www.revistaft.com.br

Revista FT | ISSN 1678-0817 | v. 30, n. 164, 2026 | DOI: 10.69849/y65ep716

A responsabilidade civil das empresas por vazamento de dados pessoais à luz da LGPD

The civil liability of companies for personal data breaches under the LGPD

Giulio Dimarzio[1]

Resumo

Com o grande crescimento da tecnologia, a coleta de dados aumentou consideravelmente, já que está presente em quase todas as atividades do cotidiano, juntamente com isso a segurança jurídica e a proteção devem acompanhar a velocidade de crescimento. Ao analisar esses casos e os riscos a privacidade, à segurança e aos direitos fundamentais que são garantidos pela Constituição Federal de 1988, tornou-se necessária a criação de mecanismos jurídicos específicos que protejam as informações e dados dos usuários. Dessa forma, surgiu então a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, que tem como função estabelecer princípios, direitos e deveres no que tange ao tratamento de dados pessoais no Brasil. Além disso, possui uma importante função de responsabilizar as empresas quando incorrerem em erros que devam ser responsabilizadas, garantindo ao titular dos dados maior segurança e privacidade, para o meio digital ser controlado e regulado de maneira correta.

Palavras-chave: Proteção de dados. Dados pessoais. LGPD.

[1]Universidade Presbiteriana Mackenzie – Campinas – São Paulo – Brasil.

Abstract

With the significant advancement of technology, data collection has increased considerably, as it is now present in almost every aspect of everyday life. Alongside this growth, legal certainty and data protection must also keep pace with technological developments. When analyzing these situations and the risks they pose to privacy, security, and the fundamental rights guaranteed by the 1988 Brazilian Federal Constitution, it became necessary to establish specific legal mechanisms to protect users' information and personal data. As a result, the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados Pessoais – LGPD), Law No. 13,709/2018, was enacted to establish principles, rights, and obligations regarding the processing of personal data in Brazil. Furthermore, the law plays an important role in holding companies accountable for violations and failures for which they may be legally liable, ensuring greater security and privacy for data subjects and allowing the digital environment to be properly controlled and regulated.

Keywords: Data protection. Personal data. LGPD.

1. Introdução

A tecnologia tem evoluído de forma drástica nos últimos anos e trazido grandes transformações na sociedade, principalmente na maneira como as informações são produzidas, armazenadas, compartilhadas e inclusive usadas. Com o avanço das redes sociais, dos celulares e das plataformas foi possível assim uma coleta de dados maior do que o normal relacionada as pessoas. Sendo assim os dados pessoais passaram a ocupar cada vez mais uma posição estratégica nas relações sociais, econômicas já que são utilizadas por empresas e órgãos muito além de somente a prestação de serviços, mas também como estratégias comerciais para atingir um possível cliente no ponto em que o mesmo tem interesse, muito com base em suas informações coletadas.

O grande crescimento de dados pessoais, proporcionam benefícios para sociedade, mas junto a eles advém inúmeros riscos relacionados a privacidade, segurança, direitos fundamentais violados dos indivíduos, já que alguns dados pessoais podem revelar algo relevante da vida de um indivíduo e se utilizados de forma inadequadas, podem resultar em fraudes, exposição indevida e outros tipos de violação. Sendo assim se tornou extremamente

necessário estabelecer mecanismos que garantam que os dados sejam tratados de forma legítima e segura.

A proteção dos dados pessoais, representa uma importante dimensão da proteção da personalidade e privacidade, em que na Constituição Federal de 1988, já haviam direitos fundamentais assegurados como intimidade, assim como Código de Defesa do Consumidor e o Marco Civil da Internet contribuíram para estabelecer regras também relacionadas ao tema, porém diante da alta e crescente complexidade do ambiente digital e a forma acelerada como se expandiu, surgiu a necessidade de uma Legislação específica, que foi a LGPD criada em 2018, Lei de número 13.709, que criou e estabeleceu regras gerais para o trato dos dados, inclusive nos meios digitais por pessoas físicas e jurídicas. A Legislação tem como objetivo proteger os direitos fundamentais de liberdade e privacidade, assim como promover maior transparência e segurança no uso das informações.

