

AS ORIGENS E ASPECTOS DA LEI GERAL DE PROTEÇÃO DE DADOS E A NECESSIDADE DE PROTEÇÃO DE INFORMAÇÕES PESSOAIS COMO MEIO DE DEFESA A DIREITOS FUNDAMENTAIS

HUGO LEONARDO GOMES DA SILVA¹
hldireito23@gmail.com

RESUMO: Este artigo buscará dispor sobre os regulamentos trazidos ao ordenamento brasileiro pela Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados. A referida Lei objetiva a proteção de direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade dos titulares de dados pessoais, enquanto busca regular as operações de tratamento de dados de forma a não bloquear o avanço da tecnologia da informação. O presente volume versará sobre os princípios, direitos e conceito que norteiam a LGPD, além de trazer informes sobre a natureza da responsabilidade civil, e alertas aos perigos que se originam a partir do uso irrestrito e irresponsável de dados. O presente trabalho de conclusão de curso foi realizado observando-se o critério hipotético-dedutivo, embasado em pesquisa bibliográfica e digital, em websites e vídeos, e busca demonstrar que este atual e fascinante assunto ainda não foi completamente esgotado fazendo assim com que a Lei 13.709/2018 possivelmente seja um dos primeiros passos em direção a normatização do ambiente digital.

PALAVRAS-CHAVE: Lei Geral de Proteção de Dados; LGPD; Direito a Privacidade; Direito Digital.

ABSTRACT: This article will seek to provide for the regulations brought to the Brazilian legal system by Law 13.709/2018, known as the General Data Protection Law. This Law aims to protect the fundamental rights of freedom, privacy and free development of the personality of the holders of personal data, while seeking to regulate data processing operations in order not to block the advancement of information technology. This volume will deal with the principles, rights and concept that guide the LGPD, in addition to bringing information about the nature of civil liability, and alerts to the dangers that originate from the unrestricted and irresponsible use of data. This course conclusion work was carried out observing the hypothetical-deductive criterion, based on bibliographical and digital research, on websites and videos, and seeks to demonstrate that this current and fascinating subject has not yet been completely exhausted, thus making the Law 13,709/2018 is possibly one of the first steps towards the standardization of the digital environment.

KEYWORDS: General Data Protection Law; LGPD; Right to Privacy; Digital Law.

INTRODUÇÃO

Nos atuais dias o termo "privacidade" vem sendo mais e mais discutido, principalmente no âmbito virtual, onde usuários alimentam suas redes sociais com massivas quantidades de informações que podem ser facilmente visibilizadas por milhares de pessoas ao redor do mundo em poucos instantes.

Ao mesmo tempo, sofreremos cotidianamente a intrusão de empresas que armazenam e coletam dados de nosso dia a dia, capitando nossos trajetos, observando nossas compras e monitorando nossas interações sociais com nossos pares. Esses gigantes compram e vendem grades quantidades de informações de populações inteiras, de forma que quando tomam posse de informações tão importantes nos preocupa pensar na influência que podem exercer.

¹Discente do Curso de Direito do Centro Universitário Estácio do Recife



Enquanto isso, ainda existe a possibilidade real de sermos vítimas de fraudes perpetradas por hackers que, por artifícios ilegais, obtenham o acesso a informações que podem trazer severas consequências as infelizes vítimas de suas práticas. Infelizmente, esse risco não encontra exclusividade apenas na virtualidade, o perigo de se ter os dados surrupiados e utilizados para fins fraudulentos colocam em risco a privacidade e a honra de quem pertencem tais informações até no plano analógico.

Todavia, através das premissas e proteções lançadas pela Lei Geral de Proteção de dados, vemos o esforço e preocupação do legislador em buscar dar a os dados pessoais, tanto no meio físico quanto no digital, uma maior seguridade, entendendo a desvantagem que a pessoa natural tem perante a empresas e outros agentes, buscando defender a privacidade e a personalidade.

A IMPORTÂNCIA DE LEIS QUE PROTEGEM DADOS

A preocupação em regulamentar aspectos de nossas vidas como pessoas é largamente discutida em todo tempo durante a história da humanidade, e na atualidade, poucos assuntos vem demandando tanta discussão e reflexão quanto as implicações do novo panorama digital que tem tomado de assalto a atenção do mundo inteiro, tanto que não se faz mais um exagero traçar um paralelo entre o atual rompante tecnológico possibilitado pela implementação e disseminação da internet e o desenvolvimento de fatores cruciais para o desenvolvimento humano como foram outrora a origem da agricultura e da escrita.

É de comum acordo no meio acadêmico que até então não podemos vislumbrar onde essa odisséia digital nos levará como raça, mas, ao paço que as luzes grandiosas são projetadas, sombras igualmente grandiosas tem origem. Os perigos é a vulnerabilidade do indivíduo frente a um mercado cada vez mais voraz, onde informações pessoais em volumes massivos valem não só grandes cifras, como podem permitir a deturpação da personalidade de indivíduos e até manipulação de populações inteiras, não fazem mais parte de distopias que buscam o entretenimento na ficção. O assunto se faz preocupante o suficiente para ter sido mencionado até mesmo pelo presidente da ONU (Organização das Nações Unidas) António Guterres que em seu discurso de abertura na assembleia geral ocorrida em 20 de setembro de 2022, apontou de forma pessimista vários problemas sérios que a humanidade enfrentará nos próximos anos, expondo a preocupação da organização quanto a temática de proteção de dados a vários chefes de estado.

Depreendemos desse discurso um tom nitidamente alarmante e urgente, observamos que tais preocupações estão listadas no mesmo bojo de alertas igualmente preocupantes como o aquecimento global, as mudanças climáticas e um possível desabastecimento mundial de alimentos, demonstrando que a proteção de dados é sim um ponto de crucial relevância internacional.

LEIS DE PROTEÇÃO DE DADOS INTERNACIONAIS

Em 25/05/2018, começa a ter validade na União Europeia a GDPR (*General Data Protection Regulation*), ela é considerada a lei mais completa em se tratando de proteção de dados pessoais, acabando servindo de base para outras legislações que surgiram ao redor do mundo nos últimos anos.

