

**PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS**

**ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS**

**NÚCLEO DE PRÁTICA JURÍDICA**

**COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO**

**ARTIGO CIENTÍFICO**

**A LEI 13.709/2018 E OS NOVOS DESAFIOS DE PROTEÇÃO DE DADOS PESSOAIS E IDENTIDADE**

OS DADOS SENSÍVEIS DA LEI LGPD

ORIENTANDO (A): Sablyne da Silva Cunha.

ORIENTADOR (A): PROF. (A): ME José Humberto Abraão Meireles.

GOIÂNIA-GO

2022

SABLYNE DA SILVA CUNHA

**A LEI 13.709/2018 E OS NOVOS DESAFIOS DE PROTEÇÃO DE DADOS PESSOAIS E IDENTIDADE**

OS DADOS SENSÍVEIS DA LEI LGPD

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUC GOIÁS).

Prof. Orientador: ME José Humberto Abrão Meireles.

GOIÂNIA-GO

2022

SABLYNE DA SILVA CUNHA

**A LEI 13.709/2018 E OS NOVOS DESAFIOS DE PROTEÇÃO DE DADOS PESSOAIS E IDENTIDADE**

OS DADOS SENSÍVEIS DA LEI LGPD

Data da Defesa: 18 de maio de 2022

BANCA EXAMINADORA

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Orientador: Prof. ME José Humberto Abrão Meireles Nota

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Examinador (a) Convidado (a): Prof. (a): ME Eufrosina Saraiva Silva Nota

**A LEI 13.709/2018 E OS NOVOS DESAFIOS DE PROTEÇÃO DE DADOS PESSOAIS E IDENTIDADE**

OS DADOS SENSÍVEIS DA LEI LGPD

Sablyne da Silva Cunha[[1]](#footnote-1)

 O presente artigo visou discorrer sobre a atuação da LGPD na proteção dos dados sensíveis do titular ou de terceiros. A informação é o novo elemento que organiza a sociedade, ainda que essa forma de comunicação não se resuma apenas no ambiente virtual, mas a computação eletrônica e a internet são ferramentas de destaque neste processo. Diante disso, levando em conta a importância deste processo, buscou-se investigar a relação dos bancos de dados eletrônicos, e em especial como o indivíduo tem se modificado e adaptado a essa nova era da informação. Portanto, há um respaldo da legislação brasileira através da Lei 13.709/18 e a Lei 12.965/14, que asseguram a proteção dos dados pessoais de todos os usuários. Logo, este artigo utilizou-se como aporte teórico, o método de estudo exploratório, a exploração bibliográfica e o uso do critério dedutivo, com escopo de assegurar que a lei LGPD é essencial para proteger os direitos fundamentais de liberdade e de privacidade dos indivíduos. Enfim, a lei de proteção de dados proporcionou resultados positivos e transformou a ciência jurídica de modo a aperfeiçoa-la, fornecendo resultados mais reais para um mundo cada vez mais conectado e complexo.

**Palavras-chave:** Proteção dos dados. Internet. Usuários.

**SUMÁRIO**

**INTRODUÇÃO.............................................................................................................5**

**1. A identidade na era da informação.......................................................................8**

1.1 A construção da identidade pessoal e a tecnologia da comunicação na comunidade..................................................................................................................8

1.2 O paradigma da privacidade na era da informação................................................9

1.3 Marco civil e a lei de proteção de dados................................................................11

**2. A inovação da lei 13.709/2018..............................................................................14**

2.1 Agentes responsáveis pelo o tratamento de dados pessoais............................... 14

2.2 O papel da compliance na LGPD.......................................................................... 14

2.3 As inovações da LGPD brasileira face ao direito comparado................................16

**3. Os dados sensíveis e o tratamento de dados pessoais com direito a distinção e não a discriminação...............................................................................................19**

3.1 O tratamento dos dados sensíveis pela LGPD......................................................19

3.2 Casos emblemáticos de vazamentos de dados sensíveis nas redes sociais.......20

**4. CONSIDERAÇÕES FINAIS...................................................................................22**

**5. REFERÊNCIAS......................................................................................................24**

**INTRODUÇÃO**

A tecnologia em seu estado atual influencia cada vez mais a vida dos indivíduos de forma que, com a criação de novos meios e reinvenção dos antigos, fez-se surgir uma nova problemática em relação ao modo de como são utilizadas estas tecnologias.

