IEJA

Instituto de Estudos
Jurídicos Aplicados

Estudos Jurídicos

LGPD e Democracia

“Dados são o petróleo do mundo digital”

Essa frase, que pode ser considerada a metáfora da década, chama a atenção para o valor de informações cujo uso e tratamento acarretam consequências que vão muito além do mundo digital. Escândalos como o vazamento de dados de milhões de usuários do Facebook e o uso desses dados pela Cambridge Analytica para influenciar as eleições americanas alertaram o mundo sobre a iminente importância em proteger e regulamentar o uso e o tratamento desses dados.

Acontecimentos como o “genocídio dos Rohingyas”, em Myanmar, entre outubro de 2016 e agosto de 2017, expuseram como a manipulação de dados de uma mídia social como Facebook pode ser utilizada para incitar violência, ódio e culminar na perseguição e morte de milhares de pessoas.

No relatório da Organização das Nações Unidas (ONU) sobre os crimes em Myanmar, os investigadores afirmaram que os militares realizaram assassinatos e estupros em massa na população de etnia muçulmana Rohingya, evidenciando intenções de genocídio, e recomendaram que o Comandante Chefe da operação, juntamente com cinco generais, deveriam ser processados por orquestrar tais crimes contra a humanidade. O relatório da ONU mostra que os militares utilizaram dados e a própria plataforma Facebook para incitar ódio e violência contra os Rohingya, recomendando que a extensão da responsabilidade dos posts e mensagens do Facebook que influenciaram essa discriminação e violência fosse investigada independentemente, além de afirmar que a resposta da plataforma ao episódio foi lenta e ineficiente.

Relatórios internos do próprio Facebook, publicados em 2018, evidenciam a influência política que as redes sociais podem exercer.

De acordo com as informações ali presentes, 64% das pessoas que se associaram a grupos extremistas o fizeram porque o algoritmo da plataforma os conduziu, ou seduziu, àqueles grupos.

O documento mostra, ainda, que notícias falsas (fake news) são compartilhadas 6 (seis) vezes mais rapidamente que notícias reais. A gravidade do tema foi, também, abordada em reportagem recente do jornal New York

Times, segundo a qual o número de países com campanhas de desinformação política duplicou nos últimos dois anos, várias com consequências eleitorais e políticas que fragilizaram a democracia em países como Honduras, Espanha, Azerbaijão, Bolívia, Ucrânia, Equador, Brasil, Estados Unidos da América e até no Reino Unido, com o Brexit. Como consequência, ex-funcionários de empresas como Facebook, Twiter, Google e Instagram, entre outras, estão cada vez mais pedindo demissão por razões éticas e expondo a maneira manipulativa que as empresas tratam e comercializam os dados de seus usuários.

Notícias falsas (fake news) são compartilhadas 6 (seis) vezes mais rapidamente que notícias reais

A LGPD foi sancionada nesse contexto mundial, para regular um mercado amplo, poderoso, altamente lucrativo e que tem apresentado mais poder e influência do que qualquer governo. O desafio, claramente, é imenso, mas a lei é o primeiro passo para proteger cidadãos não apenas do regular "hackeamento" de dados como número de cartão de crédito ou conta de WhatsApp, mas a própria Democracia.

Histórico da LGPD

O Projeto de Lei (PL) 4.060/2012, de autoria do Deputado Milton Monti, alterando os artigos 7º e 16º da Lei 12.965, de 2014 (conhecida como Marco Civil da Internet), foi sancionado em 14 de agosto de 2018 e transformou-se na Lei 13.709/18, a Lei Geral de Proteção de Dados.

Para contextualizar a tramitação e aprovação da LGPD, é importante retornar a 2013, quando, poucos meses após a apresentação do PL no Congresso, veio a público, através do site Wikileaks, inúmeros documentos de um ex-funcionário da NSA, a agência de segurança americana, mostrando que as principais empresas de internet sediadas nos Estados Unidos da América violam a privacidade de seus usuários, franqueando acesso dos

dados de seus usuários à NSA. O Google, em resposta ao relatório, admitiu que os usuários de seu serviço de email não poderiam ter a "expectativa razoável" de inviolabilidade de suas mensagens e afirmou, em processo judicial, que "todos os usuários de e-mail devem necessariamente esperar que seus e-mails sejam sujeitos a processamento automático". O escândalo teve grande repercussão internacional e causou inclusive um incidente diplomático entre Brasil e Estados Unidos quando foram divulgadas informações de que a NSA continha informações sigilosas e pessoais da Presidência da República do Brasil.