Para adequação a GDPR é necessário informar aos usuários que se esta coletando e processando seus dados, pedir consentimento antes de coletar qualquer dado, e em casos de



criança e adolescentes de até 16 anos, se faz necessário o consentimento fornecido pelo responsável legal, utilizar dados apenas para os propósitos que foram inicialmente comunicados e para os quais recebeu permissão, permitir que os usuário acessem seus dados além de terem possibilidade de corrigi-los e transferi-los, Fornecer um método de revogação de consentimento para os usuários, manter registros dos consentimentos fornecidos pelo usuários e excluir dados mediante requisição.

Em se tratando dos Estados Unidos, ainda não se percebe uma lei federal de privacidade de dados. Toda via, podemos ver algumas iniciativas a nível estadual em entes da federação americana onde já se adotam suas próprias leis regionais.

A lei de privacidade do consumidor da California é a mais completa atualmente dentro dos Estados Unidos, ela que estabeleceu um parâmetro para esse tipo de legislação no país.

Precisará se adaptar a CCPA (*California Consumers Protection*), o empreendimento que colete dados pessoais de habitantes do estado da California, ou se sua empresa controladora ou subsidiária possua o valor de receita bruta anual de U\$ 25.000,000,00 (Vinte e cinco milhões de dólares), obtenha dados pessoais de pelo menos 50.000 habitantes, domicílios ou equipamentos eletrônicos da Califórnia por ano, e ou, tenha 50% da sua renda bruta anual obtida a partir da venda de informações pessoais.

Para se adequar, precisará ter uma política de privacidade concordante com a CCPA, informar os usuários como acessar os dados que foram coletados, mediante requisição, informar para quem os dados foram vendidos, caso o faça, permitir que os usuários optem pela não venda de seus dados pessoais através de um botão ou link que diga claramente "não venda meus dados pessoais", excluir dados mediante requisição, pedir consentimento explícito antes da venda de dados infantis diretamente das crianças se elas tiverem entre 13 e 15 anos, e caso sejam mais jovens, de seus responsáveis legais, implementar um sistema de verificação de identidade para pessoas que solicitem a exclusão de seus dados e não discriminar pessoas que escolheram exercer seus direitos de privacidade ao utilizar seus serviços

Em outubro de 2019 o estado de Nevada adotou uma nova lei de diversidade de dados, em bora seja muito parecida com a CCPA ela traz algumas diferenças que a tornam menos abrangente que a lei californiana.

A lei de Nevada será aplicada caso, possua ou opere um site ou serviço online para fins comerciais, colete ou mantenha informações pessoais de habitantes de Nevada, e ou se envolva em atividades comerciais em Nevada, como vendas online, propagandas etc.

Em geral, há outros estados americanos que estão em processo de propostas e aprovações de projetos de leis para proteção de dados, mas a maioria dos deles, e o próprio governo federal, ainda não anunciaram a intenção de trabalharem melhor essa questão.

As legislações descritas acima são apenas uma pequena amostra, as leis de proteção de dados estão se proliferando no meio internacional, tendo o Brasil também sentido a necessidade de dispositivo que vise proteger informações pessoais.

LEI 13.709/2018 (LEI GERAL DE PROTEÇÃO DE DADOS)

Com o advento Marco Civil da Internet em 2014, foi lançada a primeira pedra que pavimentaria o caminho para a elaboração de uma legislação mais direcionada ao direito a intimidade, personalidade e a proteção de informações pessoais na internet.

Após isso, através de consultas públicas que viriam a ser as bases de diversos projetos de lei, com o escândalo da *Cambridge Analytica*, que gerou discussões acaloradas entre os mais diversos setores da sociedade e a entrada em vigor da GDPR na Europa, o terreno nacional se encontrava fértil para que, através dessas influências, a nossa versão de lei para proteção



de dados fosse desenvolvida.

A chamada Lei Geral De Proteção de Dado (LGPD), está em vigor desde 18 de setembro de 2020 e estabelece uma série de regras para empresas e organizações que atuam no Brasil, sendo largamente inspirada por sua antecessora europeia GDPR, se originou a partir da necessidade reconhecida pelo legislador em trazer ao país mais proteção aos cidadãos brasileiros que se tomam cada vez mais atuantes no ambiente digital e por conseguinte, mais vulneráveis.

A LGPD tem caráter extraterritorial, e se aplica a qualquer entidade pública ou privada que exerça processamento de dados pessoais e que tenham operações executadas dentro do Brasil, colete dados pessoais, ofereçam ou forneçam produtos e serviços no país ou mesmo se relacionem com indivíduos que estejam localizados em solo brasileiro.

ORIGENS DA LEI GERAL DE PROTEÇÃO DE DADOS

A Declaração Universal dos Direitos Humanos, proclamada pela Assembleia Geral das Nações Unidas em 10 de dezembro 1948, entre tantas diretrizes de valor inestimáveis para a construção do mundo contemporâneo, nos brinda com o estabelecimento do conceito de direito à privacidade em seu artigo 12, "Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques." (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948).

Tremenda influência de tal declaração internacional se faz clara e evidente ao analisarmos a carta magna nacional, onde ao decorrer de suas páginas se faz perceber inúmeras referências e inspirações que o constituinte obteve de tão alta diretriz humanística. Um desses acenos se encontra acostado ao inciso X do art. 5º da Constituição Federal de 1988⁵, onde se vê o desabrochar da semente plantada no artigo 12 da DUDH.

Uma vez inserida no ordenamento pátrio o conceito de Direito a personalidade encontrara tutela a nível infraconstitucional, mais especificamente no Código Civil em seus art. 11 a 21 atingindo no artigo 12⁸ do mesmo dispositivo legal a proteção que o titular de dados pessoais necessita para que possa demandar quanto perdas e danos sem que isso prejudique a aplicação de outras sanções legais.

Ainda no campo do Código Civil, se faz importante relatar o conteúdo compreendido no artigo 20, onde se estabelece a necessidade de autorização prévia para situações em que se utilizem dados pessoais.

