FACULDADE DE TECNOLOGIA DE SÃO PAULO

CAIO FERNANDES PEREIRA SANTOS

GDPR, CCPA E LGPD COMO INSTRUMENTOS LEGISLATIVOS PARA PROTEÇÃO DE DADOS PESSOAIS

Parecer do Professor Orientador

O TCC do aluno Caio Fernandes Pereira Santos atendeu à todas as exigências do DTI para Trabalhos de Conclusão de Curso

Conceito/Nota Final: 10.0 (Dez inteiros).

Atesto o conteúdo contido na mídia entregue e assinada por mim para avaliação do TCC.

Estou ciente de que se o aluno não tiver entregado a mídia conforme regras do Roteiro ele estará reprovado na disciplina mesmo que esteja aprovado por mim.

Orientadora: Profº. Me. Edméa Pujol Cantón

SÃO PAULO, 02 de Dezembro de 2021.

Edméa Pujol Cantón

Assinatura do Orientador

SÃO PAULO

DEZEMBRO - 2021

FACULDADE DE TECNOLOGIA DE SÃO PAULO

CAIO FERNANDES PEREIRA SANTOS

GDPR, CCPA E LGPD COMO INSTRUMENTOS LEGISLATIVOS PARA PROTEÇÃO DE DADOS PESSOAIS

SÃO PAULO

DEZEMBRO - 2021

FACULDADE DE TECNOLOGIA DE SÃO PAULO

CAIO FERNANDES PEREIRA SANTOS

GDPR, CCPA E LGPD COMO INSTRUMENTOS LEGISLATIVOS PARA PROTEÇÃO DE DADOS PESSOAIS

Trabalho submetido como exigência parcial para a obtenção do Grau de Tecnólogo em Análise e Desenvolvimento de Sistemas
Orientador: Prof°. Me. Edméa Pujol Cantón

SÃO PAULO

DEZEMBRO - 2021

Aos meus pais.

A minha querida mãe Dona Wilma, que sempre me acompanhou nos desafios dessa jornada. Neste momento, quero dedicar-lhe esta vitória e agradecer o apoio incondicional e por não ter me deixado desistir frente as dificuldades.

Amo você, mãe!

AGRADECIMENTOS

Minha Família.

Prof°. Edméa Pujol Cantón - orientadora.

Aos meus Professores do curso de ADS noite da FATEC-SP.

Aos funcionários do DTI da FATEC-SP.

“Não devemos pedir aos nossos clientes que façam um equilíbrio entre privacidade e segurança. Precisamos oferecer-lhes o melhor de ambos. Em última análise, proteger os dados de outra pessoa é proteger a todos nós.”

CEO da Apple, Tim Cook.

RESUMO

A discussão sobre legislações de proteção de dados pessoais não é tão recente. No início da década de 1990, a Europa aprovou a Diretiva n.º 95/46/EC, quando conceitos como algoritmos, arquivos em nuvem, marketing digital, aplicativos e redes sociais inexistiam. As regras valeram até 2018, quando entrou em vigência o Regulamento Geral de Proteção de Dados – General Data Protection Regulation (GDPR) –, que incentivou novas discussões sobre o assunto e influenciou a criação de leis como a brasileira Lei Geral de Proteção de Dados (LGPD) e a californiana California Consumer Privacy Act (CCPA).

No Brasil, antes da vigência da LGPD, desde setembro de 2020, o que valiam eram as regras do Marco Civil da Internet (Lei n.º 12.965/2014), que estabelecia regras para disciplinar o uso da internet e regular direitos e deveres dos internautas na navegação.

A vigência da Lei Geral de Proteção de Dados (LGPD) impacta diretamente empresas que trabalham de forma direta ou indireta com dados pessoais de clientes, tanto na esfera pública quanto privada, seja on-line ou off-line.

Com o aumento do uso indiscriminado de dados no universo virtual e o compartilhamento desenfreado de informações, seja em sites ou em redes sociais, é cada vez mais importante a aplicação de regras rígidas para proteger indivíduos.

Assim, neste trabalho são apresentados os recortes históricos e conceitos que envolvem a legislação atual, mostrando os princípios fundamentais da proteção de dados, os quais auxiliam a entender como empresas e entes públicos podem coletar e tratar informações de pessoas, estabelecendo direitos, exigências e procedimentos nesses tipos de atividades. Por fim, o trabalho responde a principal questão problema apresentada sobre a efetividade das principais legislações sobre a regulamentação de Proteção de Dados Pessoais, como a GDPR, a CCPA e a LGPD para proteger os dados dos indivíduos.

Palavras-Chave: Legislação; Privacidade; Proteção de dados; LGPD; GDPR; CCPA.

ABSTRACT

The discussion about personal data protection legislation is not so recent. In the early 1990s, Europe passed Directive 95/46/EC, when concepts such as algorithms, cloud files, digital marketing, applications and social networks did not exist. The rules were valid until 2018, when the General Data Protection Regulation (GDPR) came into force, which encouraged further discussions on the subject and influenced the creation of laws such as the Brazilian General Data Protection Law (LGPD) and the Californian California Consumer Privacy Act (CCPA).

In Brazil, before the LGPD came into effect, since September 2020, what mattered were the rules of the Marco Civil da Internet (Law No. 12.965/2014), which established rules to discipline the use of the internet and regulate the rights and duties of Internet users in navigation.

The validity of the General Data Protection Law (LGPD) directly impacts companies that work directly or indirectly with personal customer data, both in the public and private spheres, whether online or offline.

With the increase in the indiscriminate use of data in the virtual universe and the rampant sharing of information, whether on websites or social networks, it is increasingly important to apply strict rules to protect individuals.

