A LEI GERAL DE PROTEÇÃO DE DADOS: UMA ANÁLISE ESTRUTURA E OS IMPACTOS CENÁRIO BRASILEIRO

REGINE GOMES RODRIGUES: Bacharelanda em direito pelo Instituto Matonense Municipal de Ensino Superior.

Resumo: Com o crescimento do uso das mídias sociais, cresce junto a ela a preocupação com a segurança dos dados pessoais, hoje chamado de "ouro digital", dessa forma, foi criada a lei de proteção de dados brasileira. Com base nos padrões europeus, a LGPD vem para modificar toda a sistemática dos sites, além de impor restrições e limitações para ouso dos dados dos usuários que utilizam sites em geral.

Palavra-Chave: "LGPD"; "Proteção de dados"; "internet"; "Lei de proteção de dados"

SUMÁRIO: INTRODUÇÃO. 2. AS INFLUÊNCIAS INTERNACIONAIS DA CRIAÇÃO DA LEI Nª 13.709/2018. 3.A Lei Geral de Proteção de Dados – Nª13.709/2018. 3.1. Os dados sensíveis e seu tratamento. 3.2.Os dados dos menores de 18 anos. 3.3. Do termino do tratamento das informações e Direito ao Esquecimento. 3.4. Da eliminação dos dados. 3.5. Direito ao Esquecimento.

3.6. Como Realizar a implementação da LGPD. 4. CONCLUSÃO. REFERÊNCIAS.

INTRODUÇÃO

Com o surgimento da internet em 1969, nos Estados Unidos, que recebia o nome de *Arpanet (Advanced Reserch Projects Agency)* se iniciou a evolução da internet em si, com várias transformações tecnológicas. Com isso, o mecanismo de comunicação entre as pessoas foi facilitado, sendo as navegações e troca de informações tornaram-se mais ágeis.

Atualmente, a sociedade utiliza a internet para todo o tipo de interação, seja para se comunicar com um amigo distante através das redes sociais, pedir comida de restaurantes locais ou ainda realizar pagamentos, dentre outros. Tudo isso ocorre através da realização do cadastro nestes aplicativos, onde as informações pessoais como nome completo, RG/CPF, endereço, dados bancários ou ainda algumas questões ligadas à religião, etnia, raça, e preferencias políticas, quem podem vir a permanecem armazenados.

Diante dessa transformação digital, o jornal "The Economist" chamou de "*Data Driven Economy*" ou seja, "Uma economia movida a dados", sendo esse conjunto de dados, que advém de diversas fontes, que tem movido economia atualmente. Através da obtenção desses dados, as mídias sociais, tem acesso não só as informações pessoais dos usuários, mais também suas preferências pessoais, como qual tipo de pet ele possui, qual o tipo de comida ele consome e até mesmo quais lugares ele frequenta, fornecendo através disto serviços e propagandas personalizados.

Contudo, toda esta inovação gerou um desconforto nos usuários desses serviços, por não saberem até onde está interação é segura, ou se tornou uma interferência a sua vida privada. Dessa forma, o presente artigo busca destacar quais são os direitos da população e os limites entre essa interação digital que se encontra presente em nosso cotidiano.

1. O PANORAMA NACIONAL

O conceito de privacidade foi citado pela primeira vez no Art. 12 da Declaração Universal de Direitos Humanos:

> *Art. 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 o ser humano tem direito à proteção da lei contra tais interferências ou ataques.*

Dentro do ordenamento brasileiro, a defesa deste direito foi estabelecida primeiramente em 1988, com o Art. 5ª, inc. X e LXXII, da Constituição Federal, e posteriormente art. 43 ss. do Código de Defesa do Consumidor, conforme segue:

> *Art. 5º, X – São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.*
>
> *LXXII – Conceder-se-á "habeas-data"*
>
> *Para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público.*

O escritor Stefano Rodotá, em seu livro "A Vida na Sociedade da Vigilância: A Privacidade Hoje", de 2008, p.92, afirma que "A privacidade na era da informação deverá ser definida pelo direito do sujeito de manter o controle sobre as próprias informações." Nesse contexto, é valorado as escolhas pessoais,

levando em consideração o poder que o indivíduo possui sobre o tratamento de seus dados, em contrapartida, temos o controle social e exposição às ameaças cibernéticas sendo nesse sentido, o direito se impõe para tutelar e proteger a privacidade do sujeito.