A entrada da LGPD, representou um importante marco na legislação brasileira visando estabelecer parâmetros para que o tratamento dos dados pessoais seja feito com maior responsabilidade, e exigir mais cautela na coleta e utilização dos mesmos. Dessa maneira compreender o crescimento do tratamento de dados e analisar os desafios.

Com isso será analisado quando e como ocorrem os vazamentos desses dados, como isso tem crescido e afetado a todos, e entender em quais casos e quando determinadas empresas e instituições devem ser responsabilizadas e devem arcar com as devidas, buscando reforçar de que por se tratar de um tema sensível os dados pessoais precisam os mesmos ser tratados com comprometimento e ética, já que a internet está presente atualmente em todas as áreas de nossas vidas, até mesmo nas mais básicas do cotidiano.

2. A proteção de dados pessoais no ordenamento jurídico brasileiro

A proteção de dados pessoais se tornou essencial diante do avanço tecnológico e do aumento do uso de informações pessoais. No Brasil, a proteção está relacionada aos direitos fundamentais à privacidade, à intimidade e à liberdade. A Constituição Federal e outras legislações já estabeleciam mecanismos de proteção antes da criação da LGPD.

A Lei nº 13.709/2018 (LGPD) consolidou regras específicas para o tratamento e a proteção de dados pessoais. Assim, o ordenamento jurídico brasileiro busca garantir maior segurança, transparência e controle aos titulares de dados, pois assim como o uso da internet

aumentou, o uso de dados também, porém junto a isso a proteção destes dados deve ser cada vez maior, garantindo um ambiente virtual dentro dos moldes e padrões constitucionais e balizados em uma ideia de segurança para o usuário e titular dos dados não ser lesado.

2.1. Conceito de dados pessoais

De acordo com a própria Lei Geral de Proteção de Dados Pessoais (LGPD) em seu artigo segundo, os dados pessoais, tem como fundamento: O respeito a privacidade, a autodeterminação informativa, liberdade de expressão, informação, comunicação e opinião, inviolabilidade da intimidade, honra e imagem, livre iniciativa, concorrência e a defesa do consumidor, assim como os direitos humanos, livre desenvolvimento da personalidade, dignidade e o exercício da cidadania pelas pessoas naturais.

Os dados pessoais são definidos como todas as informações relacionadas a uma pessoa natural identificada ou identificável, ou seja, qualquer informação que permita o reconhecimento de um indivíduo, seja de maneira direta ou indireta. Esses dados estão presentes em diversas situações do cotidiano, desde informações básicas de identificação até registros utilizados em atividades realizadas no ambiente digital.

Além disso, a legislação estabelece uma categoria específica denominadas dados pessoais sensíveis no artigo 5, que abrange informações ainda mais particulares sobre a vida de uma pessoa, como por exemplo sua origem racial ou étnica, convicção religiosa, opinião política, dados referentes à saúde, vida sexual, entre outras informações previstas na lei. Essa classificação recebe atenção especial justamente porque envolve aspectos íntimos da personalidade, de modo que seu uso inadequado pode ocasionar discriminação, exposição indevida e prejuízos aos direitos fundamentais.

Nesse sentido, a proteção dessas informações torna-se indispensável, uma vez que os dados pessoais não se limitam apenas àqueles que identificam alguém de forma evidente. Conforme explicado em uma publicação no site do Tribunal Regional Eleitoral (TRE) do Estado do Paraná, a identificação de uma pessoa pode ocorrer tanto de maneira direta, por meio de informações como o Cadastro de Pessoas Físicas (CPF), quanto indiretamente, por elementos que, isoladamente ou quando associados a outros dados, permitem reconhecer determinado indivíduo, como é o caso de um endereço IP. Dessa forma, compreende-se que até mesmo informações aparentemente simples ou comuns podem representar dados pessoais

e, consequentemente, merecem proteção jurídica. Isso demonstra a importância da LGPD no cenário atual.