Um dos maiores avanços recentes na comunicação humana é a popularização da internet e a revolução tecnológica de massas trazida por ela. O que em seus primórdios era de acesso restrito e para fins específicos, veio a se tornar um meio de comunicação massificado, englobando em si inúmeros aspectos da vida cotidiana como trabalho, estudo, comunicação, lazer e comercio, de modo que é possível as gerações mais novas usufruírem do uso de ferramentas de comodidade como sites de buscas, redes sociais, sites de entretenimentos.

Com isso, na era da informação, os dados pessoais são manipulados com facilidade, apesar do titular ter o seu consentimento ao fornecer os seus dados nas redes sociais é de suma importância todo cuidado possível do cidadão, que somente deve fornecer os seus dados, a sites e aplicativos confiáveis, ou seja, antes de passar os seus dados pessoais, deve-se tomar cuidados como: verificar o nome do site, verificar se o site faz parte de um portal, não agir pela curiosidade de acessar qualquer link e evitar clicar em links recebidos por e-mails.

Nesta perspectiva, em 2020 entrou em vigor a Lei Geral de Proteção de Dados Pessoais (LGPD), aprovada no ano de 2018, representando um marco na defesa da privacidade Brasileira. Desta maneira, a Lei Geral de Proteção de Dados Pessoais, tem como objetivo a proteção da liberdade, tanto virtual como física do ser humano, além da promoção e do livre desenvolvimento da sua personalidade.

 Em suma, após o facebook colher e comercializar, sem autorização prévia, dados de aproximadamente 270 milhões de pessoas. Assim, forneceu uma brecha em seus termos e condições de uso. Tais informações foram utilizadas, por exemplo, para a promoção da campanha do então candidato à Presidência dos Estados Unidos *Donald Trump*.

O descumprimento da lei mencionada pode render multas de 2% do faturamento da empresa. Porém, esse preço é limitado pelo o teto máximo de cinquenta milhões de reais. Cada vazamento poderá ser considerado como uma violação individual, rendendo possíveis prejuízos para a empresa causadora do dano.

 A seguir, considerando tais informações, indagamos: quais os desafios acerca da confidencialidade das vítimas dos ataques virtuais?

 Um dos principais desafios acerca da confidencialidade dos ataques virtuais é fazer com que a informação seja restrita e esteja somente disponível para usuários autorizados.

 Sendo assim, o objetivo geral da presente pesquisa é descrever sobre a construção de identidade pessoal das pessoas, diante do avanço tecnológico e da era da informação. Logo, a Lei Geral de Proteção de Dados Pessoais se manifestou com o propósito de proteger os direitos fundamentais de liberdade e de privacidade de todos os usuários.

Por tanto, foram delineados os seguintes objetivos específicos: garantir proteção à privacidade, na era da informação, assegurar os direitos e garantias dos cidadãos no ambiente eletrônico, com o uso do Marco Civil, definir os agentes responsáveis pelo o tratamento dos dados e levantar os tratamentos específicos de privacidade previsto pela LGPD.

A seguir, relatamos sobre o compliance, que envolve conjunto a serem adotados no ambiente corporativo para que reforce a segurança das empresas e de todos os usuários, a proteção dos dados sensíveis do titular ou de terceiros, adiante, abordamos casos emblemáticos de vazamentos de dados desses mesmos dados sensíveis.

Assim, para viabilizar o teste da hipótese, utilizamos da pesquisa exploratória e exploração bibliográfica, a seguir com o uso do método dedutivo que realizou uma breve abordagem usando o raciocínio logico que chegou a conclusões mais particulares.

Na primeira seção, abordamos o assunto da identidade na era da informação, que esclareceram acerca da construção identidade pessoal, com o fundamento na importância da tecnologia da comunicação, a seguir abordamos sobre o marco Civil.

 Na segunda seção, adentramos na Lei de Proteção de Dados, observamos os ensinamentos dos doutrinadores: Patrícia Peck Pinheiro e Bruno Ricardo Bioni, acerca dos agentes responsáveis pelo o tratamento da privacidade e em especial o papel da compliance na LGPD.

 Na terceira seção, falamos do tratamento dos dados sensíveis pela LGPD e abordamos casos emblemáticos de vazamentos desses dados sensíveis.

Ao final, conclui-se que os objetivos foram atendidos e a pergunta respondida com a confirmação da hipótese, indicando em especial a LGPD as empresas, que adotaram medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

1. **A IDENTIDADE NA ERA DA INFORMAÇÃO**
	1. **A construção da identidade pessoal e a tecnologia da comunicação na comunidade**

A identidade pessoal foi construída no decorrer da existência a partir de experiências individuais e coletivas do indivíduo.

Para Erikson (1972), construir uma identidade pessoal, implica em definir quem a pessoa é, quais são os seus valores e quais as direções que deseja seguir pela a vida.