Como fatores que enfraquecem o direito fundamental da privacidade, podemos citar os mecanismos de segurança e vigilância oferecidos na era tecnológica e o detrimento da privacidade em prol do mercado, livre iniciativa e concorrência.

Dentro deste contexto, foram elaboradas diversas leis para que a proteção dos dados pessoais de forma que as informações transmitidas as empresas, fossem de forma ampla mantidas no sigilo, não apenas para a proteção do usuário, mas também, de certa forma, criar uma segurança jurídica para ambas as partes.

A esse respeito, podemos citar algumas leis que se destacam por sua grande repercussão no meio jurídico e popular, sejam elas, as leis de nº12.527/2011 (Lei de Acesso à informação), nº 12.737/2012 (Lei Carolina Dickemann) e a nº 12.965/2014 (Marco Civil), dentre tantas outras, já preparavam o caminho para a promulgação da LGPD, que chega para unificar e categorizando termos antes desconhecidos.

Com a vigência da presente lei a sociedade brasileira, o setor público, a doutrina e os institutos jurídicos, têm iniciado um processo de adequação à LGPD, que se mostra demasiadamente eficiente quanto a proteção dos dados dos usuários.

A sociedade atual é delimitada por fronteiras e a expansão tecnológica torna o acesso à informação mais democrática, facilmente acessada e com alta circulação. Dada a velocidade com que as informações são disseminadas, o direito possui a árdua missão para acompanhá-la, e a Lei de Proteção de Dados, se põe a diminuir essa distância e possíveis lacunas criadas devido à tal avanço.

A LGPD prevê ainda a anonimização de dados de forma a alcançar maior segurança aos dados fornecido aos prestadores de serviços através de mecanismos como supressão, encobrimento, generalização, perturbação, dados sintéticos e agregação, se colocam como formas de tornar a navegação na internet mais segura para a população.

2. AS INFLUÊNCIAS INTERNACIONAIS DA CRIAÇÃO DA LEI Nª 13.709/2018.

Na década de 80, a Convenção 108 do Conselho da Europa já tratava sobre o tema do tratamento automatizado de dados de caráter pessoal. Entre os assuntos abordados nesta convenção se encontra a necessidade do reconhecimento da necessidade de "conciliar os valores fundamentais no respeito à via privada e da livre circulação de informação entre os povos".

Na União Europeia, a proteção dos dados foi reforçada com a Diretiva 95/46/CE, de 1995, que tem como motivação principal, passar por todos os fundamento e finalidades que justificam o tratamento da adoção da proteção dos dados, os quais se aplicam princípios consagrados na Declaração Universal de Direitos Humanos, que de certa forma, influenciaram diretamente não apenas a formulação da lei brasileira, mais de qualquer outro país que se propôs a promover a proteção dos dados sensíveis.

Como afirma Leonardo Quintiliano em seu artigo ao "Instituto Avançado de Dados", *a proteção dos dados não pode ser tida, contudo, como óbice ao progresso econômico e social, nem ao desenvolvimento do comércio e do bem estar individual. Pelo contrário, é a segurança e confiança no sistema de tratamento de dados pelos indivíduos que potencializará o comércio e progresso social.*

Os dados protegidos pelas legislações atuais incluem as informações pessoais, que incluem até mesmo dados biométricos, que são armazenados e utilizados em registros de empresas privadas – como bancos – para o indivíduo, o cadastro de tal dado, como sua digital, se mostra como um facilitador, poupando-lhe tempo, e com isso gerará um crescimento no consumo, que nos faz retornar a questões capitalistas.

Entretanto, tal facilidade toma por base a confiabilidade na relação de consumo estabelecida entre o usuário e o prestador daquele serviço, devido ao armazenamento de informações sigilosas, que a princípio se encontram armazenadas com segurança. Devido a essa confiança, o usuário se expõe a ataques, fraudes ou até mesmo publicidades indesejadas, no caso do armazenamento de dados incorreto.

Por esta razão, a União Europeia, adotou não apenas normas, mas consolidou todos os princípios que devem reger o tratamento de dados numa sociedade da informação e de constitucionalismo multinível.

A tratativa da privacidade dos dados tornou-se mais pública nos dias atuais devido ao caso Edward Snowden, o ex-funcionário da cia que em 2013,

divulgou informações privilegiadas de operações americanas, expondo esquema de monitoramento global de ligações telefônicas e transmissões de internet dos cidadãos americanos e de alguns países, que se chamava PRISM.