2.2. LGPD

A autora Lara Rocha Garcia em sua obra: explica um pouco de forma básica o que é e como surgiu a LGPD:

> A Lei Geral de Proteção de Dados Pessoais (LGPD, Lei n. 13.709/2018), ainda em vacatio legis,1 tem causado tumulto. Afinal, para quê serve? Inspirada na lei europeia de proteção de dados, conhecida como General Data Protection Regulation (GDPR), a LGPD tem como objetivo proteger dados pessoais de pessoas naturais, ou seja, pessoas físicas. Este é o primeiro ponto: a LGPD não tem como escopo os dados das empresas (pessoas jurídicas), mas sim os dados que as empresas têm das pessoas físicas, sejam elas funcionárias, terceiras, clientes, acionistas etc. – ou seja, todo mundo. A lei, criada em 14 de agosto de 2018, tem 65 artigos e foi alterada pela Medida Provisória 869/2018 e pela Lei n. 13.853/2019. Embora seja a legislação mais recente e mais específica, não é a única lei que rege a privacidade. Esse tema já havia sido tratado em alguns outros lugares antes, como: a Constituição Federal, o Marco Civil da Internet,3 o Código de Defesa do Consumidor,4 a Lei de Acesso à Informação,5 Habeas Data6 e o Decreto do Comércio Eletrônico.7 Exatamente por ser a mais específica e exclusiva sobre o tema é que a LGPD tem principal relevância e inova ao criar sanções direcionadas, além de uma governança que inclui um novo órgão da presidência da República.

Já na própria Lei, a LGPD em seu primeiro artigo conta com uma breve descrição do que é a Lei e para que serve:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Para resumir, a LGPD possui como função regulamentar a forma e maneira como os dados pessoais são coletados, armazenados, utilizados e compartilhados por empresas,

instituições e até mesmo os órgãos públicos. Seu objetivo principal é a ideia de garantir uma segurança e transparência no tratamento dessas informações, criando e estabelecendo novas regras que devem ser seguidas por todos aqueles que lidam com dados pessoais, além disso a lei busca proteger e garantir direitos fundamentais como de liberdade e privacidade garantindo que as informações sejam utilizadas diretamente para determinado fim e sejam tratadas com ética e comprometimento.

Outro importante ponto da LGPD é garantir que os titulares possuam maior controle sobre seus dados e permitir que saibam como suas informações serão utilizadas, tratadas e possam acompanhar isso de perto, podendo contestar caso o uso esteja sendo feito de forma indevida. A Legislação estabelece ainda responsabilidades para empresas que tratam os dados e exigem que adotem medidas de seguranças e formas de combate para prevenir vazamentos e não causar prejuízos tanto morais quanto financeiro as pessoas.

Dessa maneira a LGPD fortalece a confiança nas relações entre empresas e consumidores e garantem respeito e integridade a direitos fundamentais.

2.3. Princípios da proteção de dados

No artigo 6 da LGPD são estabelecidos alguns princípios que as atividades de tratamento de dados devem observar. São esses: O primeiro princípio é o da finalidade em que faz com que os dados possuam um propósito e uso legal e legítimo dentro dos direitos e limites, tornando seu uso correto. Já o da adequação faz com que o tratamento esteja em compatibilidade com o que foi colocado de finalidade, considerando o que será utilizado. Outro princípio é o da necessidade estabelecendo que apenas dados indispensáveis para que tenha o objetivo alcançado devem ser coletados e tratados, evitando assim o uso de dados em excesso de forma desnecessária. Já o livre acesso vai garantir ao titular que tenha a possibilidade de consultar sem custo seus dados e obter informações sobre duração e a maneira como os dados estão sendo tratados. A qualidade dos dados, por sua vez, faz com que as informações sejam corretas e claras permitindo que sejam utilizadas de maneira apropriada

O princípio da transparência determina que os titulares tenham informações precisas e assertivas, além de acessíveis no que tange ao tratamento de seus dados e sobre os responsáveis por essa atividade, respeitando assim os segredos comerciais e industriais. Outro princípio importante é o da segurança que exige que sejam tomadas medidas técnicas e administrativas que possam proteger as informações diante a acessos que não estão

autorizados, como vazamentos e perdas. Complementando esse princípio, a prevenção estabelece que sejam adotadas medidas antecipadas para evitar a ocorrência de danos decorrentes do tratamento de dados pessoais, ou seja, que as empresas já tenham maneiras de proteger os dados antes de que ocorra um posterior vazamento.