O autor entende que a identidade é uma concepção de si mesmo, composto de valores crenças e metas com os quais os indivíduos estão solidariamente comprometidos.

A sociedade ao longo do tempo modificou-se com diversos aspectos de organização social, pelo qual se estruturou para estabelecer os marcos históricos.

Na sociedade agrícola, a fonte da riqueza provinha da terra. O chamado produto agrícola, que impulsionava a economia por meio da prática do escambo, tornou-se a primeira prática comercial.

Em seguida, foi criada a máquina a vapor e da eletricidade que tiveram o papel principal na produção fabril e, por seguinte, na formação das riquezas (sociedade industrial).

Adiante, após a segunda guerra mundial os serviços viraram papel principal de destaque socioeconômico.

“Segundo Bioni, Bruno Ricardo, a informação avoca um papel central e adjacente da sociedade: sociedade da informação. A informação é o novo elemento estruturante que reorganiza a sociedade, tal como fizera a terra, as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedades agrícola, industrial e pós industrial” (BIONI, BRUNO, 2021, p 5).

Posteriormente, após passar por toda evolução histórica, chegamos então ao que chamamos de era da tecnologia e da informação.

Logo, com o acesso à “internet/ computadores/ celulares”, as pessoas se conectam as redes sociais, aplicativos e sites de entretenimento.

A sociedade em geral se aprimorou com o avanço tecnológico, o criativo entrou na vida de adolescentes, jovens e adultos de forma avassaladora. Abarcando novas aprendizagens, como por exemplo, o uso de bancos virtuais, que não possui agência física, mas ainda assim, é de fácil acesso e segurança para que o indivíduo consiga fazer as suas transações com facilidade, sem nenhuma burocracia, apenas pelo o uso do aplicativo.

Os chamados bancos virtuais fornecem ao cliente cartão de crédito, cartão de débito, pagar boletos pelo o próprio aplicativo, transferir dinheiro pela modalidade pix através do uso de uma chave de segurança que identifique a conta da pessoa desejada para a transferência do dinheiro.

O avanço tecnológico é tão ágil, que hoje é raro encontrar um cidadão que não se utiliza destes benefícios virtuais, como a transação de dinheiro e o uso do pix, que facilita e resolve o problema de muitas empresas e comércios, tanto para pagamentos, quanto para recebimentos.

As redes sociais firmam seu espaço como importante ferramenta de respaldo na construção das identidades pessoais. Em uma época em que cada vez mais pessoas se utilizam desse tipo de recurso, as redes ganham corpo de intensa influência e relevam-se não como uma tendência passageira, mas como algo que modifica radicalmente as formas de relacionamento na sociedade, chamada por muitos de vitrine, ou seja, local para expor serviços e atrair clientes, o que vem acontecendo na atualidade, grandes marcas estão desacelerando seus investimentos na publicidade tradicional para contar cada vez mais com os chamados influenciadores digitais.

As redes sociais se tornaram trabalho para muitos, uma fonte de renda que garante bons ganhos se a pessoa que se apresenta como titular do perfil na rede social for muito assistida, e conseguir por consequência, incentivar que seus seguidores consumam algo que o influenciador indique.

* 1. **O paradigma da privacidade na era da informação**

O paradigma da privacidade remete a defesa da inviolabilidade, fato consagrado pela Constituição e por leis que delas resultam. A crucial indagação deste artigo envolve a discussão acerca da privacidade na era da informação com o acesso à evolução tecnológica.

‘’Ulrich Bech, ao desenvolver a ideia do que entende ser a sociedade de riscos, menciona conceitos como “riscos” e “perigo”, assinalando ao final que tais expressões são sinônimas. Ademais, assevera que tal sociedade ganha nova dimensão, sendo um verdadeiro novo paradigma manifestado por duas vertentes: os riscos da modernização e as contradições imanentes entre a modernidade e a contramodernidade da sociedade pós industrial, os perigos irreversíveis para os indivíduos.’’ (XAVIER, MARCELO, 2011, p.12).

É notório que cada revolução industrial passou por uso de um determinado componente para se tornar extremamente importante. A primeira foi o carvão, a segunda a eletricidade e a terceira sem dúvidas mais importante a invenção da internet. Nesse sentido, o teórico da comunicação, Marshall McLuhan, já prévia um número cada vez maior de pessoas conectadas há uma única rede.

A informação assume a maior relevância na sociedade democrática. Por meio disto, ela traz um limite ao direito de informar no qual o valor protegido é a privacidade do indivíduo.