Não obstante, observamos em outras legislações o interesse em também proteger a personalidade, como são os casos do artigo 31, §II, da Lei 12.527/2011 (Lei de Acesso à informação) e o artigo 7º, §VII e § IX da Lei 12.965/2014 (Marco Civil Da Internet), onde se estabelece, mais uma vez que apenas o consentimento do titular dos dados pessoais pode relativizar a inviolabilidade característica deste direito fundamental.

Mediante a gama de legislações anteriormente disposta, a LGPD buscou fundamentalmente a possibilidade de dar ao indivíduo a liberdade de construir para si a sua personalidade, buscando sempre respeitar as diretrizes instauradas ao ordenamento jurídico nacional, trazendo já em seus primeiros artigos esta preocupação. Ainda discorrendo sobre o esmero e prudência empenhadas em sua feitura, a LGPD também buscou em seu artigo 20, mecanismo que possibilita o direito de revisão das decisões automatizadas, visando proteger a personalidade.

Destinchado o percurso jurídico por onde caminhou a sociedade brasileira até que pudéssemos ter em mãos a lei 13.709, de 14 de agosto de 2018 (LGPD), necessário se faz



agora discorrer sobre os princípios que a norteiam.

PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS

São dez os princípios que a LGPD traz em seu bojo, em resumo, visitaremos cada um deles para melhor compreensão da legislação alvo deste artigo.

PRINCÍPIO DA FINALIDADE: Disposto claramente na lei 13.709, em seu artigo 6º, I objetiva exigir que a finalidade do tratamento de dados seja explícita, específica, legítima e acima de tudo informada ao titular dos dados, fazendo com que qualquer que seja o tratamento, quando incompatível com a finalidade informada ao tempo de sua colheita, tome o processo de tais informações práticas ilegal.

Por conta disto, não bastará ao controlador de dados apenas o consentimento do titular, mas sim, em respeito ao princípio da finalidade, informar sempre com maior clareza possível todas as atividades do procedimento de informações que irá realizar.

PRINCÍPIO DA ADEQUAÇÃO: Este princípio determina que o tratamento ao qual os dados serão submetidos sejam compatíveis com a finalidade apresentada pelo controlador ao tempo da colheita da concessão.

Em resumo, define que não é o bastante comunicar ao titular o propósito do tratamento, cabe também ao controlador dos dados o dever de garantir que os limites estipulados sejam devidamente cumpridos.

PRINCÍPIO DA NECESSIDADE: O Princípio da necessidade vem em auxílio ao princípio da finalidade, pois define que o tratamento de dados tenha um limite, limite este que deverá ser o mínimo necessário para que se tenham alcançado a finalidade desejada pelo controlador de dados.

Sendo assim, este princípio veda o tratamento de dados que possa avançar os limites do estritamente necessário, buscando impedir qualquer coleta desnecessária de dados que não tenham relações com a finalidade definida.

Essa trinca de princípios iniciais dita que o tratamento de dados deva ser pertinente, proporcional e não excessivo.

PRINCÍPIO DO LIVRE ACESSO: Vemos neste princípio a garantia disposta ao titular dos dados a consulta gratuita e facilitada a qualquer atividade que envolva o tratamento de seus dados, devendo tais consultas serem possíveis a qualquer momento, visto que estes dados deverão ser armazenados de maneira que possibilitem o exercício do direito ao acesso destas informações.

De forma bastante objetiva, o art. 9º da LGPD permite que o titular questione a qualquer tempo, a forma e a duração do tratamento de dados, a identificação e informações do controlador, a finalidade específica do tratamento, informações sobre o uso compartilhado pelo controlador, a responsabilidade dos agentes que realizarão o tratamento e os direitos que o titular possui.

PRINCÍPIO DA QUALIDADE DOS DADOS: Este importante princípio busca obrigar os agentes de tratamento a dispor garantias de que os dados manipulados por eles serão exatos, claros, relevantes e atualizados, observando sempre se estão em conformidade com os preceitos elencados nos princípios da finalidade, necessidade adequação. Inclusive, garantindo ao titular o direito a solicitação de revisões de decisões tomadas no processo de tratamento de dados pessoais que afetarem de alguma forma interesses próprios.

PRINCÍPIO DA TRANSPARÊNCIA: Como o próprio nome afirma, o objetivo do princípio



da transparência não é outro se não o de garantir ao titular dos dados, informações precisas e claras, bem como ter facilitado o seu acesso a formas de saber como estão sendo conduzidos os tratamentos.

Assim sendo, em resumo, este princípio objetiva dar ao titular acesso amplo, livre e sem restrições aos seus dados. Porém, cabe ressaltar que a própria lei limita tal princípio em casos que envolvam segredos industriais e comerciais que impeçam a divulgação se informações sobre formas de tratamento de dados.

PRINCÍPIO DA SEGURANÇA: De forma geral, este princípio objetiva garantir que seja empenhado na proteção dos dados pessoais possuídos pelos agentes de tratamento, todos os meios técnicos e administrativos mais eficazes e atuais disponíveis, visando evitar qualquer tipo de vazamento, acesso não autorizado, perda, alteração ou distribuição indevida destas informações.

Em resumo, o agente terá que dispor de todas as medidas, que lhe forem possíveis e razoáveis, ao seu alcance para assegurar a segurança dos dados com os quais lida.

PRINCÍPIO DA PREVENÇÃO: Visando evitar situações de risco, o princípio da prevenção objetiva, junto ao princípio da segurança, trazer aos processos de tratamento de dados mais segurança, pois demanda ao agente a obrigação de dispor de medidas preventivas contra qualquer tipo de dano aos dados.

A criação de cartilhas de boas práticas e o desenvolvimento de diretrizes de governança, onde podem ser estabelecidas normas de padrão técnico, segurança e obrigações específicas são recomendadas pela própria lei, pois tais iniciativas auxiliam e mitigam potenciais falhas.

PRINCÍPIO DA NÃO DISCRIMINAÇÃO: Tendo sua atenção voltada para impedir que o tratamento de dados possa ser usado com fins discriminatórios e atos abusivos ou ilícitos, através desse princípio, é garantido ao titular dos dados a possibilidade de conferir como suas informações estão sendo utilizadas.