Thus, in this work, historical excerpts and concepts involving current legislation are presented, showing the fundamental principles of data protection, which help to understand how companies and public entities can collect and process information from people, establishing rights, requirements and procedures in these types of activities. Finally, the work answers the main question raised about the effectiveness of the main legislations on the regulation of Personal Data Protection, such as the GDPR, the CCPA and the LGPD to protect the data of individuals.

Keywords: Legislation; Privacy; Data protection; LGPD; GDPR; CCPA

LISTA DE ABREVIATURAS E SIGLAS

GDPR	Regulamento Geral sobre a Proteção de Dados
CCPA	California Consumer Privacy Act
LGPD	Lei Geral de Proteção de Dados
UE	União Europeia
DPIA	Avaliação de Impacto de Proteção de Dados

Sumário

Introdução

Contextualização

A discussão sobre legislações de proteção de dados pessoais não é tão recente. No início da década de 1990, a Europa aprovou a Diretiva n.º 95/46/EC, quando conceitos como algoritmos, arquivos em nuvem, marketing digital, aplicativos e redes sociais inexistiam. As regras valeram até 2018, quando entrou em vigência o Regulamento Geral de Proteção de Dados – General Data Protection Regulation (GDPR) –, que incentivou novas discussões sobre o assunto e influenciou a criação de leis como a brasileira Lei Geral de Proteção de Dados (LGPD) e a californiana California Consumer Privacy Act (CCPA).

No Brasil, antes da vigência da LGPD, desde setembro de 2020, o que valiam eram as regras do Marco Civil da Internet (Lei n.º 12.965/2014), que estabelecia regras para disciplinar o uso da internet e regular direitos e deveres dos internautas na navegação.

Com o aumento do uso indiscriminado de dados no universo virtual e o compartilhamento desenfreado de informações, seja em sites ou em redes sociais, é cada vez mais importante a aplicação de regras rígidas para proteger indivíduos. Fatos ocorridos recentemente no Brasil mostram o porquê é importante este tipo de legislação.

Em janeiro de 2021, um megavazamento expôs dados de 220 milhões de brasileiros, entre eles informações como Cadastro de Pessoa Física (CPF), salário, escore de crédito, cheques sem fundos e números de telefone, entre outros.

Sobre esse megavazamento, apesar da proteção de dados já ser um tema debatido há décadas nos círculos especializados, é ainda um conceito muito novo para a maior parte das pessoas, e poucas empresas e organizações o consideram uma prioridade. Ao mesmo tempo, dados pessoais vêm sendo coletados em larga escala e tanto as práticas de mercado quanto, cada vez mais, práticas sociais vêm considerando-os como algo que pode ser compartilhado sem grandes cuidados (FGV, 2021).

No vazamento também foram divulgados dados de 104 milhões de veículos, de placas ao tipo de combustível usado, de modo que os vazamentos colocaram em alerta o setor de segurança da informação.

Logo depois, no início de fevereiro, mais de 100 milhões de pessoas, entre elas até o presidente, Jair Bolsonaro, tiveram as informações de suas linhas de telefonia celular vazadas, tais como minutos gastos com ligações, valores de faturas e até pagamentos atrasados.

Tais vazamentos colocaram em prova a vigência da LGPD e apontarão se, na prática, a legislação funcionará como deve. Com esta lei é obrigação das empresas garantir a integridade dos dados, sob o risco de multa de até 2% do faturamento com limite de até R$ 50 milhões.

Neste contexto o presente trabalho busca responder à seguinte questão problema: As principais legislações sobre a regulamentação de Proteção de Dados Pessoais, como a GDPR, a CCPA e a LGPD são efetivas para proteger os dados dos indivíduos?

Objetivo Geral

Explicar os fundamentos sobre as leis mais importantes relacionadas à privacidade e ao tratamento de dados pessoais da atualidade, as suas interpretações, as suas consequências e as suas eficiências.

Objetivos Específicos

- Entender as leis GDPR, CCPA e LGPD a partir da interpretação legal.
- Explorar os temas do Direito Digital e do Direito à privacidade dos dados.
- Identificar os desafios da proteção de Dados no Brasil e no mundo.

Justificativa

Estamos vivenciando um momento repleto de incertezas, o que é típico de uma mudança de Era e de um início de Século.

Presenciamos, na primeira década do século XXI, a ascensão à Era dos dados e, junto com ela, o consumo desenfreado em extrair o máximo desses dados, a ponto de, em um momento começarmos a dizer e a escrever que o dado é o novo petróleo!

A falta de regulamentação, a falta de segurança tanto jurídica quanto sistêmica, quanto ao uso dos dados capturados em massa em ferramentas da Internet e, posteriormente, “mastigados” desenfreadamente por algoritmos de *Machine Learning* que é um campo de estudo que dá aos computadores a habilidade de

aprender sem serem explicitamente programados para entender nossos dados, nossos comportamentos e gerar resultados que permitissem maior lucratividade e nossa maior dependência do que se chamou de ditadura do algoritmo, violava sistematicamente todas as Constituições das nações no que tange ao direito do indivíduo e seus dados (SIMON, 2013).

Percebendo isso, iniciou-se, em várias ações coordenadas, a criação de Legislação regulatória pertinente para assegurar os inalienáveis direitos do ser humano sob seus dados e sobre seus direitos como indivíduos.

Iniciativas como a GDPR, a CCPA e a nossa LGPD – Lei Geral de Proteção de Dados tentam regulamentar o uso de dados das pessoas e restabelecer seus direitos a sua propriedade individual como pessoas naturais, o direito à titularidade dos dados.