Além disso existe também o princípio da não discriminação que irá proibir que dados sejam usados com fins de discriminação ilícita ou abusiva, protegendo os titulares contra práticas que de alguma maneira prejudiquem seus direitos, e por fim a responsabilização e prestação de contas que determina que os agentes responsáveis por tratar os dados mostrem que adotam medidas eficazes cumprindo assim as exigências da LGPD, sendo assim capazes de mostrar estar em conformidade nas atividades com suas legislações, e passando ao titular dos dados segurança jurídica.

Sendo assim, após analisados os princípios previstos no artigo sexto da Lei, entende-se que estes servem de baliza e orientação para um tratamento responsável dos dados e seguro dos dados pessoais, estabelecendo limites para sua utilização e reforçando a necessidade de respeito a privacidade e transparência, sua aplicação contribui então para que não ocorram abusos e mitigar os riscos, fazendo com que exista uma maior confiança entre indivíduos, empresas e organizações que tratam informações pessoais.

Dessa maneira, conclui-se que os princípios da LGPD no artigo 6, são essenciais para garantir a proteção dos dados pessoais e estabelecem diretrizes que orientam a utilização de forma ética, contribuindo para evitar abusos e mitigar riscos e assegurar o respeito a privacidade aos direitos dos titulares, assim o cumprimento desses princípios é fundamental e fortalecem a confiança nas relações entre as empresas e os usuários.

3. O vazamento de dados pessoais e os incidentes de segurança

No capítulo em questão será estudado o que são os vazamentos de dados, como eles ocorrem, se é algo de extrema recorrência no Brasil e como isso afeta nosso dia a dia.

3.1. Conceito de vazamento

Para entender o conceito de vazamento, a Fortinet, empresa multinacional americana de cibersegurança sediada em Sunnyvale, Califórnia define como:

> Um vazamento de dados acontece quando uma parte ou fonte interna expõe dados confidenciais, geralmente involuntariamente ou por acidente. Os resultados de um vazamento de dados podem variar de perda de informações a exploração maliciosa. Muitas vezes, os vazamentos de dados levam a violações de dados.

Após a análise acima da Fortinet pode-se entender que o vazamento de dados ocorre quando dados pessoais são confiados a determinadas empresas que devem ser tratados, mas que muitas vezes por erros internos e sistêmicos, ou mesmo por falhas humanas sejam elas dolosas ou não. Logo esse vazamento pode indicar em casos apenas informações que escaparam que não são de suma importância, mas também podem ser dados comprometedores tanto para uma pessoa física que interfere em sua integridade física e moral, quanto para pessoas jurídicas que podem ter dados e segredos comerciais vazados, causando danos enormes. Por isso o vazamento de dados deve ser analisado de maneira correta, entendendo se existiu algum dano causado a aquele que teve seu dado vazado e definir reparações nesses casos.

Já de acordo com a Microsoft, uma das maiores empresas do setor de tecnologia, a mesma define vazamento de dados como:

> Um vazamento de dados é uma divulgação não autorizada de informações sensíveis, confidenciais ou pessoais dos sistemas ou redes de uma organização para uma parte externa. Os vazamentos de dados podem ser intencionais ou acidentais e podem ter consequências graves para as organizações e os indivíduos afetados.

Com base nessas ideias entende-se também que todo vazamento não é autorizado e que ocorre sem a ciência e autorização do titular e que possuem consequências graves para as empresas responsáveis por esse controle.

3.2. Como os vazamentos acontecem

Ainda de acordo com a Fortinet, são estabelecidas e indicadas algumas maneiras de como os vazamentos de dados ocorrem:

> 1. Infraestrutura fraca: uma infraestrutura de rede configurada incorretamente pode permitir que os dados sejam vazados, causando perda ou até mesmo uso indevido.