Esta situação fez com que os governos começassem a se preocupar ainda mais com os dados sigilosos. Com isso em 2016, foi sancionado na União Europeia, o Regulamento Geral sobre Proteção de Dados (GDPR). O texto normativo serviu de inspiração para os demais países passarem a dispor sobre a proteção de dados.

3. A Lei Geral de Proteção de Dados – Nª13.709/2018

O Brasil ao promulgar a Lei de Proteção de Dados, se junta a diversos países que já possui legislação específica sobre o tema, estando relacionada diretamente a proteção dos dados considerados sensíveis.

A Lei de Proteção de Dados, sancionada em 2018, contudo apenas veio a vigorar em 18 de setembro de 2020, devido à crise do Coronavírus, com exceções que tratam da aplicação de sanções administrativas. Sendo que as sanções administrativas entraram em vigor a partir de agosto de 2021, devido a MP 959/2020.

Como bem explana o artigo 1ª da LGPD, a presente lei tem por objetivo a proteção dos dados pessoais, feito por pessoa natural ou jurídica, sendo está de direito público ou privado:

> *Art. 1º. Esta Lei dispões 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 diretos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural.*

Para a aplicação da lei é necessário observar alguns requisitos, previstos no art. 3º, quais sejam: I) A operação de tratamento seja realizada em território nacional; II) A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens um serviços ou o tratamento de dados de indivíduos localizados no território nacional, ou III) Os dados pessoais objeto do tratamento tenham sido coletados no território nacional, independentemente do meio, do pais de origem ou do país de localização dos dados.

A Legislação da Proteção de dados não será aplicada nos casos previstos do art. 4º, vejamos:

> *Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:*

I - Realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - Realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

*IV - Provenientes de **fora do território nacional** e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência **proporcione grau de proteção de dados** pessoais adequado ao previsto nesta Lei.*

Nos casos previstos no nos incisos do art. 4º podemos observar quando o tratamento dos dados deverá ser regido por legislação especifica e deverá prever medidas proporcionais e estritamente necessárias ao interesse público. Trazendo a luz o inciso IV do artigo, este faz menção aos dados provenientes de fora do território nacional, por exemplo, uma empresa Europeia solicita à uma empresa brasileira que realize o tratamento das informações pessoais de cidadãos alemães. Nesse caso nenhuma das empresas se sujeitará a LDGP, pois estão tratando de dados provenientes de fora do território brasileiro. Contudo, a lei do país proveniência dos dados deverá ser compatível ou de similar grau de proteção conferido pela lei nacional.

3.1. Os dados sensíveis e seu tratamento

Aqui chegamos ao impasse, afinal, o que são dados pessoais tratados pela LGPD? O conceito de "dado Pessoal" vem conceituado no art. 5º, sendo caracterizado como informação relacionada a pessoa natural identificada ou identificável.

Dessa forma podemos observar que os dados pessoais aqui tratados estão relacionados a uma pessoa física. Pessoas jurídicas, como empresas, não possuem dados pessoais, contudo elas podem tratar de tais informações, como por exemplo, de seus funcionários.

Um dado pode ser como o CPF ou número do telefone, ou um conjunto de dados que podem identificar uma pessoa. O que vai determinar que um dado é pessoal não é quantidade, mas sim como e em que contexto serão utilizados.

Por esta razão um dos princípios trazidos pela Lei é a necessidade que limita o tratamento mínimo das informações, necessário para a realização de suas finalidades com a abrangência dos dados pertinentes, proporcionais e não excessivos em relação ao tratamento dos dados, em outras palavras, "menos é mais".

Os dados sensíveis foram pormenorizados no inciso II do art. 5º, sendo estes sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos quando vinculados a vida natural.

A LGPD em seu artigo 6º nos apresenta não apenas o princípio da necessidade como dito anteriormente, mais também outros como finalidade, adequação, livre acesso, qualidade de dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Além da tratativa de princípios e sanções, nos é apresentado os agentes de tratamento, que são indivíduos que irão manipular os dados pessoais de outrem, e também a figura do controlador, que pode ser uma pessoa física ou jurídica, de direito público ou privado, à ele compete as decisões sobre o tratamento de dados. Logo, o controlador deverá definir a finalidade e os motivos para o tratamento de dados pessoais.

Esses agentes de controle ou operadores, devem observar os art. 42 e 43 da lei, que versam sobre a responsabilidade destes na tratativa dos dados, contudo devendo ser observado que no cometimento de ilícito, há possibilidade dos agentes não serem responsabilizados, no caso de por exemplo, provaram que não trataram dos dados pessoais que lhes foi atribuído, ou se no caso de terem sido responsáveis pelo tratamento destas, não houve a violação à legislação de proteção de dados e por último quando o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

Conforme explanado no decorrer deste artigo, os dados coletados pelos prestadores de serviços precisam do consentimento do usuário para sua utilização, ou seja, uma manifestação de vontade livre, informada e inequívoca do titular dos dados.