Anos depois, apesar do investimento e melhora sobre a segurança dos dados, a cultura de Big Data, Data driven economy, Internet das Coisas e Inteligência Artificial cresceu exponencialmente, e com ela cresceu o acúmulo, o tratamento e a comercialização dos dados pessoais pelas grandes empresas, com um sensível desenvolvimento no algorítmo que "trata" esses dados. Esse crescimento, entretanto, deu-se num ambiente sem nenhuma regulamentação, com o número de escândalos sobre vazamento de dados e suas diversas consequências aumentando a cada ano. Até que, em 2018, entrou em vigor na União Européia o Regulamento Geral de Proteção de Dados (GDPR) e o Estado da Califórnia, onde estão sediadas grande maioria de empresas de tecnologia nos Estados Unidos, aprovou o Pacto de Privacidade do Consumidor (CCPA, da sigla em inglês), que entrou em vigor em janeiro de 2020. A GDPR Européia tornou-se a base legal padrão para a legislação de proteção de dados de praticamente todos os 80 países que possuem uma lei específica sobre o assunto, entre eles, o Brasil.

No Brasil, a LGPD tramitava no Congresso desde 2012, mas foi em 2018, com o escândalo sobre a Cambridge Analytica utilizando dados e a plataforma do Facebook para interferir nas eleições americanas, que o Congresso brasileiro enxergou o perigo que um mercado de dados desregulado está sujeito e, em agosto de 2018, aprovou a LGPD, com vacatio legis de 24 meses. Com a pandemia do Covid-19, várias tentativas em prorrogar a data de vigência da lei circularam no Congresso, mas o Senado Federal, em 26 de agosto de 2020, na votação da Medida Provisória (MP) 959/20, manteve a data original para a entrada em vigor da lei, que foi sancionada, entrando em vigor no dia 18 de setembro de 2020.

Fundamentos, Conceitos e Definições da LGPD

Para proteger os cidadãos brasileiros e evitar que o uso e tratamento dos dados desses cidadãos não sejam utilizados como objeto de manobra para desestabilizar o Estado Democrático de Direito, a LGPD apresenta, em seus três primeiros artigos, seus fundamentos e objetivos:

Universalidade e padronização

O regramento sobre o uso e tratamento de dados pessoais é aplicável no setor público e privado e independe do método utilizado, que pode ser informatizado ou não, on-line ou off-line e do setor econômico, aplicando-se a todas as empresas, sem exceção.

Inovação e desenvolvimento

O fomento à inovação, ao desenvolvimento econômico e tecnológico com a garantia da livre iniciativa, da livre concorrência e da defesa do consumidor.

Proteção

Respeito à privacidade, a liberdade de expressão, de informação, de comunicação e de opinião.

Proteção aos direitos humanos, ao livre desenvolvimento da personalidade, à dignidade e ao exercício da cidadania.

Segurança

Inviolabilidade da intimidade, da honra e da imagem.

Segurança das relações jurídicas e confiança do titular no tratamento de dados pessoais.

No artigo 3 tem-se o âmbito de aplicação da lei como sendo pessoas físicas ou jurídicas, de direito público ou privado, independentemente do meio,

que tratem ou coletem dados pessoais no Brasil ou para cidadãos brasileiros, independente da localização da sede da empresa ou da localização dos dados. Com isso, o legislador visa proteger o cidadão brasileiro de empresas multinacionais que tentem utilizar uma filial fora do país para não obedecer a LGPD, quando o destino final do tratamento dos dados é o cidadão e mercado nacional.

