em que, por falta de conhecimento ou descuido, o próprio usuário colabora com o golpe.

Muitos vazamentos ou compartilhamentos indevidos decorrem da falta de atenção dada à privacidade pelo próprio usuário. Assim, entender que seus dados são preciosos é o primeiro passo: cuide deles como você cuida do seu dinheiro.

Compreendido esse princípio básico, os demais cuidados tornam-se simples.

Passo 1: Agir com Prudência

Quando alguém solicitar seus dados por e-mail, telefone, WhatsApp ou redes sociais, desconfie. Verifique sempre a origem do contato, confirme se aquele número ou canal pertence à pessoa ou empresa em questão e avalie se faz sentido fornecer as informações solicitadas. Por exemplo, bancos raramente pedem fotos de documentos ou senhas pelo WhatsApp. Instituições financeiras costumam utilizar aplicativos oficiais para interações seguras.

Passo 2: Restringir Informações em Redes Sociais

Se você não utiliza redes sociais para fins profissionais, limite o acesso às suas informações apenas a pessoas autorizadas. Evite compartilhar excessivamente dados pessoais. Muitas fraudes começam pela coleta de informações em redes sociais. Analisando perfis, é possível descobrir facilmente dados como cidade de residência, nome completo, parentescos, preferências pessoais e até informações íntimas.

Passo 3: Configurar Aplicativos para Maior Segurança

Aqui estão algumas recomendações práticas para evitar a coleta indevida de dados:

3.1. Evite aplicativos ou softwares "piratas": Utilize apenas lojas oficiais para baixar aplicativos e mantenha-os atualizados. Aplicativos pirateados ou de origem desconhecida frequentemente contêm malwares que roubam dados pessoais. Por exemplo, algumas TV BOX usadas para acessar conteúdos pagos de forma clandestina já foram descobertas com softwares maliciosos capazes de espionar dispositivos conectados à mesma rede.

3.2. Privacidade no WhatsApp: Configure para que apenas contatos autorizados possam visualizar sua foto de perfil. Isso dificulta o uso indevido da sua imagem em contas falsas criadas para aplicar golpes.

3.3. Fotos de perfil diferentes: Evite usar a mesma foto em todas as redes sociais. Isso dificulta a clonagem de contas, pois cibercriminosos terão mais dificuldade em criar perfis idênticos aos seus.

3.4. Verificação de solicitações de pagamento: Sempre confirme por outros meios antes de realizar transferências ou pagamentos. Golpistas frequentemente se passam por empresas ou contatos conhecidos para obter vantagem econômica.

3.5. Autenticação em dois fatores: Ative essa camada extra de segurança no WhatsApp e em outros aplicativos importantes. Isso impede que criminosos acessem suas contas sem uma senha adicional específica.

Passo 4: Evitar Cadastros em Sites e Aplicativos Suspeitos

Não realize cadastros em sites ou aplicativos de origem duvidosa. Sempre que possível, leia os termos de uso e as políticas de privacidade antes de compartilhar informações. Muitos jogos online, filmes e aplicativos solicitam cadastros excessivos e desnecessários apenas para obter dados pessoais, com o objetivo de compartilhá-los com terceiros.

1. CONCLUSÃO

Proteger os dados pessoais é um desafio crescente no mundo digital, mas é também uma responsabilidade que começa com cada indivíduo. Compreender o valor das informações pessoais, adotar práticas prudentes e configurá-las para maior segurança são passos essenciais para mitigar riscos e evitar fraudes. A educação e a conscientização sobre o tema são ferramentas fundamentais para empoderar os usuários diante das ameaças digitais.

Por mais que regulamentações como a LGPD tragam avanços significativos, a segurança depende, acima de tudo, de atitudes preventivas. Ao cuidar dos seus dados como cuida do seu patrimô-

nio, você reduz a exposição a riscos e contribui para um ambiente digital mais seguro e consciente. Lembre-se: pequenos hábitos podem fazer uma grande diferença na proteção da sua privacidade.

PRIVACIDADE EM RISCO: O DESEQUILÍBRIO ENTRE VOCÊ E AS EMPRESAS DE TECNOLOGIA

Carolina Margonari

1. O DESEQUILÍBRIO DE PODER ENTRE TITULARES DE DADOS E EMPRESAS DE TECNOLOGIA

Imagine estar em um jogo de xadrez. Nesta partida, você tem apenas um peão no tabuleiro, enquanto o adversário conta com todas as peças completas. Nesse cenário, não importa o quanto você se esforce, seja corajoso ou persistente: o desequilíbrio é enorme. A cada jogada, o adversário estará sempre um passo à frente, controlando o jogo e antecipando seus movimentos.

