

GEOVANNA PEREIRA DE CASTRO DA SILVA

**DIREITO DIGITAL:
A ilusão de proteção de dados na internet**

GEOVANNA PEREIRA DE CASTRO DA SILVA

DIREITO DIGITAL:

A ilusão de proteção de dados na internet

Monografia apresentado ao Núcleo de Trabalho de Curso da Universidade UniEvangélica de Goiás, como exigência parcial para a obtenção do grau de bacharel em Direito, sob a orientação da Prof. M.e Camila Rodrigues de Souza Brito.

ANÁPOLIS – 2022

GEOVANNA PEREIRA DE CASTRO DA SILVA

DIREITO DIGITAL:
A ilusão de proteção de dados na internet

Anápolis, ____ de _____ de 2021.

BANCA EXAMINADORA

AGRADECIMENTOS

A minha mãe Lucimar que é minha inspiração, quando eu pensava em desistir, ela me encorajava com palavras de força, ao meu pai Joaquim, que com seu próprio jeitinho de demonstrar, tem grande orgulho desta minha fase. Agradeço pela formação que me deram, permitindo que eu chegasse a este fruto, espero passar um pouco de serenidade e da generosidade que me ensinaram, eu amo vocês.

RESUMO

O seguinte trabalho tem como objetivo analisar a importância da Lei Geral de Proteção de Dados, legislação que regula as atividades de tratamento de dados pessoais na internet, não é surpresa que em um mundo cada vez mais digitalizado é relevante estar ciente dos seus direitos ao navegar em um mar de tantas informações, entender como são usados seus dados pessoais, e entender principalmente de que forma esse acesso vem impactando em nossa vida. Sem dúvidas, a internet vem nos causando grande impacto, um detalhe a ser frisado, é a quantidade de dados pessoais que é compartilhado sem nossa anuência ao navegarmos na internet, os famosos cookies são um exemplo, pois a partir do momento em que você os aceita, ele recolher uma biografia de sua vida. Por isso e vários motivos, surge a importância de estudar e compreender o mundo digital. Com o avanço estrondoso da tecnologia estamos cada vez mais digitais, temos toda nossa vida registrada na internet, até mesmo de forma inconsciente. Assim, pode-se dizer que chegamos a um nível, onde sem o mundo tecnológico somos invisíveis, por isso eis a missão de conseguir visualizar todos esses parâmetros.

Palavras-chave: impacto, dados pessoais, mundo digital.

SUMÁRIO

INTRODUÇÃO	01
CAPÍTULO I – DIREITO DIGITAL	03
1.1 A importância e o conteúdo do Direito Digital no Brasil.....	03
1.2 Principais legislações sobre o Direito Digital no Brasil	05
1.3 Princípios do Direito Digital	08
CAPÍTULO II – A LEI GERAL DE PROTEÇÃO DE DADOS – LGPD	10
2.1 Objetivos da Lei Geral de Proteção de Dados	10
2.2 Regulamento Geral da Proteção de Dados – GDPR e a LGPD.....	11
2.3 Dos direitos do titular.....	13
2.4 Dos agentes de tratamento de dados pessoais	15
CAPÍTULO III – A ILUSÃO DE PROTEÇÃO DE DADOS NA INTERNET	19
3.1 Análise de casos concretos.....	19
3.2 Análise de decisões judiciais.....	22
CONCLUSÃO	29

REFERÊNCIAS.....	30
-------------------------	-----------

INTRODUÇÃO

O presente trabalho monográfico tem como objetivo analisar e estudar a importância da Lei Geral de Proteção de Dados, legislação que regula as atividades de tratamento de dados pessoais na internet, e destacar principalmente, a submissão a um sentimento de falsa proteção que os usuários vêm sofrendo cronologicamente.

A importância do entendimento do Direito Digital no Brasil e de que forma tal atualização vem impactando em nossas vidas, é grande objeto de estudo, da mesma forma, é indispensável o conhecimento as principais leis que regem o Direito Digital, com a finalidade de identificar o papel fundamental que tem em nosso cotidiano, dando ênfase aos princípios e valores que o digital adquiriu ao longo do direito.

Demonstrar de forma clara e objetiva o tratamento que a Lei Geral de Proteção de Dados vem atribuindo aos dados pessoais no meio digital, seja por pessoa natural ou pessoa jurídica, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, fornecendo assim, o livre desenvolvimento a personalidade da pessoa natural.

Por fim, apresentar o atual cenário da proteção de dados na internet, onde, embora esse tipo de ataque seja silencioso, o ambiente virtual está comprometido e infectado, e naturalmente, os processos de proteção e segurança da informação falham, cabendo assim decisões judiciais diante desses ataques.

Em mundo cada vez mais digitalizado, é relevante estar ciente dos seus direitos ao navegar em mundo digital coberto de informações, entender como são usados seus dados pessoais e o impacto que vem causando na vida em sociedade.

CAPÍTULO I – DIREITO DIGITAL

Esse capítulo apresenta a importância do entendimento do Direito Digital no Brasil e de que forma tal atualização vem impactando em nossas vidas, ressalta também as principais leis que regem o Direito Digital, identificando o papel fundamental que tem em nosso cotidiano, e por fim, descreve os princípios e valores que o digital adquiriu ao longo do tempo.

1.1 A importância e o conteúdo do Direito Digital no Brasil

A expressão “Direito Digital” refere-se ao conjunto de regras e princípios aplicados às tecnologias da informação, desta forma, o Direito Digital não se trata exatamente de um ramo novo e independente, mas sim de uma releitura do direito tradicional vista sob ótica moderna e adequada à era da hiperconectividade. (PROJURIS, 2021, *online*)

O direito digital consiste na evolução do próprio Direito, abrangendo todos os princípios, fundamentos e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas. (PECK, 2015, pag. 29)

A rápida evolução nesses últimos anos em relação ao uso da tecnologia não é novidade para ninguém, no nosso cenário atual é quase impossível viver sem o uso da internet. Principalmente após a pandemia covid-16, onde deixou evidente tal fato.

Acontece que nem sempre foi assim, no Brasil em especial, diante do episódio de isolamento social causado pela pandemia, diversas atividades

financeiras, comerciais, jurídicas, entre outras, foram obrigadas a migrar para o meio eletrônico. Foi à evolução mais rápida da história.

O Direito Digital abrange diversas áreas do direito, haja vista que diversos problemas surgem as mais variadas relações jurídicas, sempre em relação ao ambiente digital. Mas como todo lado da moeda, tamanho avanço trouxe também muita exposição, na qual se deve dar certa atenção, pelo fato de estarmos submetidos a um mar de informações. (PROJURIS, 2020, *online*)

Diante de uma simples observação, é possível analisar que ainda existe uma limitação de pessoas que tem ciência acerca do que realmente se trata o Direito Digital, e qual sua verdadeira importância para vida de pessoas física e jurídicas, por ser um ramo novo e ainda não integralmente explorado pelos profissionais, ainda tem muito a ser estudado. (DIGITAL, 2020, *online*)

O principal objetivo do Direito Digital é proporcionar as normatizações e regulamentações de uso dos ambientes digitais pelas pessoas, oferecendo principalmente proteção de informações existentes nesse espaço, assim, torna-se inquestionável a importância de ter ciência da garantia de seus direitos e proteção.