> Por exemplo,a empresa de segurança cibernética Cognyte deixou um banco de dados massivo desprotegido, sem autenticação ou autorização necessária para acesso. Como resultado, mais de 5 milhões de registros foram expostos on-line.
>
> 2. Erro humano: as estatísticas recentes revelam que o erro humano é a principal causa de vazamentos e violações de dados. O erro humano pode causar vazamentos de vários graus, de um e-mail enviado para as pessoas erradas a vazamentos massivos causados por credenciais roubadas. Um exemplo é a perda massiva de dados (quase 23 terabytes) sofrida pela cidade de Dallas devido à negligência dos funcionários em 2021.
>
> 3. Erro do sistema:os erros do sistema podem deixar as redes vulneráveis. Em 2019, uma vulnerabilidade do Facebook que foi corrigida desde então permitiu que golpistas raspassem os dados pessoais de mais de 530 milhões de usuários do Facebook em 106 países, incluindo seus endereços de e-mail, números de telefone, locais e outros detalhes. Em 2021, os dados foram publicados em um fórum de hackers.
>
> 4. Vulnerabilidades de terceiros: aplicativos e fornecedores de terceiros podem precisar de acesso ao seu sistema ou rede, mas podem representar um risco. Um exemplo foi o vazamento de dados do Marriott em 2020. Os hackers aproveitaram um aplicativo de terceiros para acessar mais de 5 milhões de registros de convidados.
>
> 5. Pessoas maliciosas: vazamentos causados intencionalmente por pessoas maliciosas não são tão comuns quanto vazamentos acidentais. Em 2021, quatro advogados do escritório de advocacia Elliott Greenleaf supostamente roubaram e excluiram arquivos da empresa para ajudar um escritório de advocacia concorrente a abrir um novo escritório.

Resumindo a forma como os vazamentos ocorrem, entende-se que muitas das vezes ocorrem por erros sistêmicos, erros humanos no próprio manejo da tecnologia tendo em vista o grande número de dados tratados. Mas também observa-se que existem casos e muito comumente o vazamento destes dados ocorre por malícia humana, em que um humano gerindo a tecnologia ou por conta própria de maneira dolosa, expõe dados pessoais de um titular, as vezes funcionando até como uma moeda de troca como o dinheiro.

3.3. Aumento do vazamento de dados

De acordo com uma notícia publicada pela CNN, em 2025 o Brasil ocupou a sétima posição entre os países com maior número de ataques digitais. Esse dado evidencia como as ameaças virtuais estão cada vez mais presentes no cotidiano da sociedade, especialmente

diante da crescente utilização da internet e das plataformas digitais. Muitas vezes, os próprios usuários acabam contribuindo involuntariamente para a exposição de suas informações pessoais, seja ao acessar sites sem verificar suas políticas de privacidade, aceitar cookies sem compreender sua finalidade ou compartilhar dados em plataformas sem conhecer adequadamente as condições de utilização dessas informações.

Esse cenário está diretamente relacionado à expansão da tecnologia e ao aumento da utilização de serviços digitais, redes sociais, sites, aplicativos e ferramentas de inteligência artificial. Embora esses recursos proporcionem praticidade e facilitem diversas atividades, também ampliam a quantidade de informações pessoais coletadas, armazenadas e compartilhadas pelas empresas e organizações. Consequentemente, quanto maior o volume de dados tratados, maiores podem ser os riscos relacionados à segurança da informação, entre eles os acessos não autorizados e os vazamentos de dados pessoais.

Como exemplo da dimensão que esses incidentes podem alcançar, uma notícia publicada pelo portal TudoCelular relatou um vazamento ocorrido em um servidor que expôs CPFs e outras informações pessoais de aproximadamente 148 milhões de brasileiros. O episódio demonstra que uma única falha de segurança pode atingir uma quantidade extremamente elevada de pessoas, colocando em risco informações que fazem parte da identificação e da vida cotidiana dos indivíduos. Além disso, evidencia a responsabilidade das empresas e organizações que realizam o tratamento de dados pessoais, uma vez que devem adotar medidas adequadas para proteger essas informações e evitar que sejam acessadas ou utilizadas indevidamente.