O artigo 5º da Lei apresenta seus Principais Conceitos, definindo claramente os sujeitos a que se referem cada termo utilizado na legislação e suas responsabilidades:

Dado Pessoal: qualquer informação relacionada a uma pessoa física (natural) que capacite a identificação de sua identidade, garantindo assim a proteção à privacidade (art. 5º, I). Os dados podem ser sensíveis e/ou anonimizados (art. 5º, II e III).

Titular: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (art. 5º, V).

Tratamento: Toda operação realizada com dados pessoais, como coleta, utilização, processamento, armazenamento e eliminação (art. 5º, X).

Controlador: Pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI).

Operador: Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII).

E, no artigo 6, a lei lista os princípios para o tratamento de dados, que além da boa-fé, incluem:

Finalidade: propósitos legítimos, específicos, explícitos e informados, ficando impossibilitado o tratamento incompatível com essa finalidade.

Adequação: uso dos meios compatíveis com a finalidade.

Necessidade: limitação do tratamento ao mínimo necessário para atingir a finalidade informada.

Livre acesso: consulta facilitada e gratuita aos titulares sobre o tratamento.

Qualidade: garantia de integridade e atualização dos dados pessoais.

Transparência: informações claras, precisas e acessíveis sobre as condições do tratamento.

Segurança: adoção de medidas técnicas e administrativas para proteção dos dados pessoais.

Prevenção: medidas para prevenir a ocorrência de fatos danosos.

Não discriminação: vedação para tratamentos discriminatórios ilícitos ou abusivos.

Responsabilização e prestação de contas: demonstração e comprovação do cumprimento da lei.

Embora fundamentais e de vital importância para a eficácia da lei, tais princípios exigem uma completa alteração na atual política de acumulação de dados pelas empresas, que atuam com a idéia de adquirir sempre a maior quantidade de dados possível e, agora, com a entrada em vigor da LGPD, precisarão se adaptar a adquirir o mínimo de dados para atingir uma finalidade específica e ainda com total transparência no tratamento e venda desses dados.

A lei exige uma verdadeira revolução no pensamento, na cultura empresarial em relação aos dados, como pode-se inferir também através dos requisitos exigidos para o tratamento dos dados elencados no artigo 7:

Consentimento do titular

Cumprimento de obrigação legal ou regulatória do controlador

Execução de políticas públicas pela administração pública

Realização de estudos por órgãos de pesquisa

Execução de contrato ou procedimentos preliminares a um contrato do qual seja parte o titular, a pedido do titular

Exercício regular de direitos em processos judiciais, administrativos ou arbitrais

Proteção da vida ou da incolumidade física do titular ou de terceiro

Tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias

Atendimento aos interesses legítimos do controlador ou de terceiro, salvo quando prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção de seus dados pessoais

Proteção do crédito.

Para garantir uma completa eficácia e aplicabilidade, a lei elenca os direitos dos titulares dos dados em seu artigo 18, conferindo ao titular total direito à transparência e liberdade para exigir desde a finalidade até a exclusão de seus dados. As hipóteses permitidas para transferência internacional dos dados são extremamente restritas, estando elencadas no art 33 e a as regras para segurança e sigilo dos dados, com todo o procedimento para adoção de medidas de segurança constam no artigo 46.

LGPD nos Tribunais Brasileiros

A LGPD é a primeira legislação específica para proteção de dados no Brasil, entretanto, não é a primeira lei a garantir a privacidade ou a zelar pela proteção de dados dos cidadãos, embora em outro contexto histórico e tecnológico. A proteção de dados dos usuários permeiam diversas bases legais brasileiras, desde a Constituição Federal, no seu artigo 5º, X, que garante o direito à privacidade, até os Códigos Civil (Lei nº 10.406/2002) e do Consumidor (Lei nº 8.078/1990), entre outras, como:

Lavagem de Dinheiro (Lei nº 9.613/1998, atualizada em 2003 e 2012);

Sigilo Bancário (Lei Complementar nº 105/2001);

Banco de Dados para Histórico de Crédito (Lei nº 12.414/2011);

Acesso à informação (Lei nº 12.527/2011);

Crimes Cibernéticos (Lei nº 12.737/2012);

Princípio de Garantias e Direitos para uso da Internet (Lei nº 12.965/2014) - Marco Civil da Internet.