Todavia, há também a consideração do sigilo que pretende proteger aspectos mais palpáveis como informações, senhas e segredos que se revelados pode causar danos desfavoráveis às vítimas, e é exatamente este o paradigma da privacidade: a proteção contra invasões de dados pessoais, que pode ser usado para gerar vantagem contra um indivíduo.

Como ferramenta de proteção do sigilo dos dados disponibilizados pelo usuário da internet, o mais comum é a criptografia, que é um conjunto de técnicas pensadas para proteger os dados fornecidos em ambiente virtual. A criptografia busca obscurecer o conteúdo fornecido pelo usuário da internet. Esse obscurecimento se dá por meio de algoritmos matemáticos que codificam os dados que o usuário de forma que só ele tenha acesso aos dados que expos na internet.

Embora, na Lei da LGPD em especifico não é mencionado em seus artigos a palavra criptografia. Entretanto, a LGPD menciona justamente a palavra “ininteligível”.

Nesse sentido, a criptografia faz com que uma informação/mensagem se torne ininteligível, ou seja, de difícil compreensão por aqueles que não dominam ou reconhecem o código/ linguagem que a mensagem foi traduzida. Isto porque a LGPD, ao tratar de segurança e sigilo de dados, afirma que se houver a ocorrência de incidente de segurança com os dados pessoais (ou seja, vazamento de dados, roubo de dados, etc.) a autoridade nacional irá avaliar justamente se foram adotadas técnicas adequadas que tornem os dados afetados pelo incidente de segurança ininteligível, ou seja, de difícil compreensão e decodificação por parte de quem teve acesso indevido aqueles dados, e a criptografia é, sem dúvidas, uma técnica adequada para deixar a informação ininteligível.

Por fim, a criptografia é um dos meios mais seguros para proteger todos os dados que forem fornecidos na internet, uma vez que oculto informações através de códigos. Desse modo, o remetente e o destinatário precisam de chaves para decifrar os dados. E a única fora de acessar os dados é por meio de um dos computadores utilizados na comunicação, do emissor ou receptor.

* 1. **Marco Civil da Internet e a Lei de Proteção de Dados**

O Marco Civil da Internet (MCI) é importante na era da informação para assegurar os direitos e garantias dos cidadãos no ambiente eletrônico. Para confirmar essa esfera de controle de usuários sobre os seus dados pessoais, o Marco civil da internet dispõe que o usuário poderá requerer a exclusão definitiva de seus dados pessoais fornecidos a uma determinada informação na internet, uma vez encerrada a relação entre eles.

Assim, o usuário da rede tem garantia de que sua vida privada não será violada, a qualidade da conexão estará em conformidade com o contrato e os seus dados só serão passados a terceiros, segundo o seu consentimento ou em casos judiciais. Nesse sentindo, a lei regula o monitoramento, filtro, análise, e fiscalização de conteúdo para garantir o direito à privacidade.

Essa perspectiva de controle perpassa desde a fase de coleta e compartilhamento dos dados com terceiros até o direito de apagá-los junto ao prestador de serviços e produtos de internet ao término da relação.

No Marco civil da internet foi definida em seu art. 5°, inciso I: “O sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes”. (Lei 12.964/2014)

Além disso, o conceito legal de internet é importante, pois complementa uma lacuna gigante na comunicação. A legislação brasileira é conhecida por deixar brechas que posteriormente precisam ser supridas pela doutrina ou pela jurisprudência. Nesse caso, ao editar o artigo 5°, a lei 12.964/2014, obteve um grande acerto, pois assegura os dados dos usuários perante as diferentes redes.

Contudo, o Marco Civil tem em seu corpo normativo as regras base de proteção de dados pessoais: (Consentimento).

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: VII - Não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; IX - Consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais.

A utilização dos dados deve ser compatível com o contexto em que os dados foram coletados.

Por outro lado, a lei geral de proteção de dados (Lei nº 13.709/18), mais específica, é regida para assegurar os dados de todos os usuários. Essa norma de proteção de dados aplica-se tanto ao setor público quanto ao privado, e a qualquer tratamento de dados pessoais de pessoas naturais.

Por tratamento de dados pessoais entende-se: toda operação realizada com dados pessoais, como as que referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência.

No art. 2, da lei 13.709/2018, apresenta-se os sete fundamentos que estabelecem as diretrizes da proteção de dados pessoais, são eles: O respeito a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa a livre concorrência e a defesa do consumidor: e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Porém, é importante ressaltar que tanto o Marco Civil quanto a LGPD tratam de relações na Internet sendo que, a primeira legislação trata das garantias, direito e deveres em rede, ao passo que a LGPD se centra nas circunstâncias de tratamento dos dados fornecidos pelo o usuário, ou seja, na proteção de dados de pessoas física.