4. A responsabilidade civil das empresas à luz da LGPD

Agora que foi abordado um pouco do que é a LGPD, dados pessoais e vazamentos, e foi estudado como ocorrem os vazamentos, será analisada qual é a responsabilidade civil das empresas pelos vazamentos, e como devem agir as empresas nesses casos.

Para adentrar no tema, primeiro é preciso entender o que é a Responsabilidade Civil, que segundo Carlos Roberto Gonçalves, grande autor e doutrinador do Direito Civil, diz que:

> A responsabilidade civil decorre de uma conduta voluntária violadora de um dever jurídico, isto é, da prática de um ato jurídico, que pode ser lícito ou ilícito. Ato jurídico é espécie de fato jurídico.

A responsabilidade civil surge quando uma pessoa ou empresa pratica uma conduta voluntária que viola um dever estabelecido pelo ordenamento jurídico, podendo essa conduta ocorrer por meio de uma ação ou omissão. Em outras palavras, quando alguém deixa de cumprir uma obrigação legal ou age de maneira contrária ao Direito e, com isso, causa prejuízo a outra pessoa, poderá surgir o dever de reparar o dano. Pode este ato ser lícito ou ilícito. Portanto, a ideia principal é que a responsabilidade civil está relacionada a uma conduta humana que produz consequências jurídicas e que, quando presentes os requisitos legais, pode gerar a obrigação de reparar os prejuízos causados a outra pessoa. No contexto da LGPD, por exemplo, uma empresa que deixa de cumprir seus deveres de proteção e segurança dos dados pessoais poderá ser responsabilizada caso essa conduta provoque danos aos titulares das informações.

4.1. Da responsabilidade civil

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
>
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
>
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
>
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
>
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
>
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
>
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.
>
> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
>
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

A responsabilidade civil das empresas quanto aos vazamentos de dados pessoais consiste na ideia de reparar os danos que foram causados aos titulares sejam eles morais, patrimoniais ou eventuais prejuízos financeiros. Nesse caso, o artigo 42 da LGPD estabelece que o controlador que em razão da forma como tratou os dados, causar qualquer dos tipos de danos que violem a Lei, devem reparar o titular dos dados, ou seja se uma empresa deixa de cumprir suas obrigações na proteção dos dados do titular, deverá indenizar a mesma.

A responsabilidade civil possui como finalidade reparar prejuízos sofridos à vítima e responsabilizar quem originou o dano, logo em um caso de uma empresa não ter tratado de maneira correta os dados de determinado titular, devem reparar juntamente com os eventuais prejuízos causados. Porém observa-se que nem todo vazamento de dados é de responsabilidade da empresa controladora reparar. Para que exista esse dever, devem se considerar elementos como a ocorrência do dano, ou seja a forma como ele ocorreu, a relação do prejuízo com o tratamento do dado e se realmente existiu realmente uma violação jurídica.

A LGPD também possui casos que mostram uma responsabilidade solidária fazendo com que mais de um agente de tratamento responda pelos danos que foram causados, ou seja mostra uma responsabilidade solidária que o titular pode buscar as reparações nos termos legais sem prejuízo da posterior apuração de cada responsável. Além disso, o artigo 42 prevê a possibilidade de inverter o ônus da prova quando tiver condições legais e facilitando a defesa dos direitos do titular.

Por outro lado, no artigo 43 é estabelecido hipóteses em que agentes de tratamento podem se isentar da responsabilidade desde que comprovem circunstâncias na lei, ou seja, quando não ocorreu violação à lei, deve assim a responsabilidade ser analisada de acordo com a situação.

Portanto a responsabilidade civil das empresas pela LGPD mostra uma proteção dos titulares e responsabilização dos agentes que descumprem os deveres, mas acima disso a responsabilidade civil e a LGPD servem para promover maior confiança nas relações entre titular e controlador, garantindo uma proteção maior e mais confiável aos titulares para liberarem seus dados para uma determinada empresa, sabendo que em casos de erros de tratamento as empresas serão responsabilizadas de acordo com a própria Lei.