Metodologia

A pesquisa bibliográfica realizada no presente trabalho se baseia no método científico que divide a pesquisa em quatro etapas, sendo elas: a) A observação que é a etapa em que há execução dos questionamentos sobre o fato observado, no caso as legislações em questão; b) A experimentação, que é a etapa em que são realizadas experiências para provar a veracidade de sua hipótese, no caso os estudos de casos das aplicações das legislações em questão; c) A interpretação dos resultados, momento em que os resultados de sua pesquisa são interpretados; e, por fim, d) A conclusão, onde é feita uma análise final e considerável sobre o fato da questão problema (MARCONI; LAKATOS, 2003).

1. GDPR *(General Data Protection Regulation)*

Origem e Evolução do Direito à Privacidade

Na década de 1960 o educador, intelectual e filósofo canadense, Marshall McLuhan (1911-1980), um dos principais estudiosos sobre os meios de comunicação e a relação com a sociedade, já profetizava sobre a popularização de tecnologias como a internet e um mundo digital sem fios. Afirmava que os meios eram extensões do ser humano e davam ao homem novas formas de perceber e modificar o mundo à sua volta (COSTA, 2011).

Os conceitos defendidos por esse intelectual começaram a se tornar realidade a partir do lançamento do primeiro computador, em 1977. Com a evolução tecnológica e o surgimento de soluções como a internet, telefone celular e as redes sociais, novas configurações de relacionamentos e práticas de socialização foram estabelecidas, de modo que atualmente é praticamente impossível se imaginar em um mundo sem o smartphone.

Neste mundo hiperconectado, onde o trânsito de dados de usuários da internet é cada vez maior, surgiram dilemas éticos e novos desafios que apontaram para a necessidade de ferramentas para regular o uso indiscriminado de dados no universo virtual.

Com a utilização de dados pessoais cada vez maior por empresas e entidades públicas e privadas, vários países adotaram leis de proteção para regulamentar o uso. Uma das pioneiras é o GDPR, ou Regulamento Geral sobre a Proteção de Dados, válido para países da União Europeia e empresas que tratam dados de titulares que moram nessa região.

A União Europeia até tinha leis relacionadas à privacidade, mas eram de 1995 (Diretiva n.º 95/46 CE) e não correspondiam ao cenário tecnológico atual.

O projeto do GDPR foi iniciado em 2012 e aprovado em 2016, iniciando discussões sobre a proteção de dados em vários cantos do Planeta. Inspirou, por exemplo, a criação da CCPA – Lei de Privacidade do Consumidor da Califórnia – e da LGPD – Lei Geral de Proteção de Dados – no Brasil.

Princípios Fundamentais da Proteção de Dados Pessoais

Conforme o GDPR, ao processar dados pessoais, os responsáveis devem se nortear pelos seguintes princípios básicos (PARLAMENTO EUROPEU, 2016):

- Licitude, lealdade e transparência: todos os titulares devem ser informados dos principais elementos de tratamento de seus dados pessoais de forma clara, facilmente acessível, concisa, transparente e inteligível;
- Adequação e limitação da finalidade: os dados devem ser tratados com uma finalidade específica e, subsequentemente, utilizados apenas na medida em que esse uso não seja incompatível com a finalidade;
- Necessidade ou minimização: prevê que os dados pessoais devem ser adequados, pertinentes e limitados em relação aos fins para os quais serão processados. O objetivo é diminuir a quantidade de dados, coletando apenas aqueles que sejam essenciais para o produto ou serviço ofertado
- Qualidade dos dados ou exatidão: os dados devem ser exatos e, quando necessário, objetos de atualização, além de adequados, pertinentes e não excessivos relativamente às finalidades para as quais são tratados;
- Limitação da conservação: os dados não devem ser conservados mais tempo do que o necessário;
- Segurança, integridade e confidencialidade: qualquer entidade que proceda ao tratamento de dados pessoais deve assegurar que tais dados serão tratados de modo a garantir a sua segurança;
- Prestação de contas ou responsabilização: exige que as organizações implementem medidas técnicas e organizacionais apropriadas, assim como sejam capazes de prestar contas e demonstrar eficácia, quando solicitadas.

Direito dos Titulares e Dados Pessoais

O GDPR descreve uma relação de direitos concedidos ao titular de dados para assumir o controle de suas informações para a sua própria proteção.

Um dos principais conceitos neste item está relacionado à transparência, ou seja, a empresa que coleta e trata os dados deverá deixar clara a finalidade do uso destes dados e mais, deverá ter o consentimento para este mesmo uso.

Entre os direitos dos indivíduos, pode-se remover o consentimento de ter os seus dados retificados ou definitivamente removidos após o encerramento da relação

entre as partes. Os titulares também têm direito à limitação do tratamento de seus dados por parte das empresas e entidade, podendo limitar a utilização enquanto houver equívocos em seus registros.

O guia do cidadão para a proteção de dados na EU compartilha os seguintes direitos do titular (COMISSÃO EUROPEIA, 2019):

- Transparência das informações, comunicações e regras para o exercício dos direitos dos titulares dos dados;
- Informações a facultar quando os dados pessoais são recolhidos junto do titular;
- Informações a facultar quando os dados pessoais não são recolhidos junto do titular;
- Direito de acesso do titular dos dados;
- Direito de retificação;
- Direito ao apagamento dos dados (direito a ser esquecido);
- Direito à limitação do tratamento;
- Obrigação de notificação da retificação ou apagamento dos dados pessoais, ou ainda limitação do tratamento;
- Direito de portabilidade dos dados;
- Direito de oposição;
- Decisões individuais automatizadas, incluindo definição de perfis;
- Limitações.