Por fim, a Lei Geral de Proteção de Dados Pessoais e o Marco Civil da Internet, andam lado a lado, de forma que se complementam, e são leis que provavelmente passarão por constantes evoluções legislativas a fim de aprimorar a proteção dos dados pessoais a todos os usuários.

1. **A INOVAÇÃO DA LEI 13.709/2018.**

 **2.1 Agentes responsáveis pelo o tratamento de dados pessoais**

A Lei 13.709/2018 prevê os agentes responsáveis pelo o tratamento de dados pessoais, destacando entre: Controlador, Operador e Encarregado.

O agente controlador, tem como papel principal garantir a transparência e a comunicação com o titular dos dados pessoais, a criar canais de comunicação para que os titulares dos dados tenham segurança e acesso facilitado as suas próprias informações. Assim, a obrigação do controlador é responder por danos morais e coletivos, e com qualquer outro tipo de descumprimento da legislação.

Logo, o agente operador, refere-se a uma pessoa natural ou jurídica, que possui o direito público ou privado. Por outro lado, o operador fica responsável em realizar o tratamento de dados pessoais, em nome de um controlador. Diante disto, o operador deverá realizar os devidos tratamentos de dados pessoais, de acordo com as obrigações da lei, assim, respeitando as diretrizes, política de segurança e privacidade do controlador.

Por fim, o agente encarregado, é aquela pessoa definida pelo o controlador ou operador, para que pudesse atuar dentro do canal de comunicação, que existe entre os controladores, os titulares dos dados pessoais e a Autoridade Nacional de Dados Pessoais (ANDP).

 **2.2 O Papel do Compliance na LGPD**

O compliance é um termo da língua inglesa que deriva verbo “*to comply”*, que se tornou um grande amparo para quem precisa falar sobre conformidade. Por seguinte, em uma situação livre para a língua portuguesa, significa, cumprir obedecer e executar aquilo que foi determinado.

Outrora, o Compliance visa garantir que a empresa atue de acordo e em conformidade com as regras, leis e regulamentações aplicáveis. Em razão disso, o compliance desempenhará um papel importante na vigência da LGPD. Assim, as empresas que possuem o programa *compliance* terão facilidade e economia para se adequar, justamente para que as empresas consigam trabalhar dentro da ética e tenha uma boa governança, sempre de acordo com a lei vigente da LGPD.

Na pratica, quer dizer que as empresas terão que rever seus processos que envolvam coleta e armazenamento de dados pessoais. Assim, é necessário uma reorganização e replanejamento das empresas, no intuito de identificar todos os dados pessoais sobre seu poder, e alinha-los as bases legais previstas na própria lei que á complementa.

‘’Em suma, levando em consideração que: O mercado tratava os dados coletados como ativo próprio, que poderia ser livremente utilizado e comercializado por quem deles se apropriasse. Agora a perspectiva é inversa: os dados coletados continuam a pertencer às pessoas às quais se referem, de modo que o coletor dos dados deve prestar conta do uso deles que foi feito’’ (REUTERS, THOMSON, 2019, p.694)

 Diante disso, os direitos e princípios contidos na LGPD, se reconduzem a ideia básica do dever de prestar contas, já que o agente de tratamento de dados lida com os bens alheios e de extrema relevância. Esse dever essencial é gratuito, e envolve a obrigação de corrigir informações para que os dados reflitam a realidade e não dificultem os exercícios de direitos fundamentais da pessoa natural.

Finalmente, o compliance de dados pessoais volta-se justamente para auxiliar os agentes de tratamento de dados a aplicar de forma eficaz as normas de proteção de dados e guiará a pessoa jurídica a conservar esses dados e toda a sua atividade dentro dos ditames legais, utilizando da informação em prol da minimização de incidentes que impliquem na responsabilidade empresarial.

Conforme, o autor Thomson, existem três pilares que são primordiais para reforçar o papel do compliance na LGPD no âmbito da proteção dos dados pessoais. Primeiramente, o amplo escopo de incidência da LGPD, em decorrência dos dados pessoal, de tratamento e de banco de dados, torna-se necessária a adaptação não apenas de atividades centralizadas na coleta/ou no tratamento de dados, mas mediante qualquer operação que transcorre, ainda que indiretamente, a sua utilização de informações relacionadas a pessoas naturais.

Além disso, dentro das empresas, até mesmo nas atividades mais simples, terão que se adequar à lei, levando em consideração as informações que dizem respeito aos empregados, desde que, também as listas dos clientes se sujeitem à LGPD.