O Marco Civil da Internet, instituído pelo Poder Executivo e pelo Congresso através da Lei 12.965, é o mecanismo que regulamenta o uso da Internet no país, promove garantias e obrigações aos internautas e estabelece diretrizes sobre as relações sociais em ambientes virtuais. (BRASIL, 2014, *online*)

Podemos citar as seguintes garantias e obrigações como exemplo, a neutralidade da rede em não favorecer ou denegrir os usuários; liberdade de expressão no mundo virtual; responsabilizar-se pela conduta dos indivíduos cometidos e divulgados pela Internet; armazenamento de dados em determinadas circunstâncias exigidas por lei, para proteger a confidencialidade e privacidade dos indivíduos; obrigações do poder público antes da popularização da Internet no Brasil, entre outros.

Dessa forma, a Lei 12.965 desmistifica a Internet como “terra de ninguém” e permite que os usuários utilizem ferramentas e plataformas digitais cumprindo

suas garantias legais e sujeito à devida fiscalização pelas autoridades competentes. (BRASIL, 2014, *online*)

1.2 Principais legislações sobre o direito digital no Brasil

Diante do cenário de grandes inovações tecnológicas, houve o surgimento de leis marcadas por determinados episódios, nascidas diante de situações decorrentes do meio digital.

Podemos propor destaque a quatro principais legislações criadas, onde visualizaram essa necessidade.

Lei do Marco Civil – 12.965/2015.

Lei nº 12.965, de 23 de abril de 2015 que trata do Marco Civil da internet, estabelecem no artigo 3º os princípios que regem o uso da internet no Brasil, que incluem princípios para a proteção da privacidade e dos dados pessoais.

Em seu artigo 7º, vem assegurando os direitos e garantias como internauta, a inviolabilidade de sua comunicação fluxo e a confidencialidade e a inviolabilidade e confidencialidade de suas comunicações privadas armazenadas, exceto por ordem judicial.

O artigo 10º, nº 1, que trata exclusivamente da proteção dos registros, dos dados pessoais e das comunicações privadas, enuncia de forma muito clara a possibilidade de fornecer dados privados a pedido de um juiz, e estabelece que o responsável pela guarda dos dados seja obrigado a fornecê-lo se for solicitado judicialmente.

Se o responsável se recusar a fornecer os dados solicitados pelo juiz, poderá ser responsabilizado pelo crime de desobediência nos termos do artigo 330 do Código Penal.

Lei Carolina Dieckmann – 12.737/2012

Lei 12.737/2012, conhecida como a Lei Carolina Dieckmann, lei que criou o crime de invasão de dispositivo informático. Essa lei teve início principalmente, devido ao fato da invasão de dispositivo informático, acesso indevido, seguida do vazamento de fotos íntimas.

O nome advém de um caso ocorrido com a atriz Carolina Dieckmann. Em maio de 2011, um hacker (criminoso virtual) invadiu o computador pessoal da atriz, possibilitando que ele tivesse acesso a 36 fotos pessoais de cunho íntimo. De acordo com a denúncia, o invasor exigiu R\$ 10 mil para não publicar as fotos.

O primeiro artigo 154-A, propõe um crime denominado “hacqueamento de equipamentos de informática”, que inclui hackear qualquer outro dispositivo de computador, como smartphone, tablet, etc., conectado ou não à internet. Esta ação configura-se devido ser realizada em violação de um mecanismo de segurança com o objetivo de adulterar, obter ou destruir dados sem a autorização do proprietário do dispositivo. A regra também se aplica a qualquer pessoa que instale *exploits* (software), como vírus, em seus dispositivos para obter ganhos ilícitos.

Quem produzir, oferecer, distribuir, vender ou divulgar programas de computador ou equipamentos que permitam essa prática também sofrerá as consequências do crime.

Lei que criminaliza o *stalking* e *cyberstalking*– 14.132/2021

O presidente da República, Jair Bolsonaro, sancionou a lei que tipifica o crime de perseguição, prática também conhecida como *stalking*, lei 14.132, de 2021. A norma altera o Código Penal (Decreto-Lei 3.914, de 1941) e prevê pena de reclusão de seis meses a dois anos e multa para esse tipo de conduta. (DIÁRIO OFICIAL, 2021, *online*)

O crime de *stalking* é definido como perseguição reiterada, por qualquer meio, como a internet *cyberstalking*, que ameaça à integridade física e psicológica de alguém, interferindo na liberdade e na privacidade da vítima.

A nova lei é oriunda do PL 1.369/2019, de autoria da senadora Leila Barros (PSB-DF). A matéria foi aprovada em 9 de março de 2021, como substitutivo da Câmara dos Deputados e teve relatoria do senador Rodrigo Cunha (PSDB-AL). (SENADO NOTICIAS, 2021, *online*)

É importante destacar que o avanço das tecnologias e o uso em massa das redes sociais trouxeram novas formas de crimes. Com a nova legislação poderemos agora mensurar com precisão os casos que existem no Brasil e que os criminosos não fiquem impunes como estava ocorrendo antes de sancionara lei.

Lei Geral de Proteção de Dados – 13.709/2018

LGPD é a sigla adotada para designar a Lei Geral de Proteção de Dados (Lei nº 13.709). Sancionada em 14 de agosto de 2018 pelo presidente Michel Temer, a Lei Geral de Proteção de Dados entrou em vigor em agosto de 2020 e afetou a maioria das empresas brasileiras, onde tem como principal objetivo, a proteção dos direitos fundamentais de liberdade e de privacidade e a permissão do livre desenvolvimento da personalidade da pessoa natural. (JURIDICO, 2019, *online*)

A lei surgiu com a finalidade de garantir soberania ao seu titular, ou seja, os usuários da tecnologia, a fim de regular atividades relacionadas à coleta de dados, e a criação de estruturas de fiscalização e responsabilidade.

Em seu artigo 2º a LGPD apresenta um leque de fundamentos, incluindo:

I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018, *online*)

Assim como há bases legais para o tratamento de dados pessoais, existe a obrigatoriedade do término de tratamento dos dados quando a finalidade é alcançada, quando os dados deixam de ser necessários, quando do fim do

tratamento ou quando da comunicação do titular e revogação do consentimento. (Alves Fernandes, 2020, *online*)

Devido ao fato de muitos desconhecerem a LGPD, fomenta que está veia a prejudicar os negócios e impedir o tratamento de dados pessoais na internet, o que está equivocado. A verdade é que a LGPD, veio para regulamentar à forma indiscriminada com qual tratam nossos dados pessoais. (BRUNELLI, 2022, *online*)

1.3 Princípios do direito digital

Na visão de Marcelo de Camilo Tavares Alves, ele entrega a seguinte definição baseada em princípios:

Direito Digital é o resultado da relação entre a ciência do Direito e a Ciência da Computação sempre empregando novas tecnologias. Trata-se do conjunto de normas, aplicações, conhecimentos e relações jurídicas, oriundas do universo digital. (Tavares, 2009, *online*)

O Marco Civil da Internet apresenta princípios que podem também ser estabelecidos com princípios do Direito Digital no Brasil, sejam eles:

Garantia da liberdade de expressão, comunicação e manifestação do pensamento; proteção da privacidade; proteção dos dados pessoais; preservação e garantia da neutralidade da rede, entre outros. (BRASIL, 2018, *online*)

Diante disso, entende-se que um dos objetivos da criação da LGPD, se deu principalmente para retirar a sensação de “terra sem lei” que o ambiente tecnológico trazia, pelo fato de não haver uma legislação específica para tratar sobre o tema, a lei inclusive teve embasamento no artigo 5º, XII da constituição federal:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Assim sendo, é importante esclarecer que a internet apresenta a aplicação de seus princípios da razoabilidade e proporcionalidade, todo baseado na constituição federal em seu artigo 5º, surgindo exclusivamente da necessidade de proteção aos dados pessoais, indevidamente usados por terceiros.