Segurança dos Dados Pessoais

Para garantir a segurança dos dados pessoais, o Regulamento dispõe sobre algumas medidas que as organizações devem colocar em prática, levando em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, contexto e as finalidades do tratamento, bem como os riscos – de probabilidade e gravidade variável – para os direitos e as liberdades das pessoas singulares.

O responsável pelo tratamento e o subcontratante devem aplicar as medidas a seguir para assegurar um nível de segurança adequado ao risco:

- A pseudonimização e cifragem dos dados pessoais como medidas baseadas em riscos para proteger a segurança dos dados e os direitos dos indivíduos;

- A anonimação, ou seja, a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e serviços de tratamento;
- A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
- Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Neste item, o Regulamento dispõe sobre a notificação de uma violação de dados pessoais à autoridade de controle competente, ou seja, os controladores de dados devem relatar qualquer violação às suas autoridades de proteção de dados em até 72 horas após conhecimento da mesma, a menos que seja improvável que a violação prejudique as pessoas em causa.

A comunicação da violação de dados pessoais deve ser feita ao titular dos dados o mais rápido possível. Os processadores de dados também devem notificar os controladores sobre as violações o mais breve possível.

Avaliação de Impacto sobre a Proteção de Dados e Consulta Prévia

O Regulamento orienta que quando um certo tipo de tratamento, em particular o que utiliza novas tecnologias, fica suscetível em alto risco aos direitos e às liberdades dos indivíduos, o responsável pelo tratamento deverá realizar uma Avaliação de Impacto de Proteção de Dados (DPIA) das operações previstas.

A Universidade de Coimbra apresenta os critérios e áreas sujeitas a DPIA, como por exemplo se um conjunto de operações de tratamento apresentar riscos elevados semelhantes, pode ser analisado em uma única avaliação. Ao efetuar uma avaliação de impacto sobre a proteção de dados, o responsável pelo tratamento solicitará o parecer do encarregado da proteção de dados, nos casos em que este tenha sido designado (UNIVERSIDADE DE COIMBRA, 2017).

2. CCPA *(California Consumer Privacy Act)*

Origem e Evolução do Direito à Privacidade

A globalização, popularização da internet e o surgimento de tecnologias como o aprendizado de máquina e a inteligência artificial trouxeram novas práticas de interação e socialização de dados.

Ao mesmo tempo usadas para suprir necessidades de integração e facilitar o relacionamento humano e as interações sociais, estas novas tecnologias aumentaram a criação, o processamento, armazenamento e compartilhamento de dados, trazendo novas ameaças ao universo digital.

Em sua obra, Desafios estratégicos para a segurança e defesa cibernética, Armando Junior (2020) observa que no cenário com grande variedade de redes, tecnologias e de infinitas perspectivas emerge uma faceta sempre presente nas relações humanas: o uso da internet como forma de obter recursos e vantagens de forma indevida ou ilícita.

> Nessas circunstâncias, em que coexistem ameaças e defesas, as diversas nações têm suas reações em busca da proteção de sua infraestrutura e de sua população. De forma natural, os Estados buscam resguardar seus interesses no espaço cibernético, não obstante ter o pensamento voltado para a Defesa Nacional e visão tática ou operacional, orientada para a Guerra Cibernética.

Diante deste cenário de transformação, foram necessárias novas abordagens sobre o tema privacidade de dados, proporcionando maior controle sobre o uso de suas informações pessoais.

A CCPA, sigla de California Consumer Privacy Act, ou Lei de Privacidade do Consumidor da Califórnia é uma lei de privacidade de dados que estabelece vários direitos para pessoas que residem no Estado da Califórnia, Estados Unidos, assegurando maior controle sobre as suas informações pessoais. A Lei tem aplicação extraterritorial, portanto, se a sua empresa faz negócios nesse Estado e trata dados de californianos, está sujeita às regras da CCPA.

A CCPA foi inspirada na GDPR para a proteção de dados e dos direitos à privacidade do consumidor na Califórnia, região onde está o Vale do Silício,

considerado o “berço” da inovação digital, local em que se concentram grandes empresas de alta tecnologia e dali surgiram nomes que se tornaram referência mundial em inovação tecnológica e avanços na internet, tais como Mark Elliot Zuckerberg (Facebook) e Steve Jobs (Apple).

No campo da regulação, a Califórnia também é conhecida por exercer influência sobre outros Estados, sendo pioneira na regulamentação da notificação de vazamento de dados – data *breach notification,* ou comunicação de incidente de segurança –, atualmente adotada por todos os 50 Estados dos Estados Unidos. Sancionada pelo Governo da Califórnia em junho de 2018, a CCPA entrou em vigor em janeiro de 2020 e é válida aos consumidores, às famílias e aos domicílios sediados apenas nesse Estado (DEPARTAMENTO DE JUSTIÇA DO ESTADO DA CALIFÓRNIA, 2018).

> A legislação da Califórnia classifica como residente no Estado qualquer pessoa física que esteja na Califórnia para outros fins que não sejam temporários ou transitórios; que tenha domicílio na Califórnia, mas que esteja fora do Estado para fins temporários ou transitórios.

Enquanto a legislação brasileira leva em consideração os dados anônimos, ou seja, de consumo ou estatísticos e que não permitem a identificação de seu titular, a Lei californiana define dado pessoal como toda informação que identifique, individualmente, uma pessoa ou família, residência/propriedade.

Pela Lei californiana, dados são todas as informações relacionadas a uma pessoa, ou seja, indivíduo identificável. Não há distinção entre as funções públicas, privadas ou corporativas de uma pessoa. Por isso, dados anônimos não são considerados pessoais.