Neste contexto, observa-se que a compliance de dados não se limita apenas no relacionamento com os consumidores, mas acaba repercutindo em várias esferas da atividade empresarial, a demandar adaptação também de setores que, a princípio, não estariam diretamente ligados a LGPD. No entanto, o compliance refere-se mais uma vez, a relação de trabalho: as regras de concordância adotadas nesse setor deveram ser atualizadas para apreciar também as normas da LGPD, desde que, evitem, por exemplo, que ocorra a coleta de dados desnecessários.

A seguir, um segundo fator está associado ao primeiro: uma vez que são diversas as atividades que deveram cumprir as normas da LGPD, ou seja, dentro de cada mandato da lei, níveis de exigências distintos e necessários para as hipóteses de tratamento dos dados envolvidos, até mesmo com a intenção de evitar que a proteção termine tornando inviável a exploração de certas atividades econômicas.

Por fim, o terceiro fator consiste na necessidade de conferir se é real algumas normas empregadas pela a LGPD, desde que, permitam que sejam adotados comportamentos em conformidade com a lei.

 **2.3 As Inovações da LGPD em face ao Direito Comparado**

No Brasil, a Lei Geral de Proteção de Dados Pessoais, inspirou-se na legislação europeia. Portanto, a LGPD estabelece que não importa se a sede de uma organização ou o centro de dados de uma organização estejam localizados no Brasil ou no exterior: se houver processamento de conteúdo de pessoas, brasileiros ou não, que estejam no território nacional, a LGPD deve ser cumprida.

A lei geral de proteção de dados pessoais é válida nos setores públicos, privados, em hospitais, bancos virtuais, sites, aplicativos, redes sociais. Com isso, a Lei 13.709/2018 afeta diferentes setores e serviços, seja no papel de indivíduo, empresa ou governo.

O elemento essencial da LGPD é o consentimento do cidadão que visa tratar dos dados pessoais. Logo, só é possível tal tratamento sem o consentimento, se for necessário cumprir obrigações legais, fazer cumprir a política pública prescrita em lei, realizar pesquisas por meio de instituições de pesquisa, fazer cumprir contratos, defender direitos em litígios, proteger a conduta dos profissionais da saúde, prevenir fraudes contra titulares, proteger o crédito, satisfazer interesses legítimos e não violar os direitos fundamentais dos cidadãos.

Embora, por falar em direitos, sabe-se que a lei traz garantias para o cidadão, que pode solicitar que os dados dos usuários sejam deletados, assim, podendo revogar um consentimento, transferir dados para outro fornecedor de serviços, entre outras ações.

Dessa maneira, a LGDP teve suas inovações e o seu aparecimento das seguintes formas:

* 2010: Ministério da Justiça realiza consulta pública sobre o projeto de lei de proteção de dados pessoais.
* 2011: Lei de acesso à informação – LAI aprovada (fornecendo acesso público a dados pessoais).
* 2012: Foi promulgada a Lei Carolina Dieckman (criminalizando crimes cibernéticos, como compartilhamento não autorizado de dados pessoais). Proposta da Câmera PL n. 4060: sobre o tratamento de dados pessoais.
* 2013: O senado apresentou o Projeto de Lei 330 (PLS): Proteção, Processamento e uso de Dados Pessoais.
* 2014: Entra em vigor o Marco Civil da Internet.
* 2015: Aprovado pela a comissão de ciência e tecnologia do senado (CCT), em substituição ao PLS n°330/13: dispõe sobre a proteção, processamento e o uso dos dados pessoais.
* 2016: Aprovação do regulamento Geral sobre a Proteção de dados (*GDPR*).
* 2017: Dois projetos foram tratados na Assembleia Geral: PL n. 5.2786/2016: tratamento de dados pessoais para garantir o livre desenvolvimento da personalidade e dignidade das pessoas físicas, em salas de conferência, e PLS n. 330/13.
* 2018: Marco no escândalo do “Facebook *Cambridge Analytica*” (o uso ilegal de dados de usuários pela a empresa de consultoria). Em maio entrou em vigor o GDPR na Europa. E logo, em agosto foi sancionada a lei LGPD, após a unificação dos textos da câmara e do senado no PLC n°53: dispõe sobre a proteção de dados pessoais.
* 2019: Aprovada a criação da Autoridade Nacional de Proteção de Dados (ANPD), Pelo MP nº 869. Iniciada a discussão sobre a PEC nº 17, que inclui a proteção de dados pessoais, inclusive digitais, entre os direitos fundamentais do cidadão.
* 2020: Governo adia a vigência da LGPD para maio de 2021.