Porém, como visto anteriormente, podendo esta consulta ser negada sob o pretexto de segredo industrial ou comercial, poderá ainda o titular dos dados acionar a Autoridade Nacional, que poderá mover auditoria buscando qualquer manifestação discriminatória ou ato ilegal relacionado aos dados referidos.

PRINCÍPIO DA RESPONSABILIZAÇÃO: Ao final, trata este princípio de imputar ao agente de tratamento de dados o dever de atestar que se encontra utilizando todas as medidas mais eficazes e pertinentes no esforço de cumprir as normas que visam a proteção de dados pessoais, sob a penalidade de ser responsabilizado individual ou solidariamente nas pessoas do controlador e ou operador no caso de se averiguar qualquer tipo de desrespeito a legislação. Isto posto, convém indicar que poderá ser imputado ao responsável pelo tratamento irregular de dados, penalidades que podem variar desde a mais branda, com uma advertência, até a severidade de multa que pode alcançar 2% do faturamento da empresa infratora, tendo este valor sido limitado a cifra de R\$ 50.000.000,00 (Cinquenta milhões de Reais).

APLICABILIDADE DA LEI 13.709/2018

A LGPD, expõe claramente, em seu art. 3º que poderá ser invocada independente do meio, ou seja, visando proteger o tratamento de dados tanto no meio "*offline*" quanto também no "*online*", o que a difere do seu antecessor, o Marco Civil da Internet, onde, o referido marco possui apenas abrangência em métodos online. Outrossim, não haverá de se falar em revogação tácita do Marco Civil da Internet, visto que tal legislação trata de temas diversos, não sendo especializada em proteção de dados.



A lei nos apresenta algumas hipóteses de aplicação, sendo a primeira delas quando o tratamento é realizado em território nacional, nesse caso, basta que ocorra o tratamento no Brasil, pouco importando o local onde se encontra a sede ou domicílio do agente de tratamento, ainda que no exterior. Ressalta-se que a LGPD também será válida para estrangeiros que tiverem seus dados processados no Brasil, mesmo que resida no exterior.

A próxima possibilidade é na hipótese de tratamento que objetive a oferta ou fornecimento de bens ou serviços, ou que o tratamento dos dados do titular que reside em território nacional, ou seja, o fato gerador nesse caso é a localização do fornecimento desses bens ou desses serviços ao titular. Sendo assim, é certo dizer que quando o tratamento de dado for realizado no Brasil, a LGPD será aplicada independentemente de o agente estar em território brasileiro ou em território estrangeiro.

Quanto a próxima possibilidade ocorre quando os dados pessoais objeto do tratamento tenha sido obtidos em território nacional, observado que no momento da obtenção o titular se encontrava no Brasil.

EXCEÇÕES DE INAPLICABILIDADE

A partir do disposto no item anterior, agora apresentaremos os casos em que não há a incidência da Lei, situações essas em que o agente de tratamento não será penalizado por tratamento de dados.

A primeira delas se refere a tratamento particular de dados com fins não econômicos, sendo a troca e o compartilhamento de informações de cunho comum e cotidiano, que não passa de armazenamento de registros corriqueiro como, e-mails ou contato telefônico de amigos e parentes, cartas, fotografias ou demais elementos que contenham dados de terceiros. Esses tipos de dados que são frutos da comum vivência não se enquadram na proteção concedida pela LGPD.

A segunda situação encontra amparo no direito que a Constituição garante quanto a liberdade de expressão, desde que a matéria jornalística em questão tenha por finalidade apenas levar informação através dos dados coletado, sendo essa inaplicabilidade descaracterizada quando juntamente com a intenção informativa se pretender o controlador obter qualquer vantagem econômica. Ou seja, nestes casos, só serão validos os meios de informação jornalísticos que não vinculem em seus conteúdos publicidades de serviços ou produtos relacionados ao dado coletado.

A diante, a terceira situação em que não se aplicara a LGPD se dá quando trata-se de uso de dados para fins exclusivamente artístico. Ancorado também na constituição, em seu art 5º IX. A Liberdade artística afasta a aplicação da lei de proteção de dados quanto ao de informações pessoais em obras literárias, músicas, filmes etc.

A quarta hipótese aborda o tratamento de dados para fins exclusivamente acadêmicos, onde o legislador conferiu ao agente da comunidade acadêmica que procure a utilização das informações pessoais pra compor estudo e análises praticamente "carta branca" deixando assim este seguimento fora do domínio da LGPD.

Quanto a quinta situação, sendo esta a mais sensível, se observa o tratamento de dados com fins exclusivos de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e representação de infratores penais, sendo todas estas finalidades de competência exclusiva do Poder Público. Portanto, quando o Poder Público necessitar de tratamento de qualquer dado pessoal envolvendo qualquer uma das finalidades descritas acima, não se poderá aplicar a LGPD, pois os tratamentos dos dados nessas situações só ocorrerão para a garantia de assuntos de seguridade para a coletividade



Terminando, a sexta forma onde não se prevê a incidência da Lei de proteção de dados, se refere simplesmente ao caso em que as informações pessoais sejam oriundas de país do exterior, que não tenha compartilhado estes dados como agentes de tratamento brasileiros e que possua legislação de proteção de dados compatível com a proteção concedida pela LGPD.

DEFINIÇÕES LEGAIS

As definições legais que aqui vamos dispor buscam ajudar no entendimento e aplicabilidade da Lei, trazendo seus conceitos para tomar mais lógico e intuitivo os termos presentes no estudo a LGPD, objetivando desta maneira a exclusão de dúvidas quanto este tema.

O art. 5º apresenta vários dos conceitos referidos ao longo deste artigo, assim sendo, discorreremos sobre alguns dos seus aspectos mais importantes a seguir:

DADOS PESSOAIS

O inciso 1 do art. 5º da LGPD nos traz o conceito de dado pessoal de forma sucinta e direta. Em análise a este caput podemos afirmar que dados pessoais são os dados que possuam informações que possam imediatamente identificar alguém, ou que a partir de análise de um conjunto delas se possa identificar um indivíduo. Dados como nome, endereço, conta bancária, números de CPF, RG, CNH entre outros, são consideradas como dados pessoais objetivos, pois possuem a capacidade de identificação imediata do titular.