Essa é a relação entre as empresas de tecnologia e os titulares de dados.

Contudo, apesar das vantagens existentes, essas empresas dependem dos titulares para o exercício e crescimento de suas atividades. Essa relação é bem ilustrada pela famosa frase atribuída ao jornalista americano Andy Lewis: "se você não está pagando pelo produto, então você é o produto".

2. A FALTA DE TRANSPARÊNCIA DAS EMPRESAS

Em meio às corridas tecnológicas, muitas ações estão sendo realizadas dentro dessas empresas sem que a sociedade tenha muita visibilidade. Elas buscam explorar novas tecnologias com objetivo de inovação ou manutenção das propostas já existentes.

Muitas dessas empresas não estão acostumadas com as práticas de transparência em relação aos titulares de dados. Esse exercício tem sido adotado mais recentemente, em razão das legislações criadas para estipular regras para o tratamento de dados pessoais.

Por isso, muitas falham em garantir essa transparência em seus avisos de privacidade nos sites, na coleta de dados pessoais, entre outras práticas.

3. A COMPLEXIDADE DAS LEIS DE PROTEÇÃO DE DADOS

Embora exista uma lei desde 2018, focada na proteção dos direitos dos titulares de dados, como a Lei Geral de Proteção de Dados (LGPD), muitos titulares desconhecem sua existência.

Com isso, quem deveria garantir que as regras do jogo da proteção de dados estão sendo respeitadas, muitas vezes não demonstra esse compromisso.

Enquanto isso, as pessoas seguem tendo seus dados pessoais explorados e monetizados.

O tema da proteção de dados deveria ser mais trabalhado na sociedade, incluindo sua inclusão na grade educacional.

4. CONSEQUÊNCIAS DA HIPOSSUFICIÊNCIA DOS TITULARES

Com as inovações tecnológicas, as empresas descobriram novas formas de monetizar suas atividades. Uma delas é a realização de análises dos dados pessoais.

A questão central é como, por meio dessas análises, são feitas inferências que permitem descobrir informações sobre o titular que não foram diretamente compartilhadas por ele. Essas descobertas, muitas vezes, revelam aspectos profundos e até sensíveis da vida do titular, que ele não tinha a intenção de divulgar.

Essas informações se tornam extremamente valiosas para outras empresas, que as utilizam para estratégias de marketing, e até para a política, onde podem ser usadas para influenciar comportamentos e decisões.

Muitas vezes, o titular não tem a mínima ideia de que isso é possível. Por falta de conhecimento técnico sobre o funcionamento ou o tipo de soluções utilizadas nessas ferramentas, principalmente dentro das redes sociais, ele se torna hipossuficiente, em desvantagem, diante dessas empresas. Ou seja, o titular não possui os conhecimentos técnicos necessários para exigir os limites na utilização dos seus dados pessoais.

5. A IMPORTÂNCIA DE EXIGIR MAIS DAS EMPRESAS

Em razão disso, é extremamente importante exigir dessas empresas a aplicação da LGPD e outras determinações legais, para que o titular de dados não seja prejudicado, explorado ou enganado.

Essas empresas precisam ser transparentes com seus usuários, utilizando linguagem simples e acessível, documentos de fácil compreensão e criando uma governança eficaz de proteção de dados.

6. CONCLUSÃO

O desequilíbrio de poder entre titulares de dados e empresas de tecnologia é evidente, principalmente quando se considera a falta de transparência, a complexidade das leis e a hipossuficiência dos titulares frente às práticas adotadas pelas empresas.

A complexa exploração de dados pessoais, sem o total conhecimento dos usuários, cria uma dinâmica desigual e vulnerável para os indivíduos.

Por isso, é essencial que a sociedade, os legisladores e as empresas trabalhem em conjunto para garantir um ambiente digital mais justo e seguro, no qual os titulares de dados possam exercer seus direitos com clareza e consciência.

Exigir a aplicação da LGPD e o fortalecimento das práticas de governança em proteção de dados é um passo fundamental para restaurar o equilíbrio, proporcionando maior transparência e controle sobre o uso dos dados pessoais. Somente assim será possível construir um cenário mais ético e respeitoso nas interações entre empresas e titulares de dados.

AUTORES:

Ana Paula Canto de Lima
Camilla Pinheiro Cianga
Carolina Margonari
Débora Gomes Galvão Basílio
Débora Leal Soares de Castro
Dionice de Almeida
Guilherme Peara Pereira Araújo
Louana Costa
Marison Souza
Rafael A. Carneiro de Castilho
Raniery Almeida
Vinícius Perallis

EDITORA IMPÉRIO