Estão enquadrados na CCPA como dados pessoais: nome, endereço, número de passaporte, informação comercial (incluindo registros de produtos ou serviços adquiridos), informação biométrica e profissional, atividades na internet como histórico de navegação e pesquisa, identificadores on-line, endereços de *Internet Protocol* (IP), informações a respeito da interação do consumidor com um site, aplicativo ou anúncio e dados de geolocalização, caso possam vincular direta ou indiretamente a um determinado consumidor ou a uma família, detalhes

bancários/números de conta, número de contribuinte, números de cartão de crédito/débito e até postagens em mídia social.

Princípios Fundamentais da Proteção de Dados Pessoais

A CCPA é aplicada em todas as empresas do mundo com fins lucrativos que coletam dados pessoais dos consumidores residentes no Estado da Califórnia, nos seguintes casos:

- Se compram, vendem, compartilham para fins comerciais;
- Ou se a empresa excede, pelo menos, um dos seguintes limites:
    - Trata informações pessoais de mais de 50 mil residentes na Califórnia, incluindo casas ou dispositivos;
    - Possui 50% da receita anual com origem na venda de dados pessoais dos residentes;
    - Se tem receita bruta anual acima de US$ 25 milhões

Por ser uma lei executória, empresas e sites sofrem penalidade civil e aqui entra o conceito de dano presumido. Os consumidores da Califórnia podem entrar com uma ação civil para recuperar danos, se acreditarem que houve violação de seus dados por uma empresa.

Pelo descumprimento da legislação as empresas estão sujeitas a multas que variam de US$ 2.500 (violação) a US$ 7.500 (violação intencional), se a ofensa não for remediada em até 30 dias após o recebimento da notificação pela empresa infratora. A fiscalização é feita pelo advogado geral da Califórnia.

Já o pagamento da indenização ao consumidor é feito após uma ação judicial ser ajuizada, com o envolvimento do advogado geral.

Pela CCPA o consumidor/titular tem duas opções:

- Ajuizar uma ação cível perante o Poder Judiciário, pleiteando danos estatutários de 100 a US$ 750 por consumidor. Em tese, o consumidor não precisa comprovar que teve a perda concreta e é um caso muito parecido com o dano moral;
- Danos concretos, quando determinados dados não criptografados são alvos de acesso indevido, furto ou da disponibilização de medidas adequadas de

segurança. Se conseguir comprovar que isso provocou perdas financeiras definidas, o consumidor consegue solicitar tal indenização.

Nestes dois casos é necessário o consumidor fazer um aviso prévio de 30 dias à empresa infratora. Ou seja, deverá informar o ocorrido e a empresa tem este período para sanar a violação e se isto se concretizar, os danos estatutários não permanecerão disponíveis. Somente se neste prazo a empresa não conseguir sanar a violação é que o titular poderá solicitar, ao Poder Judiciário, a indenização.

As exceções às aplicações da CCPA são as organizações sem fins lucrativos, as instituições de seguros, setor público e agentes e organizações de apoio, que seguem o regulamento IIPPA, semelhante às regras da California Consumer Privacy Act (CALIFORNIA, 2018).

Ademais, as obrigações da legislação não podem restringir a capacidade de uma empresa que:

- Cumprir as leis federais, estaduais ou locais;
- Cumprir com uma investigação civil, criminal ou regulamentar, investigação, intimação ou intimação por autoridades federais, estaduais ou locais;
- Cooperar com as agências de aplicação da Lei em relação à conduta ou atividade que a empresa, o provedor de serviços ou terceiros, de maneira razoável e de boa-fé, acreditem que possam violar as leis federais, estaduais ou locais;
- Exercer ou defender ações judiciais;
- Coletar, usar, reter, vender ou divulgar informações do consumidor que foram desidentificadas do consumidor;
- Coletar ou vender informações pessoais de um consumidor se todos os aspectos dessa conduta comercial ocorrerem totalmente fora da Califórnia.

Direito dos Titulares e Dados Pessoais

A CCPA é uma regulamentação com foco no consumidor e confere alguns direitos aos titulares dos dados. Nos termos da Lei a empresa não precisa solicitar autorização para a venda dos dados, mas o cidadão tem o direito de concordar ou não com a venda de suas informações pessoais e a empresa não pode desacatar essa opção.

3. LGPD (Lei Geral de Proteção de Dados)

Origem e Evolução do Direito à Privacidade

O homem vive uma transformação social, econômica e cultural na qual a tecnologia tem papel de destaque. Com a globalização e o surgimento de novas tecnologias como a internet das coisas, o aprendizado de máquina e a inteligência artificial o interesse por dados vem crescendo exponencialmente no mundo todo, a ponto de os dados serem considerados o “novo petróleo”.

Com a popularização da internet e das redes sociais surgiram novas configurações de relacionamentos e de práticas de socialização de informações. Sempre que as pessoas “curtem” uma postagem no Facebook ou Instagram, por exemplo, demonstra as suas preferências por determinados temas ou assuntos.

Nos últimos anos surgiram novas práticas de coletas de informações pessoais. Com o aumento do compartilhamento de dados pessoais feito em transações como a aqui descrita – para a compra de seu livro – e até à comercialização não consensual houve apelo à privacidade e a exigência de regulamentação com normas e regras para a coleta e o tratamento dos dados pelas empresas.

A União Europeia deu início à proteção da privacidade on-line em 2012. Em 2016 aprovou o Regulamento Geral de Proteção de Dados (GDPR), apontado como o maior conjunto de proteção à privacidade on-line já criado desde o início da internet e que obrigou empresas de todo o mundo, inclusive gigantes como o Facebook e Google, a mudarem a forma como tratam os dados. Com a GDPR outros países deram início à criação de inéditas leis sobre este tema.