Também observamos o conceito de dado pessoal ser delimitado no Decreto 8.771/2016, que altera o Marco Civil da Internet em seu art.14, inciso 1, tendo servido claramente de base para o caput definidor constante na LGPD, onde lemos:

DADOS PESSOAIS SENSÍVEIS

Os dados considerados sensíveis, resumidamente falando, são informações de cunho étnico, ideológico religioso, posicionamento político, orientação sexual, dados contendo informações médicas, genéticas, biométricas entre outros.

Percebamos que esses dados em específico são vinculados ao pensamento ou a condições fisiológicas de uma pessoa natural, e por esse motivo gozam de proteção especial por poder acarretar discriminação de algum tipo se por ventura sejam divulgados de maneira imprópria. Levando isso em conta, a LGPD apresenta uma forma mais rígida de tratamento a tais dados, visando evitar que a partir de vazamentos ou de tratamentos incorretos, os dados sensíveis sirvam para apoiar segregação de qualquer espécie. Um exemplo claro do que pode ocorrer em circunstância de dados processados sem a devida precaução são o surgimento de "bolhas de informação" onde o indivíduo é conduzido por algoritmos que possuem ciência de seus interesses, e a partir disso, indica apenas conteúdos alinhados com este foco.

DADOS ANONIMIZADOS

Se um dado pessoal é o tipo de informação que pode identificar um indivíduo e o dado sensível é o que pode vincular a ele informações que tem origem na vida privada, ideologias e pensamentos, o dado anonimizado é a informação pessoal que não possui suficiente conteúdo para que seja o seu titular reconhecido.

O dado anonimizado pode ser obtido já em um formato de anonimização ou ser submetido a processo de descaracterização, onde o dado desassociado de seu original dono, estando concluído o processo no momento em que não se possa mais relacionar de forma alguma a informação coletada ao titular dos dados.

BANCO DE DADOS



A LGPD, protegerá tanto os dados guardados em meios físicos, como por exemplo, uma estante repleta de arquivos de funcionários ativos e inativos de uma empresa, quanto informações armazenadas em servidores ou em software em nuvem, como no caso de lista de fiéis que compareceram a uma missa por intermédio de vídeo conferência. Sendo assim, podemos dizer que bancos de dados são os diretórios, físicos ou virtuais, onde os dados são armazenados e tratados.

TITULAR

O titular é a pessoa natural a quem os dados pessoais se referem e são alvos de tratamento, sendo o principal sujeito tutelado por esta Lei que objetiva a proteção de seus direitos fundamentais de liberdade, privacidade e livre desenvolvimento da sua personalidade.

CONTROLADOR, OPERADOR E ENCARREGADO

Fixado pela lei como o maior responsável pelas decisões tomadas acerca do tratamento de dados pessoais, a figura do controlador pode ser de pessoa jurídica ou natural, de direito público ou privado, sendo de importante para a melhor aplicação da LGPD que seja definido de forma clara quem possui este aspecto. O operador é a quele que visa executar o tratamento de dados nos moldes definidos pelo controlador. Podendo ser esse agente de natureza pública ou privada e ser pessoa natural ou jurídica como é o caso do controlador, possui responsabilidades quanto as informações que processa e no caso de inobservância a instruções legítimas do controlador, sendo também citado pela LGPD, juntamente com o controlador, como "agentes de tratamento".

Encerrando este tópico, figura o encarregado, que se trata de pessoa indicada pelo controlador para que atue como intermediador, fazendo contato direto como o próprio controlador, os titulares e a Autoridade Nacional de Proteção de Dados sempre que necessário for.

TRATAMENTO DOS DADOS

O art 5º, inciso X da LGPD traz em seu bojo a definição sobre o que considera tratamento de dados pessoais. A partir desta definição, observasse a abrangência da proteção que a LGPD dedicada ao procedimento de uso e processamento de dados pessoais, dispoño inclusive de diferentes diretrizes para o correto tratamento para os dados tidos como sensíveis, dados de crianças e adolescentes, e demais dados que contenham informações de indivíduos, buscando assim, mais uma vez, assegurar que tais tratamentos não tragam dano a personalidade, honra e privacidade dos titulares.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A ANPD (Autoridade Nacional de Proteção de Dados), foi criada em 2018 e sancionada em 2019, e é o órgão independente, parte do governo federal ao qual compete a aplicação e fiscalização da LGPD, elaborando diretrizes e regulamentos quanto ao tratamento de dados pessoais, divulgando a sociedade brasileira a importância das políticas de proteção de dados e aplicando penalidades em caso de não observância da legislação.

DIREITOS DO TITULAR

Consta no art. 17 da LGPD, a afirmativa de que "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,2018), ou seja, os dados serão sempre de pessoas naturais, e sendo assim, como já visto anteriormente, não podem ser objeto de cessão ou transferência, pois os mesmos são configurados como direitos da personalidade de natureza intransmissível e irrenunciável, fazendo desta forma que qualquer negócio jurídico de cessão ou transferência de dados pessoais seja considerado nulo. Os direitos que podem ser pleiteados pelo titular dos dados através de requisição junto ao controlador são encontrados ao art. 18 da LGPD, onde a Lei admite alguns direitos subjetivos ao titular dos dados para que este possa controlar de maneira efetiva o fluxo de seus dados pessoais



quando em posse de agentes de tratamento. São esses os direitos a:

CONFIRMAÇÃO DA EXISTÊNCIA DE TRATAMENTO

Como se lê, é o direito que visa garantir ao titular a possibilidade de, a qualquer tempo, confirmar se suas informações pessoais estão sendo alvo e tratamento. Este é um direito alinhado ao princípio da transparência citado anteriormente, possibilitando a busca pela informação, mesmo que já tenha havido o aviso de que tais dados seriam foco de tratamento ao momento da sua coleta.