No entendimento de Jose Afonso da Silva (2000, p. 247):

A liberdade de comunicação consiste num conjunto de direitos, formas, processos e veículos, que possibilitam a coordenação desembaraçada da criação, expressão e difusão do pensamento e da informação. É o que se extrai dos incisos IV, V, IX, XII, e XIV do art. 5º combinados com os artigos. 220 a 224 da Constituição. Compreende ela as forma de criação, expressão e manifestação do pensamento e de informação, e a organização dos meios de comunicação, está sujeita a regime jurídico especial.

Diante desse pensamento, é possível concluir que a liberdade de expressão encontra também em outros direitos, como o simples fato do direito de se informar e ser informado, direito a resposta, liberdade em expressar opiniões, sejam ela políticas ou religiosas.

Assim os direitos fundamentais, nesse caso, como princípios, podem ser entendidos como valores morais compartilhados por uma comunidade em dado momento e lugar, que migram do plano ético para o jurídico quando se materializam em princípios abrangidos pela Constituição. (BARROSO, 2008, p. 352)

Notado em seu caráter princípio lógico, os direitos fundamentais, entre os quais o direito de liberdade de expressão, está inserido em um sistema normativo complexo, formado de regras e princípios, no qual a interpretação sistemática é essencial para a compreensão da amplitude de uma garantia. Conclui-se que, a proteção a nossos direitos é inquestionável.

CAPÍTULO 2 - A LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

Esse capítulo procura demonstrar de forma clara e objetiva o tratamento que a Lei Geral de Proteção de Dados vem atribuindo aos 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.

2.1 Objetivos da Lei Geral de Proteção de Dados

Conforme conceitua Rafael Fernandez em sua obra “Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais”, a LGPD é uma Lei que:

Dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade natural, inclusive por meio digital.

Conforme o art. 5º da LGPD, dado pessoal é toda informação relacionada a pessoa natural identificada ou identificável, e toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos do artigo 17º da LGPD (BRASIL, 2019, *online*), o titular dos dados pessoais tem direitos, que podem ser exercidos mediante requerimento expresso ao Ministério da Defesa.

Os direitos do titular são a confirmação da existência de tratamento, acesso aos dados, correção de dados incompletos, inexatos ou desatualizados,

eliminação dos dados pessoais, entre outros. Uma boa estratégia de adaptação, ajustada às necessidades do cliente com impacto mínimo no dia-a-dia da empresa pode trazer excelentes resultados.

Um dos segredos de uma boa implementação é focar não apenas no cumprimento da norma, mas, sobretudo na adequabilidade da cultura organizacional e dos processos e procedimentos da empresa pois ao colocar a privacidade de seus clientes como algo intrínseco aos seus fluxos e processos, além de adequar a empresa às regulamentações, a empresa também terá todo o seu processo produtivo e fluxo mapeado, podendo agregar um modelo de gestão estratégica dos principais indicadores da empresa e gestão de dados.

No geral, as leis de proteção de dados pessoais possuem como características em comum a liberdade e a transparência, tendo mais enfoque nessa segunda premissa. A primeira lei mundial de proteção de dados pessoais foi criada em 1970 na Alemanha, “dados pessoais constituem uma projeção da personalidade do indivíduo e que, portanto, merece uma tutela forte” (SCHERTEL, 2011, p.8). Notou-se então a necessidade de uma maior proteção dos dados pessoais, visto que eles constituem uma projeção da personalidade do indivíduo e que, portanto, merecem de forma rígida uma proteção por parte do Estado jurisdicional.

2.2 Regulamento Geral de Proteção de Dados - GDPR e a LGPD

O *General Data Protection Regulation* ou Regulamento Geral de Proteção de Dados, conhecido como GDPR, enfatizou a inspiração da LGPD. Seu objetivo é garantir maior controle sobre a coleta e tratamento dos dados pessoais dos usuários, estabelecendo políticas que devem ser seguidas e impor sanções a quem não as plantar em prática, conforme claramente previsto em lei, outro ponto importante a ser mencionado é sobre a aplicabilidade da regra.

A LGPD visa proteger os cidadãos brasileiros, enquanto o GDPR é para os cidadãos dos países da associação Europeia. A unificação de um regulamento geral, que conta com 28 estados-membros participantes e que estão vinculados na mesma ordem, torna a aplicação no continente europeu mais eficiente, uniformizando os procedimentos e diretrizes que todos os membros devem seguir.

No entanto, embora haja uma base sólida, para o GDPR ser usado como padrão para fazer cumprir as leis de proteção de dados, em muitos casos é essencial usar análises comparativas, dependendo do tipo de negócio que uma empresa está executando, ou seja, comparações entre as leis relativas aos dados de um determinado titular de direitos, averiguarem quais regras podem ser aplicadas em uma determinada situação, Patrícia Peck Pinheiro citou em um de seus livros que:

[...] uma instituição brasileira que capture dados no Brasil, em território nacional, mas que tenha um aplicativo que permita que o cliente seja de qualquer cidadania, nacionalidade, residência, e, portanto, o usuário do serviço, titular dos dados, pode ser um europeu, que mantém sua vida em um país da União Europeia, mas está temporariamente a trabalho no Brasil, utiliza cartão de crédito internacional, acaba por atrair, em termos de aplicação de leis e jurisdição para a sua operação, tanto a regulamentação nacional (LGPD) como também a regulamentação Europeia (GDPR). Se essa instituição brasileira utilizar recursos na nuvem e fizer a guarda internacional dos dados pessoais em outro país, poderá atrair ainda outras regulamentações. (PINHEIRO, 2018, p. 30 - 31).

Em conclusão, a LGPD visa proteger os cidadãos brasileiros e o GDPR os cidadãos dos países da Associação Europeia. No entanto, por estarem relacionados, dois ou mais planos podem ser usados em alguns casos. Quando se trata de dados pessoais, o GDPR será mais rigoroso em termos de conformidade política de proteção de dados, e segurança da informação e regulamentos sobre este assunto. Com relação à LGPD, atualmente não há previsão explícita na lei, podendo ser regulamentada posteriormente.