Nos Estados Unidos surgiu a California Consumer Privacy Act, ou Lei de Privacidade do Consumidor da Califórnia, e no Brasil a regulamentação veio com a Lei n.º 13.709, ou Lei Geral de Proteção de Dados (LGPD), aplicada a pessoas físicas e jurídicas, de direito público e privado, que façam tratamentos de dados pessoais, seja a coleta, o armazenamento, compartilhamento ou a exclusão (BRASIL, 2018).

Com a vigência da LGPD, muito tem se dito em privacidade digital, que em uma interpretação mais simplista, podemos dizer que a palavra se refere à vida privada, particular ou íntima de alguém, sendo o direito de se estar só e ficar isolado da sociedade. O conceito do direito à privacidade, porém, é mais profundo e teve origem na Antiguidade, quando era associado à vida cotidiana e estava relacionado

ao sentimento, algo que as pessoas aspiravam. Era limitado à classe burguesa ou de pessoas que moravam em lugares mais distantes do restante da comunidade.

No Brasil, o direito à privacidade é garantido desde 1988, pelo Artigo 5º, Inciso X, da Constituição da República Federativa do Brasil, que diz:

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

O direito à privacidade também é citado no Artigo 21 do Código Civil, que diz que: “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta Norma”.

No início da década de 2000, com o surgimento de redes sociais como Orkut e posteriormente Facebook, Twitter e Instagram, e de grandes marcas como Amazon, o que antes era feito presencialmente ou por telefone, passou a ser feito por e-mails, pela troca de mensagens e outras ferramentas digitais. Surgiu, então, o relacionamento baseado na internet, que trouxe novas oportunidades de negócios. Paralelamente surgiu uma nova matéria-prima: o dado.

É dessa época a promulgação do Marco Civil da Internet (Lei n.º 12.965/2014), que disciplina o uso da internet no Brasil e regula direitos e deveres dos internautas na navegação. Assim como a LGPD, tem como foco proteger os dados pessoais e a privacidade dos usuários.

Nos últimos anos a expressão privacidade digital é cada vez mais usual, mas que fique bem claro: privacidade e proteção de dados são questões diferentes.

> Por exemplo, se uma pessoa publicar um dado em sua página pessoal numa rede social, ele se torna público. Entretanto, isso não significa

> que este dado pode ser utilizado indiscriminadamente. Aquele que vier a utilizá-lo, deve respeitar os direitos do Titular do dado, previstos na LGPD. Tais dados, portanto, não estão sob a égide do princípio constitucional da privacidade, mas sim sob o escopo da proteção de dados. (IRAMINA, 2019)

A promulgação da LGPD modifica, altera e amplia os conceitos do Código Civil e do Marco Civil da Internet. A LGPD está centrada mais nas circunstâncias de tratamento dos dados fornecidos pelos usuários.

Princípios Fundamentais da Proteção de Dados Pessoais

O Artigo 6º da LGPD dispõe sobre os princípios fundamentais da proteção de dados de pessoais, mas antes de listá-los consideremos que a boa-fé no tratamento de dados pessoais é premissa básica. Ou seja, antes de se usar os dados de alguém, é preciso levantar questões como: “Qual é o objetivo deste tratamento?” “É preciso mesmo utilizar essa quantidade de dados?” “O cidadão com quem me relaciono deu o consentimento?” “O uso dos dados pode gerar alguma discriminação?”

Além da boa-fé, os princípios estabelecidos nesse artigo da LGPD são:

- Finalidade: especificada e informada explicitamente ao titular;
- Adequação à finalidade previamente acordada e divulgada;
- Necessidade do tratamento, limitado ao uso de dados essenciais para alcançar a finalidade inicial;
- Livre acesso: fácil e gratuito das pessoas à forma como os seus dados são tratados;
- Qualidade dos dados: deixando-os exatos e atualizados, segundo a real necessidade no tratamento;
- Transparência, ao titular, com informações claras e acessíveis sobre o tratamento e os seus responsáveis;
- Segurança para coibir situações acidentais ou ilícitas, tais como invasão, destruição, perda ou difusão;
- Prevenção contra danos ao titular e aos demais envolvidos;
- Não discriminação, ou seja, não permitir atos ilícitos ou abusivos;
- Responsabilização do agente, o qual obrigado a demonstrar a eficácia das medidas adotadas.

Direito dos Titulares e Dados Pessoais

A LGPD empoderou a pessoa física e impõe como principal objetivo proteger o direito de liberdade e privacidade do indivíduo, que agora tem assegurada a titularidade de seus dados pessoais. Sendo assim, qualquer pessoa física pode pedir para acessar os seus dados em uso por uma organização, a quem foram repassados e para qual finalidade (MATTOS, 2018).

É possível ainda pedir a eliminação ou correção destes dados, caso entenda que estão incompletos ou desatualizados, por exemplo.

A Lei apresenta princípios para garantir informações claras ao titular dos dados e imposição de limitações ao seu tratamento:

- A confirmação da existência de tratamento;
- O acesso aos dados mantidos pelo controlador que lhes diz respeito;
- A correção de dados incompletos, inexatos ou desatualizados;
- A anonimização, o bloqueio ou a eliminação de dados, desde que sejam considerados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
- A portabilidade de seus dados pessoais a outro fornecedor de serviço;
- A eliminação dos dados pessoais quando retirado o consentimento dado anteriormente;
- A relação de com quem os seus dados foram compartilhados;
- A informação de que poderá negar consentimento e quais as suas consequências;
- A revogação do consentimento.