Exemplificando a aplicabilidade da legislação existente para a proteção de dados, em dezembro de 2019, o Ministério da Justiça, através do Departamento de Proteção e Defesa do Consumidor e da Secretaria Nacional do Consumidor, multou o Facebook no valor de R$ 6,6 milhões de reais pelo compartilhamento indevido de dados, baseado no Código do Consumidor.

O Supremo Tribunal Federal (STF), ao analisar questões sobre a proteção de dados, utilizou tais leis em diversos julgamentos, como:

MS 23.452 (relator: ministro Celso de Mello): sobre o sigilo bancário, fiscal e telefônico;

RHC 132.115 (relator: ministro Dias Toffoli): sobre a aplicação do sigilo telefônico para e-mails, mostrando a rápida adaptação dos instrumentos legais existentes às evoluções tecnológicas;

RE 1.037.396 (relator: ministro Dias Toffoli): questionando a constitucionalidade do art. 19 da Lei 12.965, de 2014, o Marco Civil da Internet, que versa sobre a responsabilidade civil do provedor de internet de tornar indisponível conteúdo ofensivo, obedecendo decisão judicial;

ARE 660.861 (relator: ministro Luiz Fux): sobre o dever da empresa hospedeira de sítio na internet fiscalizar o conteúdo publicado e retirá-lo do ar quando considerado ofensivo, sem intervenção do Judiciário;

RE 1.010.606 (relator: ministro Dias Toffoli): sobre a aplicabilidade do direito ao esquecimento na esfera civil quando for invocado pela própria vítima ou pelos seus familiares;

ARE 1.042.075 (relator: ministro Dias Toffoli): sobre a licitude do acesso a informações contidas em aparelho celular;

ADC 51 (relator: ministro Gilmar Mendes)

A Federação das Associações das Empresas de Tecnologia da Informação (Assespro Nacional) impetrou a Ação Direta de Constitucionalidade

pedindo a declaração de constitucionalidade do MLAT, um acordo de cooperação jurídico-penal firmado entre Brasil e Estados Unidos sobre o acesso americano a dados virtuais armazenados fora de sua jurisdição.

O ministro Gilmar Mendes convocou uma audiência pública sobre o tema, onde representantes de empresas como Yahoo, Facebook e associações de empresas nacionais compareceram para discutir o assunto, apresentando diversas questões fáticas e jurídicas relevantes sobre a constitucionalidade e efetividade do acordo. Ao final da audiência pública, o ministro afirmou a necessidade em encontrar "um ponto de encontro entre o Estado, os novos modelos de negócio na economia digital e os direitos dos cidadãos à privacidade".

ADI 6.387, ADI 6388, ADI 6389, ADI 6393, ADI 6390 (relatora: ministra Rosa Weber)

Impetradas contra a Medida Provisória (MP) 954/2020 que previa o compartilhamento obrigatório de dados de usuários de empresas de telecomunicações com o IBGE, para a produção de estatística oficial durante a pandemia do coronavírus.

O Tribunal, por maioria, referendou a medida cautelar deferida pela ministra Rosa Weber, relatora do processo e suspendeu a eficácia da MP, vencido o ministro Marco Aurélio. Ao deferir a liminar, a ministra Rosa Weber reconheceu e aplicou os conceitos introduzidos pela LGDP na legislação, associando-os a direitos fundamentais constitucionais e alegou que o compartilhamento afrontava os direitos fundamentais da intimidade e vida privada.

A ministra, ao citar a LGPD, ressaltou a importância em observar os princípios de autodeterminação informativa, adequação, necessidade e transparência sobre as atividades de tratamento dos dados. O respeito ao devido processo legal na elaboração de políticas públicas envolvendo o tratamento de dados pessoais foi exaltado, uma vez que a MP previa o compartilhamento de dados de forma geral e irrestrita, com finalidade relativamente indeterminada e praticamente sem mecanismos de segurança;

ADI 5.527 (relatora: ministra Rosa Weber) e ADPF 403 (relator: ministro Edson Fachin)

Analisando a possibilidade de bloqueio de serviços de aplicativos de mensagens (WhatsApp) por ordem judicial e a constitucionalidade da ordem judicial de acesso, por órgãos do Estado, ao conteúdo de comunicações protegidas por criptografia.