ACESSO AOS DADOS

O acesso aos dados pessoais devem ser facilitados e o titular deve poder consultá-los de forma clara, conforme preconizam os princípios de livre acesso e de qualidade dos dados, de forma que, assim que tiver a confirmação de que exista tratamento de dados referentes a si, ou ainda se já ciente de tais processamentos, o titular possa obter informações sobre as finalidades, os prazos, as origens e qualquer outra informação que desejar saber durante o período de tratamento.

CORREÇÃO DE DADOS INCOMPLETOS, INEXATOS OU DESATUALIZADOS

Tal direito se origina do princípio da qualidade dos dados, objetiva conferir ao titular a possibilidade de, constatado alguma inexatidão, desatualização ou incompletude, possa se exigir do controlador a correção devida de forma imediata, devendo o controlador manter registros e históricos destas mudanças e correções, para que, futuramente, possam servir de meio de comprovação tanto ao titular quanto aos agentes de tratamento envolvidos.

ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO DE DADOS DESNECESSÁRIOS

Como já anteriormente mencionado, o dado anonimizado é aquele que não possui a capacidade de identificar o titular de onde se originou. Sendo assim, a lei proporciona o direito a segurança de dado através desta anonimização sempre que solicitado.

O direito ao bloqueio de dados é uma medida de caráter temporário, onde objetiva a suspensão do tratamento por algum período. Em contra partida, a eliminação de dados requer a parada de qualquer tratamento e a exclusão total de informações pessoais pertencentes ao titular, ambas as situações podem ser exigidas tanto no decorrer do tratamento quanto ao seu final.

Estes direitos têm origem no princípio da necessidade, pois visam a retirada de dados desnecessários, excessivos ou que já alcançaram suas finalidades.

PORTABILIDADE DOS DADOS

A portabilidade de dados tem como objeto dar ao titular a possibilidade de transferir seus dados pessoais, mediante requisição expressa, a outro controlador, que após confirmar a migração, terá o agente de tratamento primitivo a possibilidade de manter as informações do titular que possuir. Porém, em caso de dados que se encontrem anonimizados pelo controlador, a portabilidade não poderá ser realizada, pois a legislação considera mais benéfico ao titular que referidos dados permaneçam anônimos.

ELIMINAÇÃO DE DADOS

Na circunstância que o titular desejar pela eliminação de suas informações pessoais, poderá ele pleitear a exclusão de seus dados pessoais junto ao controlador. Como anteriormente referido, o consentimento do titular é o requisito basilar para o tratamento de dados, sendo assim, qualquer processamento que estes dados recebam fora deste consentimento se perfará irregular, logo, poderá também ser descartado mediante pedido do titular. Oportuno frisar que a LGPD prevê que em casos que houverem obrigações legais ou regulatórias a serem cumpridas pelo controlador, estejam servindo para propósitos de estudos por órgão de pesquisa, forem transferidos para terceiros de forma a respeitar requisitos de tratamento



disposto em lei, ou em caso de uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados, será facultado aos agentes de tratamento a manutenção de dados após o término de seu tratamento.

INFORMAÇÃO DAS ENTIDADES PÚBLICAS E PRIVADAS COM AS QUAIS O CONTROLADOR COMPARTILHOU OS DADOS

Originado diretamente do princípio da transparência, este direito objetiva garantir ao titular a oportunidade de averiguar a quais entidades, de caráter público ou privado, o controlador, após previa permissão, compartilha ou compartilhou seus dados. Não sendo permitido ao agente de tratamento a ocultação de tais informações, com exceção apenas nas hipóteses de segredos comerciais e industriais.

INFORMAÇÃO SOBRE A POSSIBILIDADE DE NÃO FORNECER CONSENTIMENTO

Esta regalia, também vinculada ao princípio da transparência, tem como objetivo garantir ao titular de dados a possibilidade de saber que poderá oferecer, ou não, consentimento para o tratamento de seus dados, e além disso, quais as possíveis consequências de sua recusa ou anuência.

Em função do exposto, caso não se encontre dispostas esses informes de forma clara, poderá o titular exigir ao controlador esclarecimentos expressos e explícitos.

REVOGAÇÃO DO CONSENTIMENTO

Por fim, este é o direito que proporciona ao titular a segurança de, a qualquer momento, revogar o consentimento disposto ao início do processo. Devendo ser realizado através de manifestação expressa, sendo a este petitório garantido acesso facilitado e gratuito, de modo que, mesmo que no instante seguinte ao fornecimento do aceite, poderá o titular rescindir o consentimento, salvo nos casos relatos no item 5.6 anteriormente abordado. Sendo o consentimento fator primordial para a coleta e tratamento de dados pessoais, logicamente, o momento em que anuência é revogada demarca o fim da permissão possuída pelos agentes de tratamento para processar dados do titular, acarretando então irregular e ilegal todos os métodos doravante aplicados as informações pessoais, em respeito aos já largamente referidos princípios constitucionais da personalidade e privacidade.

Ao final deste tópico, convém dispor ainda que a alteração de finalidade do tratamento deverá sempre ser comunicadas ao titular, onde em todas as ocasiões, decidirá ele pela manutenção do consentimento ou a revogação da permissão.

RESPONSABILIDADE CIVIL

Originando-se da violação de norma legal que preexista no ordenamento, a responsabilidade civil pode ter em sua natureza a contratualidade ou extracontratualidade.

Uma vez tendo ocorrido a violação de direitos, o violado poderá pretender indenização por parte de quem os violou, seja esta lesão de natureza moral ou patrimonial.

A LGPD, em sua busca pela completude, tratou de trazer o tema responsabilidade civil em seu arcabouço, de forma a estabelecer ao controlador e ou operador, que em razão a tratamento irregular de dados pessoais der pavimento a danos deverá obrigatoriamente repará-los. Vide o art.42 da LGPD:

Vemos ao apreciar o caput disposto acima que não se tratou do importante elemento da responsabilidade civil que é a culpa, sendo assim, certas doutrinas defendem a configuração da responsabilidade objetiva para casos de dano envolvendo tratamento dados pessoais. Em contra partida, existem juristas que defendem a natureza subjetiva da responsabilidade civil voltada a LGPD, visto ser essa a predominância no meio jurídico civil e a lei geral de proteção de dados não se fazer, na opinião dessa vertente de pensamento, propriamente clara quanto a objetividade da responsabilidade, tendo traçado a subjetividade



que defende na leitura dos artigos 42 e 44 com seus incisos e parágrafo único, da LGPD, no sentido de que não basta apenas o desempenho da atividade de tratamento de dados para que seja possível imputar responsabilidade ao agente, sendo necessário para tanto, contrariedade da lei ou a não adoção de medidas adequadas.