Com relação aos dados de crianças e adolescentes, em nossa lei geral de proteção de dados, os menores de 18 anos precisam do consentimento de, pelo menos, um de seus pais ou responsáveis, para autorizar a coleta e o processamento dessas informações. De acordo com os regulamentos europeus, menores de 16 anos ou mais podem dar seu próprio consentimento. Em relação às responsabilidades e penalidades das auditorias, a LGPD destaca que as auditorias são realizadas pela ANPD. (Agência Nacional de Proteção de Dados)

No entanto, sanções administrativas e multas podem ser delegadas a outros órgãos, como o MPF – Ministério Público Federal. O GDPR tem um órgão

central, chamado *European Data Protection Board*, e é responsável por monitorar e aplicar penalidades e multas. Relativamente ao tratamento de dados sensíveis, o GPDR proíbe-o expressamente, com duas exceções, nomeadamente: dados sensíveis tornados públicos pelo interessado; dados relativos a membros atuais ou antigos de instituições, associações ou organizações sem fins lucrativos, tratados para fins legítimos e com as devidas medidas de segurança.

Há uma disposição na LGPD sobre processamento de dados que é considerado sensível. Quando se trata de notificações de violação de dados, como no caso de vazamento de informações sobre pessoas físicas na LGPD, não há um prazo claro para notificar as autoridades supervisoras competente. As regras só devem ser aplicadas dentro de um prazo razoável e são altamente subjetivas. De acordo com os regulamentos europeus, os incidentes devem ser informados às autoridades competentes no prazo de 72 horas. (BRASIL, 2019, *online*)

Apesar das diferenças entre LGPD e GPDR, há muitas semelhanças entre elas e, conforme discutido acima, esta última serve de base para a formação da primeira. Vale destacar também que, como lei, a LGPD continha dispositivos mais abertos e subjetivos, o GPDR, por outro lado, é um regulamento, suas disposições são mais objetivas e diretas, com regras bem definidas para as diferentes situações que possam emergir.

Em face do exposto, pode-se resumir esse estudo com as seguintes palavras; enquanto a LGPD exige registro de tratamento dos dados pessoais. A GDPR exige o registro de tratamento de dados pessoal e específico as informações sujeitas à manutenção de registros.

2.3 Dos direitos do titular

O dado pessoal é ativo importante para a atividade empresarial, social e pessoal, bem como para a concretização de políticas públicas e desenvolvimento econômico global, sendo que a LGPD conceitua dado pessoal como informação relacionada à pessoa natural identificada ou identificável, consoante o Artigo 5º, Inciso I. (BRASIL, 2019, *online*)

Então, ao menos, pode-se dizer que se trata de informação que, isolada ou associada, seja capaz de permitir a identificação de uma pessoa natural. Logo, nome, prenome, estado civil, número do Cadastro da Pessoa Física, número da cédula de identidade, estado civil, profissão, informações relativas à origem social ou étnica, à saúde, às convicções políticas ou religiosas, são alguns exemplos de dados pessoais, o que permite distinguir de dados gerais que não possuem vínculo objetivo com a pessoa. (DONEDA, 2006, p. 157)

Fica evidente, portanto, que a LGPD visa proteger transgressões das características ou do conjunto de atributos que formam a projeção da pessoa. (BITTAR, 2015, *online*)

A lei dá ao titular, o direito à confirmação da existência do tratamento de seus dados pessoais por parte do controlador, ou seja, a empresa que os trata. Este é um direito derivado dos princípios de transparência e garante aos titulares a ciência do tratamento, como ele é ou será feito.

Dados pessoais são quaisquer informações que possam identificar direta ou indiretamente uma pessoa. Esses dados incluem nome, RG, CPF, data de nascimento, endereço, telefone, comportamento de consumo, histórico de pagamentos, entre outros. Também existem os dados pessoais sensíveis que podem levar a qualquer tipo de discriminação contra o titular dos dados tais como a ascendência étnica ou racial, opinião política, religião e dados relativos à saúde ou vida sexual.

Com a publicação da lei Geral de Proteção de Dados (LGPD), o titular dos dados passou a receber diversos direitos em relação aos seus dados pessoais. É importante garantir o cumprimento das solicitações dos titulares de dados para evitar violações de dados que podem levar a multas e penalidades, é importante observar que enquanto os proprietários são protegidos por seus direitos, as empresas são protegidas por lei para fins específicos.

Conforme art. 17 da Lei Geral de Proteção de Dados: “toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os

direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta lei.” (BRASIL, 2019, *online*)

Outra previsão da lei que expressa o consentimento de tratamento de dados é no caso de interesse legítimo. Nesse ponto, Sergio Pohlmann, na sua obra “LGPD Ninja”, destaca que:

Entendamos interesse legítimo como algo que é importante para alguém, tendo como base uma justificativa amparada pelo bom senso. Para que o interesse legítimo possa ser aceito como um caso de tratamento de dados válidos, o mesmo deve cumprir com os três pilares a seguir: 1. O legítimo interesse não poderá ser exercido no caso de prevalecerem direitos e liberdades fundamentais do titular, que exijam a proteção de seus dados. 2. As finalidades devem ser legítimas. 3. O caso deve estar baseado em situações concretas (POHLMANN, 2019, p. 84 - 85).

Outro ponto que está expressamente previsto nos casos de autorização é o tratamento dos dados pessoais na proteção do crédito. Como por exemplo, as contidas no Serasa ou Cadastro Positivo, podem ser consultados por outras empresas, já para profissionais em privacidade e proteção de dados:

É garantido ao usuário informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial, artigo 6º da LGPD. (BRASIL, 2019, *online*).

2.4 Dos agentes de tratamento de dados pessoais

A Lei Geral de Proteção de Dados, destinada a regular o tratamento de dados pessoais, veio para adequar-se à nova realidade imposta pela economia digital, fato este que torna imprescindível o seu conhecimento, uma vez que a grande maioria dos profissionais autônomos e empresas trabalham com dados pessoais.

De acordo com a LGPD, os agentes de tratamento de dados pessoais são o operador e o controlador, os quais são assim definidos pela legislação:

Art. 5º VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem às decisões referentes ao tratamento de dados pessoais. (BRASIL, 2019, *online*)

Art. 5º VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. (BRASIL, 2019, *online*)

Assim, podemos ver que o controlador de dados é quem toma as decisões sobre o tratamento de dados, enquanto o operador é responsável por obedecer às formações do controlador de dados.

Para uma relação jurídica segura para ambas as partes, é imprescindível a celebração de um contrato entre o operador e o controlador de uma determinada base de dados. Isso significa que para cada processo de processamento de dados pessoais, deve ser especificado quem é o responsável e quem é o operador. Isso se deve ao fato de uma empresa poder atuar como controlador em um processamento de dados pessoais e operador em outro processamento, ou seja, em um banco de dados diferente. (MUNIZ, 2021, *online*)

Além disso, o contrato entre o operador e o controlador de dados também deve conter a obrigação de o operador notificar imediatamente o controlador de dados em caso de incidente de dados pessoais, para que o controlador de dados se comunica com a Autoridade Norueguesa de Proteção de Dados e os titulares de dados, se necessário.

Se o controlador não seguir as formações dadas pelo controlador ao iniciar uma decisão sobre o tratamento de dados pessoais Ele ficará responsável por todas as tarefas relacionadas ao projeto de lei.

Com relação ao controlador de dados, Rony Vainzof (BLUM, 2019, p. 106) esclarece que o “conceito de controlador inclui absolutamente todas as decisões sobre atividades que refletem o ciclo de vida dos dados pessoais”. Do projeto à coleta ou aceitação, todas as formas de processamento até o descarte.

Ademais, segundo o referido autor (APUD BLUM, 2019, p. 106).