Atualmente, alguns sites tem solicitado aos seus usuários durante o cadastro, ou ainda para usuários habituais que confirmem estarem cientes o uso dos dados, conforme estipula a LGDP, a exemplo, temos as opções de privacidade do Windows 10:

Configuração de Privacidade Windows 10 - 1Configuração de Privacidade - Windows 10

É importante vigorar aqui que o consentimento dado pelo usuário poderá ser revogado a qualquer momento, da mesma forma que foi fornecida.

3.2. Os dados dos menores de 18 anos.

A LGDP ainda se tratando de dados pessoais, trouxe a luz o tratamento das informações de crianças e adolescentes menores de dezoito anos em seu artigo 14, pois se tratam de pessoas mais vulneráveis.

Levando em consideração duas tratativas, sendo a primeira elencada pelo Estatuto da Criança e do Adolescente (ECA) que tem como critério cronológico a capacidade do menor em seu art. 2ª, sendo consideradas crianças menores de 12 anos e adolescentes aquelas que tiverem entre 12 e 18 anos. E a segunda a do Código Civil, que tem como critério o regime de capacidade, sendo

os menores de 16 anos absolutamente incapazes e aquelas entre 16 e 18 anos relativamente incapazes devendo ser assistidos por seus responsáveis.

Sendo adotado para fim de tratamento de informações o precedido pelo Código Civil, dessa forma os dados fornecidos por menores deverão ser acompanhadas pelo consentimento tácito dos pais ou responsáveis.

Com isso, jogos e aplicativos e outras atividades semelhantes que possam ser utilizados por menores, deveram garantir que o fornecimento de informações pessoais do titular seja apenas estritamente necessário para a realização da atividade proposta pelo mesmo. Devendo estes dados serem coletado de forma clara, simples e acessível, com recursos visuais quando for adequado, tendo em vista que será necessário o consentimento do responsável e o entendimento adequado da criança.

3.3. Do termino do tratamento das informações e Direito ao Esquecimento

A previsão do término do tratamento se encontra art. 15 da LGPD, ocorrendo nas seguintes hipóteses:

I. Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance d finalidade especifica almejada;

II. Fim o período de tratamento;

III. Comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no §5º do art. 8 º da LGPD, sendo resguardado interesse público;

IV. Determinação da autoridade nacional, quando houver violação ao disposto na Lei Geral de Proteção de Dados.

Na primeira hipótese em que afirma ter sido alcançada a finalidade, sendo esta verificada a partir dos propósitos legítimos, específicos, explícitos e informados ao titular, cabendo ao controlador estipular o final do ciclo de vida dos dados e da necessidade de retê-los para outra finalidade, tendo nesta última outra base legal.

Quando os dados deixam de ser necessários ou pertinentes, o controlador deverá realizar uma verificação de risco dos dados armazenados, sendo analisado neste interim, o risco quanto a manutenção dos mesmos.

O fim do período de tratamento, ocorre quando a finalidade especifica que permitia o uso destes dados se finda, por exemplo dados trabalhistas ou previdenciários.

Da mesma forma que os dados podem ser descartados como podemos observar nas hipóteses citadas acima, existe ainda a possibilidade de retenção destes dados após o término do tratamento, previsto no art. 16 da LGPD, importante frisar que apenas há tal possibilidade, se as informações aqui armazenadas forem anonimizadas, sendo as possibilidades: i) o cumprimento de obrigação legal; ii) estudo por órgão de pesquisas, iii)transferência a terceiro, desde que respeitados os requisitos de tratamento previsto na lei; e iv) uso exclusivo do controlador sendo vedado o acesso de terceiros as mesma.

3.4. Da eliminação dos dados

No caso da não aplicação das hipóteses de retenção dados, a eliminação seja do dado ou de um conjunto de dados dos bancos de dados, deverá ser realizada, independentemente do procedimento utilizado pelo empregado responsável. Devendo ser inclusos backups, múltiplos acessos, servidores diferentes, armazenamentos em nuvens, entre outros meios de armazenamento. O responsável pelo tratamento destes dados, deverá informar e comprovar aos demais agentes sobre a conclusão do procedimento de eliminação.