A ADI e a ADPF questionam a constitucionalidade dos arts. 7º, II, art. 10, parágrafo 2º, e art. 12, incisos III e IV do Marco Civil da Internet, que vêm sido utilizado pelo judiciário para bloquear os serviços de aplicativos de mensagens; e, se a sanção prevista no inciso III do art. 12 do mesmo diploma legal pode ser aplicada pelo Poder Judiciário. Na ADPF, houve a recusa da empresa em fornecer conteúdos que serviriam de prova numa ação criminal.

A ministra Rosa Weber afirmou não haver ilegalidade na utilização da criptografia, que inviabiliza o acesso direto ao conteúdo das mensagens pelas empresas e garante um serviço mais seguro aos usuários. A ministra afirmou também não haver inconstitucionalidade nos dispositivos legais questionados, mas equívoco na interpretação realizada por algumas autoridades ao querer obrigar as empresas a reduzir a proteção da privacidade e comunicação dos usuários.

O ministro Edson Fachin também defendeu a inconstitucionalidade das determinações de bloqueio do aplicativo pelos juízes de primeira instância. O ministro também defendeu o direito à liberdade de expressão, a privacidade e ao sigilo das comunicações e concluiu reconhecendo a criptografia e anonimato como ferramentas para garantir tais direitos na internet, não enxergando nenhuma vantagem na promoção de medidas de relativização da segurança da internet, mesmo que em nome da segurança pública.

As decisões do STF têm evidenciado o posicionamento do Tribunal no sentido de garantir online a proteção dos direitos que as pessoas possuem offline, deixando claro que Direitos digitais são direitos fundamentais, como defende o Conselho de Direitos Humanos das Nações Unidas (A/HRC/RES/32/13). No Congresso, em consonância com a visão do tribunal, está em tramitação a Proposta de Emenda à Constituição (PEC) 17/2019, que altera a Constituição para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. A PEC está pronta para ser incluída na pauta do Plenário da Câmara dos Deputados.

A LGPD e os escândalos envolvendo vazamentos e o tratamento manipulativo de dados entretanto, acrescentam à discussão sobre a garantia dos direitos fundamentais a diferenciação entre a necessidade em garantir a liberdade de expressão e de privacidade, e a capacidade de alcance de opiniões, em sua grande maioria falsas, além de não solicitadas, e que, recentemente, têm sido utilizada para enfraquecer a democracia em vários países.

Com esse objetivo, o Projeto de lei 2.630/20, em tramitação na Câmara dos Deputados, tem como foco o combate à divulgação de notícias falsas (fake news) na internet e defende a elaboração de políticas públicas eficazes para combater a divulgação das fake news. O PL elenca normas e diretrizes para garantir a transparência nas redes sociais e em serviços de mensagem para coibir o uso abusivo e potencialmente danoso aos indivíduos ou à coletividade. Algumas organizações civis e acadêmicas, entretanto, argumentam que o tema precisa ser discutido de maneira mais ampla e mostram a preocupação do PL impactar o regime de liberdade de expressão assegurado pelo Marco Civil da internet. Além do PL, o Congresso investiga membros do governo federal na CPI das fake news e, no STF, o ministro Alexandre de Moraes conduz um inquérito (INQ 4781) para investigar crimes cometidos contra membros da Corte.

O ministro Dias Toffoli, então presidente da corte, instaurou o inquérito afirmando que o Tribunal e seus ministros têm sofrido, há algum tempo, ataques a sua integridade e honorabilidade por milícias digitais buscando atingir a instituição e o Estado Democrático de Direito. O ministro frisou que o objetivo do inquérito não é apurar críticas ou discordâncias, mas ataques digitais que anseiam minar a credibilidade da instituição:

“Estamos falando de notícias fraudulentas usadas com o propósito de auferir vantagem indevida, seja ela de natureza política ou econômica ou cultural”, disse.