 Em síntese, em 01 de agosto de 2021 a Lei 13.709/2018 entrou em vigor.

1. **OS DADOS SENSÍVEIS E O TRATAMENTO DE DADOS PESSOAIS COM DIREITO A DISTINÇÃO E NÃO A DISCRIMINAÇÃO**
	1. **O tratamento dos dados sensíveis pela LGPD**

A Lei Geral De Proteção De Dados Pessoais (LGPD) define o dado sensível em seu art. 5º, inciso II: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, saúde, vida sexual, genética ou biometria, quando vinculado a pessoa natural. O conteúdo dos dados sensíveis trazidos no art. 5º, II, da LGPD são opções realizadas pelo legislador motivados pelo o efeito potencialmente lesivo do seu tratamento.

‘’De maneira diferente, Doneda compreende que os dados sensíveis seriam determinados tipos de informação que, caso sejam conhecidas e processadas prestar-se-iam a uma potencial utilização discriminatória ou particularmente lesiva’’ (DONEDA, 2003, p. 160-161).

Segundo o exposto, Doneda assume a posição de que esta categoria de dados é determinada de acordo com o efeito de seu tratamento em relação aos demais dados pessoais. O valor tutelado, nesse caso, seria a igualdade material, acima do conteúdo tradicional da privacidade, e a liberdade, que permitiria ao titular dos dados o exercício de direitos de maneira autônoma, sem limitações excessivas ou indevidas.

Em conformidade com o doutrinador Doneda, um dado, em si, não é perigoso ou discriminatório – mas o uso que ele se faz, pode sê-lo (DONEDA, 2003, p. 162). Em vista disso, pode concluir que o conceito de dados sensíveis deve ter funcionalidade de acordo com o tratamento que é concedido a eles.

A seguir, quando o foco for menor de idade, deve-se obter o consentimento expresso de um dos pais ou responsável para solicitar apenas o estritamente necessário para a atividade econômica ou governamental, e nenhum conteúdo pode ser repassado a terceiros. Sem o consentimento, só poderá coletar dados se for para urgências para entrar em contato com os pais ou responsáveis para proteger crianças e jovens.

Vale ressaltar, sobre os dados sensíveis, autônomos, empresas e governo também podem tratá-los se tiverem o consentimento explícito da pessoa, e para um fim definido. E, sem o consentimento do titular, a Lei Geral de Proteção de Dados Pessoais estabelece que isto é possível quando for indispensável em situações ligadas: a uma obrigação legal; a políticas públicas; a estudos via órgãos de pesquisas; a um direito, em contrato ou processos judiciais; á preservação da vida e da integridade física de um titular ou de um terceiro; à tutela dos procedimentos feitos profissionais das áreas de saúde ou sanitária; à preservação de fraudes contra o titular nos cadastros em sistemas eletrônicos.

 **3.2 Casos emblemáticos de vazamentos de dados sensíveis nas redes sociais.**

O vazamento de dados são sempre um sinal de alerta para as empresas e os consumidores. Podem expor e-mails, credenciais de redes sociais, registros médicos, propriedade intelectual, segredos de negócio, informações financeiros, bancários e entre outras informações sensíveis.

Diante o exposto, em 2019, ocorreu vazamento de dados sensíveis da empresa ‘’First American Corporation’’ de seguros e serviços financeiros. Cerca de 885 milhões de registros foram vazados, incluindo dados extremamente sensíveis contendo, por exemplo, informações bancárias detalhadas. Os documentos eram copias digitadas que podiam ser acessadas via o site da empresa ‘*’firstam.com*’’.

 Embora fossem documentos destinados à visualização apenas das partes envolvidas em uma transação (em grande parte da compra e venda de imóvel), estavam disponíveis ao acesso para qualquer pessoa, alterando um único digito e sem proteção de login, ou duplo fator de autenticação. O desenvolvedor Bem Shoval descobriu a falha da pior maneira possível: após visitar um link de seus próprios documentos.

Em dezembro de 2020, a reportagem do Jornal de São Paulo, revelou que dados de 243 milhões de brasileiros cadastrados no Sistema Único de Saúde (sus) ou beneficiários de planos de saúde ficaram expostos na internet por falhas de segurança do ministério de saúde.

As informações que ficaram expostas na internet, como nomes completos, CPFs, endereços e telefones, deveriam estar protegidas por login e senha, mas havia uma vulnerabilidade no código que permitia que qualquer usuário consultasse o banco de dados.

A Open Knowledge Brasil (OKBR), uma organização do terceiro setor que promove segurança digital, transparência e acesso a dados públicos, relatou falhas semelhantes ao Ministério da Saúde.