[...] para o titular e para a ANPD não pode haver dúvidas. Assim, o responsável pelo tratamento deve identificar-se com as informações de contacto do titular dos dados de forma simples, clara, adequada e claramente demonstrada. Além de fornecer informações sobre o processamento de dados, como a finalidade específica do

processamento, formato e tempo; e informações sobre o compartilhamento de informações e sua finalidade.

Perante isto, fica evidente a importância da definição contratual de responsável pelo tratamento e operador, uma vez que aquele tem maiores deveres e responsabilidades na realização do tratamento de dados pessoais.

Trata-se de duas entidades, as quais participam do processo, são eles os agentes de tratamento de dados. Eles têm diferentes responsabilidades de tratar os dados pessoais dos usuários.

Dessa maneira, ambas as entidades têm um papel importante no procedimento, mas também existe um terceiro que não é chamado de “agente de tratamento”, mas que também garante todo o auxílio necessário para que uma comunicação exista entre o processo.

Os processadores de dados pessoais têm suas funções mencionadas na LGPD – Lei Geral de Proteção de Dados, que os caracteriza em duas classes distintas: “Responsável” e “Manipulador”. Mas quem são os agentes de tratamento de dados pessoais? De acordo com a lei Geral de Proteção de Dados, o controlador de dados é a pessoa que exerce controle geral sobre:

I – As finalidades para as quais os dados receberão tratamento e. (BRASIL, 2019, *online*)

II – As maneiras pelas quais os dados pessoais são e serão tratados, seja por si só, em conjunto ou em comum com outros agentes de tratamento de dados pessoais. (BRASIL, 2019, *online*)

Dessa forma, cabe ao controlador decidir os motivos pelo tratamento e como serão as ações tomadas para este fim. Ele é o agente responsável por todo o ciclo de vida das informações sob seu tratamento, desde a coleta até a exclusão efetiva dos dados.

A LGPD deixa claro que o controlador é o principal tomador de decisões e tem o maior poder de controle sobre as finalidades ações, processos e procedimentos aplicados para o tratamento de dados pessoais. O controlador

também é responsável pelos dados processados sob sua supervisão e por eventuais violações da LGPD durante esse processo. (*COMMAND*, 2021, *online*)

Com o objetivo de elucidar e regular questões semelhantes às anteriores, a garantia Nacional de Proteção de Dados Pessoais editou em maio de 2021 o “Guia para determinar os responsáveis pela gestão de dados pessoais”. Eles enfatizam que os processadores devem ser definidos com base em sua natureza institucional.

Pessoas sob seu comando, como funcionários, funcionários do governo ou equipes corporativas não é considerado controlador (de forma independente ou conjunta) ou operador, pois essas pessoas atuam sob o comando do agente terapêutico.

Desta forma, uma pessoa singular pode ser considerada responsável pelo tratamento de dados pessoais, mas apenas quando agir de acordo com os seus próprios interesses institucionais e de acordo com as suas decisões sobre a finalidade e a forma do tratamento. Você também pode ser considerado um controlador de dados pessoais se for uma pessoa física ou jurídica diferente do controlador e não for uma subordinada ou membro do controlador.

É claro que o processador deve estabelecer suas políticas, regras e procedimentos internos em relação à proteção de dados pessoais e definir programas de conscientização sobre proteção de dados dentro de seu programa de gerenciamento, não funcionários, funcionários e agentes considerados processadores, mas para cuja conformidade são responsáveis pelas regras estabelecidas por seus empregadores.

Além de ser uma figura central na proteção dos direitos dos titulares de dados pessoais, os agentes devem cumprir a lei para garantir que as ações de tratamento realizadas por outros agentes cumpram o estabelecido por lei. A LGPD também estipula que o controlador de dados é responsável por elaborar relatórios de impacto na proteção de dados pessoais e nomear um controlador de dados que atue como uma ponte de comunicação entre o controlador de dados e a autoridade nacional e entre o controlador de dados e o controlador de dados. Os proprietários do assunto do processamento de dados pessoais.

CAPÍTULO III - A ILUSÃO DE PROTEÇÃO DE DADOS NA INTERNET

Nesse capítulo, será apresentado o atual cenário da proteção de dados na internet, embora esse tipo de ataque seja silencioso, o ambiente está comprometido e infectado, e naturalmente, os processos de proteção de segurança da informação falham. Muitas empresas passam meses com ambiente infectado sem detectar. Esse silêncio tem feito com que muitas empresas sintam que estão bem protegidas, gerando um falso sentimento de segurança.

3.1 Análise de casos concretos

Com o avanço repentino da internet em decorrência ao covid-19, onde tudo se modernizou, e nossos registros físicos migraram todos para o virtual, não se podia esperar que tudo fosse perfeito. Da mesma forma que existiu rapidez, inovação, sofisticação, houve falhas, vazamentos de informações importantes que feriram todo o funcionamento administrativo.

É relevante ressaltar alguns casos, para que seja feita uma análise concreta da situação.

A fonte do vazamento supostamente foi uma falha de segurança na API – *Application Programming* do LinkedIn, que é uma Interface de Programação de Aplicação rotineiramente usada, por exemplo, para transferir dados entre diferentes sistemas, aplicações ou web sites. (MAGANHATI, 2021, *online*)

A fonte do vazamento supostamente foi uma falha de segurança na API – *Application Programming* do LinkedIn, que é uma Interface de Programação de Aplicação rotineiramente usada, por exemplo, para transferir dados entre diferentes sistemas, aplicações ou websites. (MAGANHATI, 2021, *online*)

Entretanto, em uma declaração oficial sobre o caso, o LinkedIn afirma que nem todos os dados poderiam ter sido obtidos através da API, e que o mais provável é que as informações tenham sido coletadas através de outras fontes como, por exemplo, por meio de técnicas de “Raspagem de Dados”, ou *Scraping*, que é uma forma sistematizada de se agrupar informações publicamente disponíveis, o que pode ser feito no próprio LinkedIn ou em outras redes sociais e serviços similares. (DODT, 2021, *online*)

O conjunto de dados que estava à venda na *darknet* inclui uma série de informações que cibercriminosos e outros golpistas adorariam obter, essas informações poderiam facilitar tentativas de roubo de identidade, e todo tipo de ataque baseado em engenharia social. Basicamente esse conjunto de dados “vazados” formam um perfil básico de uma vítima e isso efetivamente facilita a execução de diversos ciberataques. (DODT, 2021, *online*)

Outro caso bastante atual, que inclusive é sucesso no Brasil, foi o caso do Banco Central, que sofreu a invasão de seus dados, o BC informou, que aproximadamente 137,3 mil chaves Pix de clientes da Abastece Aí, tiveram dados vazados. Essa é a quarta vez que acontece o mesmo problema desde o lançamento do sistema de pagamentos instantâneos, ou seja, o famoso Pix. (JOVEM PAN, 2020, *online*).

Os dados expostos foram: nome do usuário, Cadastro de Pessoas Físicas (CPF), instituição de relacionamento, agência, número e tipo da conta, data de criação da chave Pix. Com isso, dados protegidos pelo sigilo bancário, como saldos, senhas e extratos, felizmente, não foram expostos.