Comprovado não haver ainda unanimidade, e sendo esse ainda um assunto que gera certa controvérsia no meio acadêmico, ambas as correntes doutrinárias aguardarão um consenso que provavelmente virá apenas das mãos do poder judiciário.

Considerando, para o fim acadêmico ao qual este trabalho se propõe, que a responsabilidade seja objetiva baseada na teoria do risco, partimos para a análise do artigo 43 da LGPD, onde se pode averiguar quais são os excludentes de ilicitude que poderão alegar os agentes de tratamento de dados:

Similarmente aos excludentes de ilicitude previstos no Código Civil e no Código de Defesa do Consumidor, a Lei Gral de Proteção de Dados afasta a responsabilidade pelo dano alegado pelo titular dos dados quando o agente de tratamento comprovar que não houve tratamento dos dados que lhe foram atribuídos, ou que, mesmo havendo existido o tratamento, não houver violação a LGPD, e por fim, que o dano tenha ocorrido por culpa de terceiro ou mesmo do próprio titular.

Oportuno apontar que a Lei nº13.709 de 14 de agosto de 2018, além de todo o já exposto no tocante da responsabilidade civil, ainda prevê a responsabilização solidária pelos danos causados pelo tratamento de dados que não obedecerem a legislação e, nos casos em que o controlador estiver envolvido com o tratamento de dados de forma direta, o tratamento de dados resultar em dano ao titular, também haverá a solidariedade. Para essas duas situações é possível o afastamento da responsabilidade através dos excludentes de ilicitude listados ao art.43.

Quanto a possibilidade de se inverter o ônus da prova, considera o legislador que, o titular de dados se encontra em desvantagem frente aos controladores e operadores, por esse motivo a inversão do ônus da prova poderá ser concedida caso haja hipossuficiência para produzir provas, ou caso a sua produção seja por demais onerosa, sendo essa uma designação similar à que o Código de Defesa do Consumidor atribui ao consumidor. Inclusive ressalta-se que em caso de violação de direitos de titular de dados no âmbito da relação de consumo, estará o controlador sujeito responsabilidade disposta no CDC, (Lei Nº 8.078, de 11 de Setembro de 1990).

Por fim, encontra-se no §4 do art.42 a possibilidade de ação regressiva, porém, ainda é difícil mensurar o grau de culpa de agente, e, em alguns casos, se faz árduo até mesmo encontrar o causador do dano.

OS GRANDES PERIGOS AO MEIO SOCIAL DO PROCESSAMENTO DE DADOS E A EFICÁCIA DA LGPD.

Ao longo destes últimos 30 anos, observamos as distâncias serem reduzidas a mero cliques, podemos acompanhar bibliotecas inteiras caberem na palma de apenas uma de nossas mãos, tivemos a oportunidade de nos maravilhar com um aparato que é capaz de reunir, em um só aparelho, as capacidades de dezenas de instrumentos essenciais para o desenvolvimento do cotidiano entre outros avanços formidáveis.

Experimentamos nas últimas décadas um aumento exponencial nas capacidades tecnológicas em geral, várias áreas foram completamente reinventadas e esses acontecimentos resultam em grandes desafios para a humanidade como um todo.

Vemos deste histórico de ascensão típica de um conto de Asimov, resultarem vários



incidentes nunca antes vistos pela humanidade, que assistiu a dinâmica da vida mudar quase que de repente. Só agora vemos os perigos aos quais estamos expostos. Expressões como, crimes cibernéticos, Ciberterrorismo, espionagem digital, já fazem parte do nosso vocabulário, e para contrapor tais ameaças a cidadania, os estados precisaram empreender vários esforços no sentido de tentarem encontrarem a justa posição entre a segurança e a livre iniciativa, ambas tão importantes para a continuação do desenvolvimento humanos e científico, na busca garantir a manutenção do *status quo*.

A partir dessa série de preocupações que países de todo mundo começaram a buscar legislar sobre pontos importantes desse novo paradigma mundial, e uma das suas principais preocupações foram as medidas protetivas de dados. Sobre a importância de proteger dados pessoais já tecemos ao longo deste artigo vários apontamentos, de como somos monitorados dia após dia, temos nossas informações pessoais coletados a todo o momento, e não nos referimos apenas ao nosso CPF ou CNH, que geralmente são recolhidos pelos tratadores de dados pessoais apenas uma vez, na contratação de serviços, ou nas realizações de pesquisas e etc, mas também captando constantes micro informações a nosso respeito.

Vemos que informações gerais de um indivíduo, como o que ele gosta de assistir, para onde ele costuma ir, com quem costuma falar, que horários costumam estar mais ativo entre outras, são perfeitamente capazes, em quantidade suficiente, de indicar a um fabricante, comerciante ou criador de conteúdo digital o que tem alguma chance de agradar está pessoa.

Continuemos agora imaginando que esse mecanismo se encontra minerando esses metadados de uma cidade inteira, sendo, a partir de uma amostra suficiente, capaz de através de estatística, vincular a um certo seguimento desta comunidade, propaganda direcionadas ao que agradariam estas pessoas, buscando vincular um candidato à prefeitura, por exemplo, a esses seus interesses. Por ventura, este candidato consegue replicar este método a outros seguimentos sociais e finalmente alcança a candidatura almejada. Essa vitória, possivelmente, se deu mediante exploração de dados recolhidos quase que de forma inofensiva, mas que em conjunto e bem compilados, possuem o poder de estabelecer impérios econômico e influenciar eleições importantíssimas para o cenário mundial. E tudo isso só se faz possível por que os produtos vendidos e comprados neste grande mercado somos nós, nossas vidas, nossas interações.