3.5. Direito ao Esquecimento

Conceitualmente o direito ao esquecimento, também chamado como "direito de ser deixado em paz", faz referência ao direito de uma pessoa não permitir que algo que ocorreu em um momento de sua vida, não seja exposto e lhe traga mais transtornos. Tal direito se põe diretamente ligado aos conceitos da dignidade humana e a privacidade, que são princípios básicos previstos na Constituição Brasileira.

A exemplo de aplicabilidade deste direito, no Brasil, podemos citar alguns casos marcantes, como a Chacina da Candelária, onde o programa Linha Direta, procurou por Jurandir Gomes de França, um dos envolvidos no crime, que havia absolvido das acusações no Tribunal do Júri, o então serralheiro entrou com uma ação contra a emissora e o STF sustentou a importância do direito ao esquecimento, afirmando ainda que a exposição no programa causou danos à honra do mesmo.

A lei Europeia de proteção de dados, que deu base à elaboração da LGPD, aborda o direito ao apagamento dos dados, em seu artigo 17, "*o titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus*

dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos (...)"

Entretanto, é importante pontuar que o término do tratamento e direito ao esquecimento não são sinônimos. Ademais, o direito ao esquecimento não implica necessariamente na eliminação dos dados pessoais.

3.6. Como Realizar a implementação da LGPD

A adequação e implementação da Lei de Proteção de Dados, dependerá das particularidades de cada empresa, assim como dos dados a serem recolhidos dos usuários. Dessa forma, é necessário que a empresa realize mapeamento, defina uma base legal para o tratamento dos dados, assim como prazo e locais de retenção dos dados recolhidos, além de revisões de contratos e políticas de privacidade da empresa.

Devendo tais procedimentos serem realizados com a devida assessoria de um encarregado de dados e do departamento jurídico da empresa.

De pronto, a criação de um plano bem elaborado, concederá a empresa uma tratativa ainda mais próxima ao cliente, conhecendo as divergências entre empresa/cliente, e tomando conhecimento de possíveis problemas que podem resultar numa má qualidade de serviço prestado.

4. CONCLUSÃO

A Lei Geral de Proteção de dados, veio para completar um conglomerado de leis esparsas que o ordenamento jurídico Brasileiro possui, trazendo mais seriedade e aplicabilidade para a proteção dos dados pessoais e dados sensíveis, ainda que as sanções administrativas ainda não estejam vigorando, a adequação a presente lei se faz necessária por toda e qualquer empresa que faz uso destas informações sensíveis.

Como podemos observar, mesmo sendo uma legislação consideravelmente nova, se vale de aspectos antigos quanto a sua elaboração, com inspiração no Regulamento Geral sobre Proteção de Dados (GDPR), terá um grande impacto nas empresas e nos consumidores. No Brasil, atuais casos de uso indevido, comercialização e vazamento de dados, as novas regras garantem a privacidade dos brasileiros, além de evitar entraves comerciais com outros países.

Em conclusão, a legislação atual, não tem como intuito dificultar a vida e s relações comerciais, mas trazer respaldos e segurança, estipulando

regras claras sobre o uso indevido das informações fornecidas pelos usuários de serviços.

REFERÊNCIAS

BRASIL. Constituição: República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988.

CARDOSO. Loni Melillo. LGPD: INSPIRAÇÃO, VIGÊNCIA E O DESAFIO DA EFICIÊNCIA DA NOVA LEI, disponível em: ConJur - Loni Cardoso: Inspiração, vigência e o desafio da eficiência da LGPD, acessado em 05/10/2021.

Lei de Proteção de Dados – Lei nª 13.709/2018, disponível em: L13709 (planalto.gov.br), acessado em 03/10/2021.

PANEK. Lin Cristina Tung. LEI GERAL DE PROTEÇÃO DE DADOS Nª13.709/2018 ANÁLISE DOS PRINCIPAIS ASPECTOS E DO CONCEITO PRIVACIDADE NA SOCIEDADE INFORMACIONAL

QUINTILIANO. Leonardo. CONTEXTO HISTORICO E FINALIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD), disponível em : https://iapd.org.br/contexto-historico-e-finalidade-da-lei-geral-de-protecao-de-dados-lgpd/ , acessado em 04/10/2021.

RODOTÁ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008

SEBRAE, LEI GERAL DA PROEÇÃO DE DADOS PESSOAIS, disponível em: https://www.sebrae.com.br/sites/PortalSebrae/canais_adicionais/conheca_lgpd, acessado em 08/10/2021.