5. Medidas preventivas para proteção dos dados pessoais.

A adoção de medidas preventivas é extremamente fundamental visando garantir a proteção de dados pessoais, assim como reduzir os riscos de vazamentos e acessos não autorizados nas empresas. Nessa ideia, é essencial que as organizações e instituições adotem e implementem políticas internas de segurança, adotem procedimentos adequados para tratar informações em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), assim como capacitar seus colaboradores. Dessa forma, este capítulo vai abordar a importância das medidas preventivas e do compliance para prevenir incidentes que envolvam dados pessoais, destacando sua contribuição para a segurança das informações.

5.1 Medidas preventivas para evitar vazamentos de dados

Com base na Randoncorp, algumas medidas são utilizadas para evitar o vazamento de dados, como medidas pode se entender:

Uma das primeiras medidas para evitar vazamentos de dados é a utilização de senhas fortes e difíceis de adivinhar. Senhas muito simples ou que seguem padrões comuns facilitam o trabalho de pessoas mal-intencionadas que tentam acessar contas e sistemas sem autorização. Por isso, é importante utilizar combinações de letras, números e caracteres especiais, evitando informações pessoais que possam ser facilmente descobertas.

Outra medida importante é a autenticação em dois fatores, que acrescenta uma etapa de segurança no momento do acesso. Mesmo que alguém consiga descobrir a senha de um usuário, será necessário realizar uma segunda verificação, geralmente por meio de um código enviado ao celular ou aplicativo. Dessa forma, as chances de uma pessoa não autorizada conseguir entrar na conta são reduzidas. Também merece destaque o controle de acesso, que consiste em limitar a entrada nos sistemas apenas às pessoas autorizadas. Isso pode acontecer por meio de reconhecimento facial, biometria ou outras formas de identificação, dificultando o acesso de terceiros.

A criptografia também possui um papel importante nesse processo, pois transforma as informações em códigos que dificultam sua leitura por pessoas que não possuem autorização. Além disso, é fundamental que os programas e sistemas utilizados pelas empresas estejam

sempre atualizados, uma vez que as novas versões costumam corrigir falhas de segurança e melhorar a proteção contra possíveis ameaças.

Outro recurso que merece atenção é o uso de antivírus e ferramentas de proteção digital, que ajudam a identificar arquivos suspeitos, bloquear ameaças e alertar sobre possíveis tentativas de invasão. Da mesma forma, o certificado SSL contribui para a segurança dos sites, pois permite a criptografia das informações transmitidas entre o navegador do usuário e o servidor, protegendo dados durante o acesso e o envio de informações.

Por fim, a realização de backups periódicos é uma medida indispensável, pois permite recuperar arquivos e informações importantes caso aconteça algum problema, como falhas nos sistemas, ataques virtuais ou exclusões acidentais. Manter cópias de segurança atualizadas ajuda a evitar perdas maiores e garante que a empresa consiga dar continuidade às suas atividades.

Diante desses cuidados, fica evidente que a prevenção de vazamentos depende da adoção de diferentes medidas de segurança, que precisam funcionar em conjunto. Quando essas práticas são aplicadas corretamente, tanto as empresas quanto os usuários conseguem reduzir os riscos de exposição de informações, preservando a privacidade e a segurança dos dados pessoais em um cenário cada vez mais dependente da tecnologia.

6. Conclusão

Após análise do artigo e da problemática dos tratamentos de dados e de como as empresas devem ser responsabilizadas por isso, conclui-se que a responsabilidade civil das empresas pelo vazamento de dados é um tema muito atual e crescente com o grande avanço da tecnologia, já que as informações pessoais estão presente em inúmeros aspectos do dia a dia. As empresas controladoras desses dados possuem responsabilidade e quando for comprovado mediante ao que está na Lei devem reparar o titular dos dados, porém a proteção desses dados vai muito além do cumprimento de obrigações legais, pois envolve o respeito a privacidade que é um direito fundamental, à segurança e a confiança das pessoas que compartilham seus dados e informações para diversas empresas e instituições.