E esse não foi o único desafio enfrentado pela autoridade monetária para consolidar o Pix, que também virou isca para diversos golpes. A coisa ficou tão feia que alguns parlamentares tentaram propor projetos de lei para barrar o Pix até que

mecanismos de segurança fossem implementados pelo BC. (MARQUES, 2021, *online*)

O Superior Tribunal de Justiça também foi vítima de ataque no ano de 2020, calcula-se que 255 mil processos que tramitaram na corte ficaram expostos ao ataque, não há informações se o cibe criminoso conseguiu fazer cópia de todo esse volume, mas essa é uma possibilidade que preocupa a Corte. Além disso, há um “risco elevado” de o hacker ter conseguido fazer o download de documentos com informações dos servidores do tribunal. (ADVISOR, 2020, *online*)

A falha de segurança é um dos incidentes mais graves envolvendo o setor público no Brasil. (AFFONSO, 2020, *online*)

Ao que tudo indica a invasão aos sistemas do STJ usou o *ransomware*, um programa malicioso que seqüestra dados e exige resgate para devolvê-los. A ação é uma velha conhecida dos especialistas em cibe segurança. O vírus da vez pode ter sido o *RansomExx* (também conhecido como sequestro digital), que já atacou governos e empresas de outros países também. (SOUZA, 2020, *online*)

Esse ataque revela um grande temor da comunidade jurídica e confirma o que se sabe desde os tempos mais remotos da humanidade: a necessidade de confiança e de segurança jurídica. Desde as fontes escritas mais antigas que conhecemos, provenientes da Mesopotâmia, a confiança na autoridade que aplicaria as regras regentes da sociedade, ou seja, o direito, é fundamental para o funcionamento dessa comunidade. A estrutura das legislações de escrita cuneiforme, por exemplo, o famoso Código de *Hammurabi*, revela a presença de três partes distintas: um prólogo, o texto normativo e o epílogo. Assim, o prólogo tinha a função de legitimar a autoridade real, enaltecendo as características do soberano e revelando que ele tinha sido escolhido pelos deuses para governar sobre os povos, criando as normas a serem seguidas por todos.

O texto normativo trazia as regras a serem aplicadas, com o mais variado conteúdo, típico para a sociedade da época. Por fim, o epílogo trazia maldições e consequências nefastas, estabelecidas pelo soberano, para aqueles que não cumprissem suas normas. (HIRATA; GODOY, 2020, *online*)

3.2 Análise de decisões judiciais sobre a proteção de dados no Brasil

A entrada em vigor da Lei Geral de Proteção de Dados em 2020, foi uma surpresa para os operadores do direito, diante desse cenário inovador, existiu a necessidade de decisões judiciais com base na LGPD.

Como apresentado, a necessidade de uma lei específica sobre a proteção de dados pessoais decorre da forma como está sustentado o modelo atual de negócios. (PECK, 2021, pag. 39)

A proposta da Lei é alterar profundamente como o tratamento de dados pessoais é entendido em nosso país. Por mais exemplificada que a lei se apresente, cerca de 85%, não estão preparadas para sua aplicação, diante disso, o número de conflitos judiciais tende a aumentar. (CLOUD, 2020, *online*)

Algumas decisões tiveram um marco importante para desmascarar a falsa ilusão de proteção de dados, a qual se submete.

No Tribunal de Justiça de São Paulo, foi a primeira condenação a ter conhecimento no país com a aplicação direta da Lei Geral de Proteção de Dados. O juízo da cidade condenou uma construtora por ter feito uso indevido dos dados pessoais de seus clientes. (CLOUD, 2020, *online*)

A construtora teria compartilhado dados do autor á empresas estranhas ao contrato, sem o consentimento do titular dos dados pessoais. O autor havia comprado um imóvel, por meio de contrato firmado com a ré, e em seguida diversas empresas ficaram, insistentemente, oferecendo serviços, citando a compra feita com a construtora. Assim, o autor requereu e conseguiu indenização por danos morais no valor de 10 mil, sendo a empresa condenada, por ter descumprido obrigação de não fazer.

A fundamentação do juízo se deu expressamente em dispositivos da LGPD.

Com efeito, os elementos de prova coligidos aos autos revelam a comercialização de dados pessoais de terceiros pelo réu, vale dizer,

informações relacionadas com pessoa natural identificada ou identificável (artigo 5º, I, da Lei 13.709/2018).

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

- I – o modo pelo qual é realizado;
- II – o resultado e os riscos que razoavelmente dele se esperam;
- III – as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

11. Tal prática, portanto, está em patente confronto com o princípio constitucional da inviolabilidade do sigilo de dados, insculpido no artigo 5º, XII, da Constituição Federal e o fundamento do respeito à privacidade, previsto no artigo 2º, I, da Lei Geral de Proteção de Dados Pessoais, sem prejuízo de outros Diplomas Legais aplicáveis à espécie, a demonstrar a probabilidade do direito invocado. O perigo de dano, por sua vez, da persistente violação à privacidade dos titulares dos dados, a tornar impositiva a suspensão do comércio erigido pelo réu. (BRASIL, 2018, online)

Diante dessa decisão, percebemos a importância dos princípios da LGPD, uma vez que foi central nas primeiras decisões após a entrada em vigor da Lei.

Em Brasília, o Tribunal de Justiça decidiu sobre o caso de uma empresa *e-commerce*, que foi processada por uso indevido de dados pessoais. Na ação, o autor provou que o *e-commerce* atuou como intermediário de comercialização maciça de dados pessoais. (FERNANDES, 2021, *online*)

Conforme o caso, um vendedor que exercia suas atividades por meio do portal, ofertava cadastros e banco de dados em geral, tendo o réu como beneficiário dos pagamentos.

Na fundamentação do caso, o juiz teve sua decisão baseada, diretamente, na Lei Geral de Proteção de Dados.

Um dos direitos fundamentais do consumidor é de acesso à informação adequada acerca dos serviços que lhes são postos à disposição.

Especificamente sobre o assunto referente ao tratamento de dados, a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados LGPD) prescreve questões fundamentais da disciplina da proteção de dados, dentre outros, o respeito à privacidade, a autodeterminação informativa, a inviolabilidade da intimidade, da honra e da imagem, a

defesa do consumidor, os direitos humanos, o livre desenvolvimento da personalidade e a dignidade (art. 2º), (BRASIL, 2018, *online*).

Patente que os dados independentemente de sensíveis ou pessoais (art. 5º, I e II, LGPD) foram tratados em violação aos fundamentos de sua proteção (art. 2º, LGPD) e à finalidade específica, explícita e informada ao seu titular (art. 6º, I, LGPD), (BRASIL, 2018, *online*).

Assim, a decisão do magistrado, baseou-se especificamente nos princípios da LGPD, como o da privacidade, consentimento e a inviolabilidade do sigilo de dados, uma vez que as pessoas naturais eram identificáveis e o uso compartilhado de dados foi feito irregularmente.