 Em nota ao jornal, o Ministério da Saúde afirmou que os incidentes reportados foram investigados para apurar a responsabilidade da exposição de base cadastral do ministério. A pasta acrescentou também que, após o incidente do vazamento dos dados do Ministério da Saúde, ações foram tomadas para impedir novos incidentes, assim como ações administrativas para apurar o ocorrido.

 Desde então, outro sistema do Ministério da Saúde ficou fora da internet durante meses, por sua passível ação de Hackers. Em dezembro de 2020, o Data Sus ficou inacessível, deixando os cidadãos sem informações. O problema demorou quase um mês para ser sanado.

 Em suma, de acordo com os dois casos de vazamento de dados sensíveis apresentados, a Lei Geral de Proteção de Dados Pessoais apresenta possíveis sanções de advertência, multa diária, ou com limite de 2% do faturamento da empresa, bloqueio dos dados pessoais objeto da violação, suspensão parcial do funcionamento dos bancos de dados, e proibição parcial ou total do exercício da atividade relacionada ao tratamento de dados.

**CONSIDERAÇÕES FINAIS**

Este trabalho tem como analise de estudo a inovação tecnológica e digital que acaba influenciando o indivíduo na construção da identidade humana e como consequência, manifestando uma nova percepção da privacidade.

A Lei Geral De Proteção de Dados Pessoais tem como papel principal assegurar os direitos humanos, a dignidade, o exercício da cidadania nos termos da legislação.

Diante disto, o intuito da pesquisa é levantar os problemas relacionados a vazamento de dados pessoais na rede social. Apesar do cidadão ter o livre acesso ao termo de uso quando fornece os seus dados pessoais, eles ainda assim estão sujeitos a ataques que podem gerar danos.

A lei Geral de Proteção de Dados pessoais e o Marco Civil da internet andam lado a lado, de forma que se complementam, e são leis que provavelmente passarão por constantes evoluções legislativas a fim de aprimorar a proteção de dados pessoais para todos os usuários. Logo, tais leis, em especial a LGPD, são essenciais para a construção de respeito a identidade e privacidade dos indivíduos e foram idealizadas para transformar a ciência jurídica de modo a aperfeiçoa-la buscando resultados reais para um mundo cada vez mais conectado e complexo.

**LAW 13.709/2018 AND THE NEW CHALLENGES FOR PROTECTING PERSONAL DATA AND IDENTITY**

**THE SENSITIVE DATA OF THE LGPD LAW**

 This article aims to discuss the role of LGPD in the protection of sensitive data of the holder or third parties. Information is the new element that organizes society, although this form of communication is not limited to the virtual environment, but electronic computing and the internet are prominent tools in this process. Therefore, taking into account the importance of this process, we sought to investigate the relationship of electronic databases, and in particular how the individual has changed and adapted to this new information age. Therefore, there is support from Brazilian legislation through Law 13.709/18 and Law 12.965/14, which ensure the protection of the personal data of all users. Therefore, this article used as theoretical support, the exploratory study method, the bibliographic exploration and the use of the deductive criterion, with the aim of ensuring that the LGPD law is essential to protect the fundamental rights of freedom and privacy of individuals. Finally, the data protection law provided positive results and transformed legal science in order to improve it, providing more real results for an increasingly connected and complex world.

**Keywords:** Data protection. Internet. Users.

**REFERÊNCIAS**

MORAES, Alexandre de. **Curso de Direito Constitucional**. 26! ed. São Paulo: Atlas, 2010.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais**: comentários à Lei n.13.709/2018 (LGPD)/ Patrícia Pinheiro – 2. ed. ­– São Paulo: Saraiva Educação, 2020.

PINHEIRO, Patrícia Peck. **Direito Digital**.­ – 7, ed. – São Paulo: Saraiva Educação, 2021.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento – 3. ed. – Rio de Janeiro: Forense, 2021.

SERPRO. **Tratamento Dos Dados Sensíveis Pela LGPD**. Site: <https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-sensiveis-lgpd>;

REUTERS, Thomson. **Lei Geral De Proteção De Dados Pessoais E Suas Repercussões No Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019.

BLOG. **Vazamento de Dados**. Site: <https://www.gat.digital/blog/vazamento-de-dados/>;

ARAGÃO, ARAGÃO. **Vazamento de Dados.** Jota/mercado informações – São Paulo, reportagem publicada dia 28/01/2022, às 06:33, site:

<https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil-28012022>;

1. Qualificação do autor. [↑](#footnote-ref-1)