Devemos compreender que a legislação de proteção de dados significa, sobre tudo, a continuação de uma profunda mudança no meio jurídico, buscando não só a proteção conta os costumeiros golpes que utilizam nossos documentos pessoais para fins ilegais, mas além disso, tem a importante função de ser o bastião que tenta defender o hipossuficiente titular de informações pessoais de se ver despojado de sua personalidade em qualquer grau, evitando que seja alvo de descaracterização por incorreto, ou malicioso, tratamento de seus dados.

Esta importante legislação ainda objetiva resguardar o titular de dados pessoais das investidas de agentes de tratamento que, se não devidamente reguladas, possuem o condão de manipular e incutir necessidades e desejos "fabricados" em outros, podendo assim manobrar nossos intentos e macular nossas vontades.

CONCLUSÃO

Ao momento do encerramento deste volume, se chega a angustiante conclusão de que não temos domínio sobre nossos dados. Possuímos pouca ou nenhuma noção quanto a quantidade de nós que está agora vulnerável em algum recôndito obscuro da rede. Quando seremos julgados por esses amontoados de informações e não como as pessoas que somos?



Em que momento seremos um conjunto de informações vendidas a quem melhor pagar, para que depois de obtidos, esses aspectos virtuais de nossas vidas sejam usados para nos induzir a comprar o sapato daquela estrela do futebol ou o perfume daquele ator? Quando deixaremos de fazer nossas próprias escolhas pela influência de entidades que nos conhecem tão bem que, por vezes, são capazes de prever como será nosso comportamento futuro? A preocupante notícia é que, possivelmente, todas esses acontecimentos estão ocorrendo agora mesmo.

Referente a tais preocupações agora se abatem legislações por todos os cantos do planeta buscando a mitigação destes danos, sendo uma delas, a Lei 13.709/2018, Lei Geral de Proteção de Dados, onde, observando princípios cravados na história da humanidade, objetiva assegurar ao titular de dados o direito de se defender contra abusos, equívocos ou ardis aos quais podemos estar sendo alvos.

Contudo, tamanha é a complexidade deste tema, que a LGPD, sem sombra de dúvidas, se torna uma importante ferramenta que, no entanto, não consegue ainda alcançar a plenitude de sua função, tanto por ainda não possuir a efetiva aplicação a todos os campos que busca regular, quanto pela imprevisibilidade frente a todo esse desenvolvimento desenfreado da tecnologia e do plano digital. Sendo assim, uma importante base que somada a outras preciosas legislações, terão a difícil missão de acompanhar de perto os avanços dessa nova dinâmica da era da informação.

REFERÊNCIAS

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

BLUM e SANTOS, **Reflexões Sobre a Lei Geral De Proteção De Dados Pessoais**, NOONIS, 2020. Disponível em: < <https://noomis.febraban.org.br/especialista/renato-opice-blum/reflexoes-sobre-a-lei-geral-de-protacao-de-dados -pessoais>>. Acesso em: 24 de out. de 2022.

BRASIL, CNN. **'Mundo está em perigo e paralisado'**, diz Guterres na Assembleia-Geral da ONU 1 NOVO DIA, Youtube, 20 set. 2022. Disponível em: <<https://www.youtube.com/watch?v=oqwNHXzbOrA>>, Acesso em: 24 out. 2022.

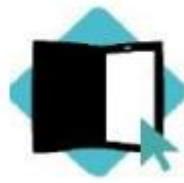
BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016].

Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 24 out. 2022.

BRASIL. **Lei n. 10.406, 10 de janeiro de 2002**. Institui o Código Civil. Diário oficial da união, Brasília, DF, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em: 24 out. 2022.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Lei de acesso a informação. Brasília, DF: Presidência da República, [2012]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm. Acesso em: 24 out. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei geral de proteção de dados pessoais (LGPD). Brasília, DF: presidência da república, [2020]. Disponível em:



https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em: 24 out. 2022.

BRASIL. **Lei nº 12.965, de 23 Abr de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2014/Lei/L12965.htm. Acesso em: 19 dez. 2014.

COTS e OLIVEIRA, **Lei Geral de Proteção de Dados Pessoais Comentada**. 2 ed. São Paulo: Editora Revista dos Tribunais, 2019.

DECLARAÇÃO universal dos direitos humanos, 1948. Disponível em: <<https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>>. Acesso em: 24 out. 2022.

FEIGELSON, B.; SIQUEIRA, A. H. A. **Comentários à lei geral de proteção de dados lei 13.709/2018**. 1 ed. São Paulo: Editora Revista dos Tribunais, 2019.

GDPR [Guia Completo]: **Tudo que você precisa saber sobre a lei**, FIA BUSINESS SCHOOL, 2019. Disponível em: <<https://fia.com.br/blog/gdpr/>>. Acesso em: 24 de out. de 2022.

GONZÁLEZ, Mariana. **5 desafios da proteção de dados pessoais com a LGPD**, Idblog, 2018. Disponível em: <<https://blog.idwall.co/desafios-protecao-de-dados-pessoais-lgpd/>>. Acesso em: 24 de out. de 2022.

Guia completo para estar em conformidade com a CCPA, Iubenda. Disponível em: <<https://www.iubenda.com/pt-br/help/43967-guia-completo-para-conformidade-com-a-ccpa>>. Acesso em: 24 de out. de 2022.

LEONARD, M. **Fundamentos de Direito Digital**. 1 ed. São Paulo: Editora Revista dos Tribunais, 2019.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais comentários à LGPD**: 3.ed. São Paulo: Saraiva Educação, 2021.

ROSEVALD, Nelson. **A LGPD e a despersonalização da personalidade**, Migalhas, 2021. Disponível em: <<https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/350374/a-lgpd-e-a-despersonalizacao-da-personalidade>>. Acesso em: 24 de out. de 2022.

TALKS, TEDx. **Por que proteção de dados pessoais importa?** 1 Bruno Bioni 1 TEDxPinheiros, Youtube, 17 out. 2019. Disponível em: <<https://www.youtube.com/watch?v=Tz15VfvQA6>>. Acesso em: 24 out. 2022.