Nesse sentido, quando em determinado caso ocorrer vazamento de algum dados, os prejuízos podem ultrapassar as perdas financeiras, e chegam a atingir também a intimidade, tranquilidade e principalmente a segurança dos indivíduos, logo por isso é fundamental que as

empresas entendam que é de suma importância cuidar das informações que recebem com enorme seriedade e que como abordado no artigo, adotem medidas preventivas para evitar que ocorram vazamento e que ajam com responsabilidade diante de possíveis incidentes quando devem ser responsabilizadas pelos mesmo e que comuniquem a ANPD (Agência Nacional de Proteção de Dados), quando for necessário.

Assim a proteção de dados deve ser vista como um compromisso ético com a sociedade, para evitar que dados pessoais, sensíveis e importantes não sejam vazados e estejam livres onde não deveriam estar e que não sejam apenas uma mera exigência jurídica embasada em uma Lei, mais do que evitar penalidades, proteger os dados pessoais é um interesse comum dos cidadãos e isso demonstra o respeito, a preservação da confiança e acima de tudo contribui para um ambiente digital mais seguro e responsável, já que nos dias atuais, a internet tem acarretado em diversos desafios, com diversos dados vazados e usos indevidos dos mesmos.

Por fim, vale destacar que a efetiva proteção dos dados pessoais, não é algo que depende apenas de uma lei existente, mas sim parte da conscientização das empresas e da sociedade sobre os riscos envolvidos no uso inadequado dessas informações, logo as organizações precisam entender que a confiança dos titulares é feita por meio de atitudes responsáveis e transparentes. Dessa maneira, a segurança e prevenção representam um grande passo para reduzir casos de vazamento e uso indevido de dados e que as empresas se forem responsáveis devem sim serem responsabilizadas, e arcar com eventuais indenizações e danos morais e patrimoniais.

Referências

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 out. 2026.

CNN. **Brasil foi 7º maior alvo de ataques digitais em 2025; veja como se proteger.** 10 fev. 2026. Disponível em: https://www.cnnbrasil.com.br/economia/money/tecnologia/brasil-foi-7o-maior-alvo-de-ataques-digitais-em-2025-veja-como-se-proteger/. Acesso em: 14 out. 2026.

FORTINET. **O que é vazamento de dados? Causas e prevenção.** [20--]. Disponível em: https://www.fortinet.com/br/resources/cyberglossary/data-leak. Acesso em: 14 out. 2026.

GARCIA, Lara R. **Lei geral de proteção de dados pessoais (LGPD).** São Paulo: Editora Blucher, 2020. *E-book* (16 p.). ISBN 978-65-550-6016-4. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786555060164/. Acesso em: 08 out. 2026.

GONÇALVES, Carlos R. **Direito Civil Brasileiro - Responsabilidade Civil Vol.4 - 21ª Edição 2026.** 21. ed. Rio de Janeiro: SRV, 2025. *E-book* (9 p.). ISBN 978-65-840-0453-5. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786584004535/. Acesso em: 11 out. 2026.

RANDONCORP. **Vazamento de dados: 8 dicas para evitar que ocorra em sua empresa.** 30 abr. 2025. Disponível em: https://www.randoncorp.com/pt/blog/vazamento-de-dados/. Acesso em: 14 out. 2026.

MICROSOFT. What is a data leak? Microsoft Security, [s. d.]. Disponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-a-data-leak. Acesso em: 19 out. 2026.

TRIBUNAL REGIONAL ELEITORAL DO PARANÁ (TRE-PR). O que são dados pessoais? Disponível em: https://www.tre-pr.jus.br/transparencia-e-prestacao-de-contas/lei-geral-de-protecao-de-dados/o-que-sao-dados-pessoais. Acesso em: 19 out. 2026.

TUDO CELULAR. Vazamento em servidor expõe dados de milhões de brasileiros. TudoCelular, [s. l.], [s. d.]. Disponível em: https://www.tudocelular.com/seguranca/noticias/n265953/vazamento-servidor-expoe-dados-milhoes-brasileiros.html. Acesso em: 2 nov. 2026.