Afinal, o juiz deferiu a tutela de urgência postulada na inicial, determinado ao réu, ou seja, a empresa *e-commerce*, que disponibiliza dados dos indivíduos, seja de forma gratuita ou onerosa, sob pena de multa de 2 mil reais a cada descumprimento. (TJFD, 2020, *online*)

Em 21 de setembro de 2020, o Ministério Público do Distrito Federal e Territórios (MPDFT) ingressaram com Ação Civil Pública contra um usuário que se utilizava de um site de *e-commerce*, operando no formato de marketplace, para comercializar dados pessoais. (MANZUETO, LEAL, 2020, *online*)

A primeira ação civil pública com aplicação da LGPD, ajuizada pelo MPDFT, foi em face de uma empresa de informática que comercializava informações pessoais como nomes, e-mails, contatos para SMS, bairro, O presidente da República, Jair Bolsonaro, sancionou a lei que tipifica o crime de perseguição, prática também conhecida como *stalking*, lei 14.132, de 2021. A norma altera o Código Penal (Decreto-Lei 3.914, de 1941) e prevê pena de reclusão de seis meses a dois anos e multa para esse tipo de conduta. O ato foi publicado no Diário Oficial da União de quinta-feira.

O crime de *stalking* é definido como perseguição reiterada, por qualquer meio, como a internet *cyberstalking*, que ameaça à integridade física e psicológica de alguém, interferindo na liberdade e na privacidade da vítima.

A nova lei é oriunda do PL 1.369/2019, de autoria da senadora Leila Barros (PSB-DF). A matéria foi aprovada em 9 de março como substitutivo da Câmara dos Deputados e teve relatoria do senador Rodrigo Cunha (PSDB-AL), é importante destacar que o avanço das tecnologias e o uso em massa das redes sociais trouxeram novas formas de crimes. Com a nova legislação poderemos agora mensurar com precisão os casos que existem no Brasil, e que os criminosos não fiquem impunes como estava ocorrendo. (SENADO NOTICIA, 2021, *online*)

No site, onde eram vendidas as informações, era possível encontrar pacotes de dados pessoais de acordo com as profissões exercidas pelos seus titulares.

Diante desse absurdo, houve grave violação à praticamente todos os princípios estabelecidos pela LGPD, como o direito à intimidade, à privacidade, à imagem, ao consentimento, entre outros. (BRASIL, 2018, *online*)

Mas, apesar dessas inúmeras violações, a ação foi extinta sem resolução de mérito, uma vez que a petição inicial foi considerada inepta por falta de interesse de agir. Toda a situação teve fundamento, pelo fato do juízo analisar que, a entrada em vigor da LGPD se deu no momento em que a empresa ré ficou fora do ar, assim, os responsáveis pelo site, alegaram estarem procurando adequar seus serviços às normas vigentes. (FACHINI, 2022, *online*)

Ao usuário em questão foi oferecida uma grande quantidade de informações pessoais, entre elas: nome e endereço do CPF. O MPDFT afirmou que houve um tratamento ilícito de dados pessoais que causou danos aos titulares dos dados e não apenas contra a LGPD – lei Geral de Proteção de Dados Pessoais.

A 17ª Vara Cível do Tribunal de Justiça do Distrito Federal e Território acolheram as pretensões do MPDFT. O usuário foi condenado a abster-se de fornecer dados pessoais, gratuitamente ou mediante pagamento, sob pena de coima de R\$ 5.000,00 por transação (TJDFT, 2020, *online*).

A decisão afirmou que privacidade e intimidade são direitos constitucionalmente amparados, lembrando que o STF reconheceu o direito

fundamental à privacidade em 2020 antes da implementação da LGPD. Também foi usado como uma discussão de decisões que exigem consentimento específico de cada proprietário para compartilhar seus respectivos dados.

O principal ponto de atenção nessa sentença foi à aplicação retroativa da LGPD, uma vez que os fatos ocorrer antes da entrada em vigor da lei – que só entrou em vigor em 18 de setembro de 2020. Às controvérsias entre operadores do direito, mas a própria LGPD prevê que ela pode produzir efeitos por situações ocorridas antes de sua vigência, com base em seu art. 63:

Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados. (BRASIL, 2018, *online*)

Importante ressaltar, contudo, que o art. 63 trata de disposições transitórias da LGPD e que compete à ANPD (Autoridade Nacional de Proteção de Dados) regulamentar, o que ainda não foi feito. Além disso, a sentença ainda é passível de recurso pelo usuário réu. (LEAL, 2022, *online*)

Os dados biométricos são todos aqueles dados que permitem a identificação individual, única e exclusiva de um indivíduo. (BRASIL, 2028, *online*)

Houve também, a primeira ação em andamento sobre dados biométricos, que, de início, causou grandes dúvidas com a entrada em vigor da LGPD. É uma questão delicada, pois engloba dados sensíveis dos titulares, e está muito presente no nosso cotidiano. Um exemplo, é o desbloqueio do celular com reconhecimento facial ou digital nos bancos, usamos a biometria, entre outros casos.

Um caso que apelou para mais uma decisão do tribunal, foi o uso da biometria, é fato que a biometria faz parte do nosso cotidiano e, por isso, já está em andamento uma das primeiras ações sobre a matéria, questionando o uso desse tipo de dado conforme a LGPD. (CLOUD, 2020, *online*)

O caso ocorrido em relação ao tema teve início com um estudante beneficiário de bilhete eletrônico para uso em transportes públicos, na cidade de

Recife, onde questionou a forma de política a proteção de dados utilizada pela empresa.

O cadastro biométrico é imposto pela empresa sem esclarecimento da política de proteção de dados feita pela pessoa jurídica em questão.

Nesse sentido, o autor alega que houve violação do art. 1 da LGPD, entre outros dispositivos, uma vez que teria ocorrido violação da privacidade.

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. (BRASIL, 2018, online)

Diante do apresentado, conclui-se que nos últimos anos, o Brasil teve um avanço gradativo em direção aos direitos digitais por meio da Constituição Federal, da Codificação de Defesa do comprador, Codificação Civil, Lei de Acesso à informação e da Lei do registro Vantajoso e dos direitos Civis da internet. No entanto, com a lei geral de 14 de agosto de 2018 sobre proteção de dados pessoais – LGPD, no âmbito da lei 13.709/2018, o país atingiu seu objetivo de proteger os dados pessoais e aumentar a segurança jurídica sobre o assunto. (JUSTIÇA DO TRABALHO, 2022, *online*)

A LGPD exige o tratamento de dados pessoais, inclusive dispositivos digitais, por entidades públicas ou privadas, a fim de proteger os direitos fundamentais à liberdade e à privacidade bem como o livre desenvolvimento da personalidade da pessoa física. Assim, a importância desta norma reside na apresentação das regras que regem o tratamento de dados pessoais, que incluem: os princípios que regem a proteção de dados pessoais; bases legais que podem justificar o tratamento de dados; e o monitoramento e responsabilização dos envolvidos no processamento de dados pessoais. (MPF, 2022, *online*)

Para além de garantir o direito à proteção dos seus dados, de quem possui e trata e garante a sua utilização para os fins pretendidos; A LGPD também confere aos titulares de dados pessoais o direito de solicitar informações como

confirmação da existência de tratamento de seus dados pessoais, acesso aos dados correção de dados, eliminação de dados desnecessários e portabilidade de dados pessoais para outro provedor de produtos e serviços.

Portanto, a instauração de uma cultura de privacidade e proteção de dados, é a principal ambição da LGPD. O trabalho se inicia com a Lei, entretanto o Brasil ainda percorrerá um caminho que se renovará a cada trecho, conforme as evoluções das tecnologias e os enfrentamentos de novos ataques cibernéticos que se reinventam constantemente.