Conclusão

O Regulamento Europeu de Proteção de Dados Pessoais foi o incentivo para outros países olharem mais atentamente para o assunto privacidade e proteção de dados pessoais e a investirem em legislações específicas.

Logo após a aprovação do Regulamento foi criada a CCPA – California Consumer Privacy Act, ou Lei de Privacidade do Consumidor da Califórnia –, aprovada em 2018 e com vigência a partir de janeiro de 2020, para suprir a necessidade de a Califórnia proteger melhor os seus residentes. Na sequência, em 18 de setembro, começou a vigorar a brasileira LGPD – Lei Geral de Proteção de Dados.

No Brasil, por força da Lei n.º 14.010/2020, as sanções entraram em vigor a partir de agosto de 2021, com punições que podem chegar a 2% do faturamento até o limite de 50 milhões de reais.

As três legislações têm diferenças conforme a particularidade de cada região, mas assemelham-se em um ponto principal: proteger os dados dos indivíduos, de modo que se baseiam em princípios de transparência e consentimento. A outra semelhança é a permissão ao usuário de revogar a concessão dos dados e a garantia de que possa atualizá-los quando bem entender.

No Brasil a ANPD cumprirá um papel educativo para conscientizar as organizações sobre a importância de proteger os dados dos indivíduos. Por isto, pela legislação, ao ser notificada pelas autoridades, a empresa será advertida e terá um prazo para adotar as medidas corretivas. Mas as sanções virão, de modo que as multas pelo descumprimento da legislação serão pesadas – por isto é importante as empresas se adequarem (GOV, 2020).

Conforme a LGPD, primeiramente virá a advertência, com indicação de prazo para a adoção de medidas corretivas. Depois serão aplicadas as outras sanções previstas no Artigo 52 da LGPD, a saber:

- Advertência, com indicação de prazo para adoção de medidas corretivas;
- Multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50 milhões de reais por infração;
- Multa diária, observado o limite total de R$ 50 milhões;

- Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- Eliminação dos dados pessoais a que se refere a infração.

Assim como ocorre na LGPD, o processo de *compliance* à GDPR, bem como a manutenção no cumprimento das regras são desafiadores para qualquer empresa.

Segundo levantamento realizado pela Sociedade Internacional de Advogados DLA Piper e citado no Jornal Econômico, as infrações ao Regulamento já originaram cerca de 272,5 milhões de euros em multas na Europa, nos últimos dois anos, e mais de 281 mil notificações aos reguladores nacionais (JORNAL ECONÔMICO, 2021)

Pelo Regulamento cada autoridade de controle pode aplicar as sanções em casos de descumprimento da Normativa, podendo gerar às empresas multas administrativas em diversas circunstâncias.

Quando dispõe sobre sanções, o Regulamento prevê a multa máxima a ser aplicada em uma organização não conforme: até 20 milhões de euros, no caso de uma empresa, ou até 4% de seu volume de negócios anual da receita global correspondente ao exercício financeiro anterior, consoante o montante mais elevado. A sanção para outros tipos de violação é a multa máxima de 2% da receita global anual, ou 10 milhões de euros, o que for maior.

A imposição dessas sanções é estabelecida pelos Estados-Membros, que são proporcionadas e dissuasivas, ou seja, as penalidades variam conforme a gravidade e duração da infração.

No que se refere às sanções, o GDPR dispõe sobre práticas mandatórias, tais como avaliação de impacto e registro dos processos e prevê as boas práticas voluntárias, como as que envolvem a adoção de códigos de conduta e de certificação como estratégias de autorregulação.

O relatório de impacto à proteção de dados pessoais deve ser feito pelo controlador quando o tratamento resultar em elevado risco para o direito e a liberdade das pessoas. Esta avaliação de impacto é obrigatória no caso de:

- Avaliação sistemática e completa dos aspectos pessoais relacionados a pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzam efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;
- Operações de tratamento em grande escala de categorias especiais de dados;
- Controle sistemático de zonas acessíveis ao público em grande escala.

O desafio de fazer valer a legislação nos países integrantes da União Europeia é vencido graças ao trabalho de cooperação entre as autoridades de proteção de dados (CONJUR, 2019). Pelo Regulamento a autoridade de controle principal coopera com as outras autoridades de controle, trocando entre si informações e podendo realizar operações conjuntas em casos de investigações, ou monitorizar a execução de medidas relativas a responsáveis pelo tratamento, ou subcontratantes estabelecidos nos Estados-Membros.

Referências Bibliográficas

BRASIL. Comitê Central de Governança de Dados. Guia de Boas Práticas – Lei Geral de Proteção de Dados (LGPD). 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia--lgpd.pdf Data de acesso: 29/11/2021

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm Data de acesso: 29/11/2021

CALIFORNIA. CCPA – California Consumer Privacy Act. 2018. Disponível em: http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 Data de acesso: 29/11/2021

COMISSÃO EUROPEIA. Um guia do cidadão para a proteção de dados na EU. 2019. Disponível em: https://ec.europa.eu/info/sites/default/files/gdpr2019-citizens_brochure-pt-v02.pdf Data de acesso: 29/11/2021

CONJUR. Um ano de GDPR: o que podemos aprender com os erros e acertos da Europa. 2019. Disponível em: https://www.conjur.com.br/2019-mai-31/opiniao-podemos-aprender-europa-ano-gdpr Data de acesso: 29/11/2021

COSTA, M. Os estágios da história da humanidade / o meio é a mensagem / aldeia global. 2011. Disponível em: https://aprendendoteoriadacomunicacao.blogspot.com/2011/05/marshall-mcluhan-os-estagios-da.html Data de acesso: 29/11/2021