O Plenário do STF, na Arguição de Descumprimento de Preceito Fundamental (ADPF) 572, cujo objeto era a Portaria 69/2019 da Presidência do STF (portaria que instaurou o inquérito) declarou a legalidade e constitucionalidade do Inquérito (INQ) 4781, prevalecendo o entendimento do relator, ministro Edson Fachin, de que a ADPF 572, é totalmente improcedente

“diante de incitamento ao fechamento do STF, de ameaça de morte ou de prisão de seus membros e de apregoada desobediência a decisões judiciais” disse o relator.

A LGPD apresenta-se, nesse cenário, como mais um instrumento capaz de defender as instituições, os cidadãos e o Estado Democrático de Direito, ao proteger o uso e tratamento dos dados e, assim, impedir a desenfreada disseminação das chamadas fake news por algoritmos digitais.

ANPD, Agentes de tratamento e responsabilidade civil

Nos artigos 37 a 40, a LGPD define os agentes responsáveis pelo tratamento de dados, o Controlador e o Operador, e define suas atribuições, as medidas de segurança que devem ser adotadas e estimula a formulação de regras de boa prática e governança. No artigo 41 apresenta a figura do Encarregado, elencando as atividades a este atribuídas e, nos artigos 42 a 45, a lei explicita a responsabilização civil que recai sobre os agentes responsáveis pelo tratamento de dados, quando houver violação da legislação.

Os artigos 52 a 54 da lei enumeram as sanções administrativas cabíveis aos agentes de tratamento que não obedecerem as regras sobre o uso e tratamento dos dados pessoais, apresentando penalidades rigorosas com multa de até 2% do faturamento da empresa, no total de R$ 50 milhões por infração, penalidade que não substitui a aplicação de sanções administrativas, civis ou penais. Tais sanções, entretanto, só entrarão em vigor no dia 1 de agosto de 2021, nos termos do art 65, inc I-A, incluído pela lei no 14.010/20.

Para garantir a aplicabilidade e eficácia da lei, seu artigo 55-A institui a Autoridade Nacional de Proteção de Dados, ANPD como órgão fiscalizador e regulador. O original artigo 55 gerou grande discussão no Congresso Nacional durante a tramitação da lei e foi vetado pelo então Presidente da República, Michel Temer, por vício de iniciativa. Logo depois, o Presidente criou a ANPD através da Medida Provisória 869/2018.

A ANPD possui autonomia técnica garantida por lei, mas será vinculada à Presidência da República, que editou o Decreto no 10.474/20 aprovando a estrutura regimental e o quadro demonstrativo dos cargos em comissão e das funções de confiança da Autoridade. A composição da ANPD será:

Conselho Diretor (CD), Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), corregedoria, ouvidoria, órgão de assessoramento e unidades administrativas/ especializadas para aplicação da LGPD.

O CD será formado por 5 membros, nomeados pelo presidente da República, com mandatos de 4 anos.

O CNPD terá 23 representantes, todos nomeados pelo presidente da República, sendo 11 do Estado (6 do Poder Executivo, 1 do Senado, 1 da Câmara dos Deputados, 1 do Conselho Nacional de Justiça, 1 do Conselho Nacional do Ministério Público e 1 do Comitê Gestor da Internet no Brasil), 4 de entidades da sociedade civil, 4 de instituições científicas e 4 do setor empresarial.

Competirá a ANPD a edição de normas e procedimentos para regulamentação da LGPD, bem como sua interpretação, fiscalização e aplicação das sanções previstas na lei, além de atuar juntamente com outros órgãos e entidades com competência sancionatórias e normativas de proteção ao Consumidor, entre outras atribuições descritas no artigo 55-J.

Instituto de Estudos
Jurídicos Aplicados

Ensinar é o que fazemos Direito

ieja.instituto institutoieja

ieja.instituto institutoieja institutoieja

institutoieja.com.br

SHIS QI 26, Conjunto 7, Casa 14, Lago Sul-DF
(61) 3970-5406 • contato@institutoieja.com.br