CONCLUSÃO

Diante do apresentado, pode-se concluir que o Direito Digital é um ramo muito complexo do Direito, da mesma forma a lei geral de proteção de dados, que assegura parâmetros de proteção na internet, e por se tratar de assuntos que estão presentes em nossa vida, é indispensável a necessidade de entender seu papel e a transformação que vem causando no mundo digital que impacta diretamente na sociedade humana.

A internet invadiu nossas vidas e veio para ficar, conseqüentemente, a intimidade e privacidade foram expostas, mesmo de maneira inconsciente. Assim, a análise de casos concretos de invasão que forçaram a criação de leis, com o fim de evitar a propagação desses crimes, assim, é possível observar que mesmo diante de uma legislação sigilosa, ainda estamos expostos a diversos ataques ao qual necessitamos aprender a nos proteger.

Assim, temos a consciência da existência de leis que visam nossa proteção, porém, diante de um falso sentimento de proteção, devido aos ataques sem fim, o próprio poder judiciário enxergou a necessidade de decisões rígidas a fim de estabelecer um basta a invasões de privacidade.

Consumamos assim, que a necessidade de expandir o entendimento para se proteger é imprescindível, pois não basta por si só a legislação tomar conta de tudo, e sim, a necessidade de atualização pessoal diante de um mundo digitalizado, que toma conta de todos seus registros pessoais, desta forma, trabalharia uma forma com o fim de evitar esses ataques indesejado

REFERÊNCIAS BIBLIOGRÁFICAS

ACCENTURE, Tenbu, **Quais os Direitos dos Titulares de Dados Pessoas na LGPD**. Disponível em: <<https://www.tenbu.com.br/quais-os-direitos-dos-titulares-de-dados-pessoais-na-lgpd-2/>>. Acesso em: 30 de agosto de 2022.

ALVES, Marcelo de Camilo Tavares. **Direito Digital**. Disponível em: <https://monografias.brasilecola.uol.com.br/direito/direito-digital-direito-privacidade-vedacao-ao-anonimato-na-era-digital>. Acesso em: 29 de julho de 2022.

ANDRADE, Walmar. **Direito Digital – Guia básico: conceito, princípios, características, fontes e áreas de atuação**. Disponível em: <<https://walmarandrade.com.br/direito-digital/>>. Acesso em: 01 de setembro de 2022.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8.ed., rev. aum. e mod. por Eduardo C. B. Bittar. São Paulo: Saraiva, 2015.

BRAGA, Carine, **Direito dos Titulares**. Disponível em: <<https://pt.scribd.com/presentation/542464501/UFF-Direito-Dos-Titulares>>. Acesso em 01 de setembro de 2022.

BRASIL, planalto, **Lei Geral de Proteção de Dados**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709/>. Acesso em 20 de outubro de 2022.

BRASIL, **Constituição da República Federativa do Brasil**. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm.> Acesso em: 15 de agosto de 2022.

BRASIL, **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 29 agosto de 2022.

CARVALHO, Stefani. **Acordo com a Lei Geral de Proteção de Dados**. Disponível em: <<https://stefanidecarvalho.jusbrasil.com.br/>>. Acesso em: 04 de setembro de 2022.

DODT, Cláudio. **O que o caso o LinkedIn nos ensina sobre segurança de dados**. Disponível em: <<https://exame.com/bússola/o-que-o-caso-do-linkedin-nos-ensina-sobre-seguranca-de-dados/>>. Acesso em 20 de outubro de 2022.

ESCRITÓRIO, Projuris. **Direito Digital: o que é, importância e áreas de atuação.** Disponível em: <<https://www.projuris.com.br/blog/direito-digital/>>. Acesso em 22 de outubro de 2022.

FERNANDES, Rafael. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais**, São Paulo, pag. 17, 2020.

FREITAS, Alfredo. **LGPD: Lei Geral de Proteção de Dados do Brasil.** Disponível em: <<https://www.serpro.gov.br/lgpd/noticias/2019/elabora-politica-privacidade-aderente-lgpd-dados-pessoais>>. Acesso em: 09 de agosto de 2022.

GUGELMIN, Felipe, **Vazamento de Dados de Milhões de Perfis no LinkedIn.** Disponível em: <<https://br.financas.com/noticias/vazamento-teria-exposto-dados-pessoais/>> Acesso em 16 de outubro de 2022.

HIRATA E GODOY, Alessandra e Cristina, **39 dias após o ataque cibernético ao STJ: reflexões e desafios.** Disponível em: <<https://www.migalhas.com.br/coluna/migalhas-de-protacao-de-dados/337701/39-dias-apos-o-ataque-cibernetico-ao-stj--reflexoes-e-desafios/>>. Acesso em 18 de outubro de 2022.

LEAL, Rodrigo. **Primeira Ação Civil Pública com base na LGPD: Sentença com Aplicação Retroativa da Lei.** Disponível em: <<https://www.tauilchequer.com.br/pt/perspectives-judicial/>> Acesso em 10 de outubro de 2022.

MAGANHATI, ricardo, **Phishing no LinkedIn: um perigo da pandemia.** Disponível em: <<https://blog.axur.com/pt/phishing-no-linkedin-um-perigo-da-pandemia/>>. Acesso em 01 de outubro de 2022.

MARQUES, Ana, **Windows 11, dados vazados, problemas com Uber e mais: a tecnologia e 2021.** Disponível em: <<https://tecnoblog.net/especiais/windows-11-dados-vazados-problemas-com-uber-e-mais-a-tecnologia-em-2021/>>. Acesso em 20 de outubro de 2021.

MESQUITA, aline, **Agentes de Tratamento de Dados.** Disponível em: <<https://www.oitchau.com.br/blog/lei-de-protacao-de-dados-tudo-que-voce-precisa-saber/>>. Acesso em: 20 de agosto de 2022.

MINISTÉRIO PÚBLICO, Fundação Escola Superior. **Lei Carolina Dieckman: você sabe o que essa lei representa.** Disponível em: <<https://fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/>>. Acesso em 29 de outubro de 2022.

PAN, Jovem, **Dados de 137,3 mil chaves Pix são vazadas, diz Banco Central.** Disponível em: <<https://jovempan.com.br/noticias/economia/dados-de-1373-mil-chaves-pix-sao-vazados-diz-banco-central.html/>>. Acesso em 20 de outubro de 2022.

PINHEIRO, Patrícia Peck, **Proteção de Dados Pessoais**, Pag. 39. 3ª edição revisada, atualizada e ampliada, São Paulo: Saraiva, 2021.

PINHEIRO, Patrícia Peck. **Direito Digital**. 6ª edição revisada, atualizada e ampliada, São Paulo: Saraiva, 2016.

SOARES, Gabriella. **Nova lei já teve 584 decisões judiciais no Brasil**. Disponível em: <<https://www.poder360.com.br/justica/em-1-ano-de-lgpd-nova-lei-ja-teve-584-decisoes-judiciais-no-brasil/>> Acesso em 20 de outubro de 2022.

VAINZOF, Rony. Disposições preliminares. In: BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (Coord.). **LGPD – Lei Geral de Proteção de Dados Comentada**. São Paulo: Thomson Reuters Brasil, 2022.