DEPARTAMENTO DE JUSTIÇA DO ESTADO DA CALIFÓRNIA. Lei de Privacidade do Consumidor da Califórnia (CCPA). 2018. Disponível em: https://oag.ca.gov/privacy/ccpa#sectione Data de acesso: 29/11/2021

FGV. O maior vazamento de dados pessoais na história brasileira e quais lições devemos aprender. 2021. Disponível em: https://portal.fgv.br/artigos/maior-vazamento-dados-pessoais-historia-brasileira-e-quais-licoes-devemos-aprender Data de acesso: 29/11/2021

GOV. Guia de Boas Práticas segundo a Lei Geral de Proteção de Dados (LGPD). 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf Data de acesso: 29/11/2021

IRAMINA, A. RGPD V. LGPD: adoção estratégica da abordagem responsiva na elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. 2019. Disponível em: https://core.ac.uk/reader/337598120 Data de acesso: 29/11/2021

JÚNIOR, A. Desafios estratégicos para a segurança e defesa cibernética. [S.l.]: Contentus, 2020.

MARCONI, M. A; LAKATOS, E. M. Fundamentos da Metodologia Científica. São Paulo: Editora Atlas, 2003

MATTOS, F. Guia para a Lei Geral de Proteção de Dados. 2018. Disponível em: https://www.mattosfilho.com.br/EscritorioMidia/LGPD_MattosFilho.pdf Data de acesso: 29/11/2021

PARLAMENTO EUROPEU. Regulamento Geral sobre a Proteção de Dados (GDPR). 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=pt Data de acesso: 29/11/2021

SIMON, P. Too Big to Ignore: The Business Case for Big Data. 2013

UNIVERSIDADE DE COIMBRA. Avaliação de Impacto sobre a Proteção de Dados. 2017. Disponível em: https://www.uc.pt/protecao-de-dados/protecao_dados_pessoais/avaliacao_impacto_protecao_dados/avaliacao_impacto_protecao_dados Data de acesso: 29/11/2021

Referências Bibliográficas Complementares

BBC NEWS. Falta de privacidade mata mais que terrorismo: o surpreendente alerta de professora de Oxford. 2020. Disponível em: https://www.bbc.com/portuguese/geral-54558878 Data de acesso: 29/11/2021

BBC NEWS. “Não podemos salvar nossa privacidade, mas a democracia nunca precisou dela”, diz filósofo político Firmin DeBrabande. 2021. Disponível em: https://www.bbc.com/portuguese/geral-55238831 Data de acesso: 29/11/2021

BL CONSULTORIA DIGITAL. Série LGPD. 2020. Disponível em: https://blconsultoriadigital.com.br/category/lgpd/serie-lgpd Data de acesso: 29/11/2021

DOCUSIGN. GDPR: entenda o que é o Regulamento Geral de Proteção de Dados. 2018. Disponível em: https://www.docusign.com.br/blog/gdpr-entenda-o-que-e-o-regulamento-geral-de-protecao-de-dados Data de acesso: 29/11/2021

EL PAÍS. Facebook e Apple poderão ter o controle que a KGB nunca teve sobre os cidadãos. 2016. Disponível em: https://brasil.elpais.com/brasil/2016/10/27/internacional/1477578212_336319.html Data de acesso: 29/11/2021

EXIN PRIVACY E DATA PROTECTION. Privacidade, dados pessoais e GDPR. 2020. Disponível em: https://dam.exin.com/api/&request=asset.permadownload&id=3813&type=this&token=b919a584f9c26623c236268316de989f Data de acesso: 29/11/2021

G1. Reportagem do G1 “Entenda o caso de Edward Snowden, que revelou espionagem dos EUA”. 2013. Disponível em: http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html Data de acesso: 29/11/2021

IDWAL. LGPD Comentada. 2020. Disponível em: https://guialgpd.com.br/lgpd-comentada Data de acesso: 29/11/2021

JOTA REGULAÇÃO E NOVAS TECNOLOGIAS. California knows how to fine: o que sabemos até agora sobre o enforcement do CCPA? 2020. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/regulacao-e-novas-tecnologias/california-knows-how-to-fine-o-que-sabemos-ate-agora-sobre-o--enforcement-do-ccpa-15082020 Data de acesso: 29/11/2021

JORNAL ECONÔMICO. Regulamento da proteção de dados gerou mais de 272 milhões de euros em multas na Europa. Jornal Econômico. 2021. Disponível em: https://jornaleconomico.sapo.pt/noticias/regulamento-da-protecao-de-dados-gerou-mais-de-272-milhoes-de-euros-em--multas-na-europa-694111 Data de acesso: 29/11/2021

MINUTO DA SEGURANÇA. GDPR – 101 controles básicos para a conformidade. 2018. Disponível em: https://minutodaseguranca.blog.br/gdpr-101-controles-basicos-para-a-conformidade/ Data de acesso: 29/11/2021

VIOLA, M. 2019. Transferência de dados entre Europa e Brasil: análise da adequação da legislação brasileira. Disponível em: https://itsrio.org/wp-content/uploads/2019/12/Relatorio_UK_Azul_INTERACTIVE_Justificado.pdf Data de acesso: 29/11/2021

YOUTUBE. Privacidade e Proteção de Dados no Brasil | Carlos Affonso Souza | TEDxPetrópolis. Disponível em: https://youtu.be/Zau-x-j_Uu8 Data de acesso: 29/11/2021

YOUTUBE. Proteção de dados no mundo (GDPR, CCPA e outras legislações), da Nextlaw Academy. Disponível em: https://youtu.be/FnFcF9jWfNw Data de acesso: 29/11/2021