**UNIVERSIDADE ESTADUAL DA PARAÍBA**
**CAMPUS I – CAMPINA GRANDE**
**CENTRO DE CIÊNCIAS JURÍDICAS**
**CURSO DE DIREITO**

**JÚLIO CÉSAR DE ARAÚJO SOUZA FAUSTINO**

# ANÁLISE DOS PROJETOS DE LEI SOBRE PROTEÇÃO DOS DADOS PESSOAIS NO BRASIL À LUZ DO REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA

**CAMPINA GRANDE-PB**
**2018**

**JÚLIO CÉSAR DE ARAÚJO SOUZA FAUSTINO**

# ANÁLISE DOS PROJETOS DE LEI SOBRE PROTEÇÃO DOS DADOS PESSOAIS NO BRASIL À LUZ DO REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de bacharel em Direito.

**Orientador:** Prof. Me. Antônio Silveira Neto.

**CAMPINA GRANDE-PB**
**2018**

F251a Faustino, Julio Cesar de a S.

Análise dos projetos de Lei sobre proteção dos dados pessoais no Brasil à luz do regulamento geral sobre a proteção de dados da União Europeia [manuscrito] : / Julio Cesar de a S Faustino. - 2018.

30 p.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Estadual da Paraíba, Centro de Ciências Jurídicas , 2018.

"Orientação : Prof. Me. Antônio Silveira Neto , Departamento de Direito Privado - CCJ."

1. Privacidade de Usuários na Internet. 2. Proteção de Dados Pessoais. 3. Projeto de Lei.

21. ed. CDD 344.01

**JÚLIO CÉSAR DE ARAÚJO SOUZA FAUSTINO**

# ANÁLISE DOS PROJETOS DE LEI SOBRE PROTEÇÃO DOS DADOS PESSOAIS NO BRASIL À LUZ DO REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de bacharel em Direito.

Aprovado em: 18/06/2018.

**BANCA EXAMINADORA**

Prof. Me. Antônio Silveira Neto (Orientador)
Universidade Estadual da Paraíba (UEPB)

Prof. Me. Amilton de França
Universidade Estadual da Paraíba (UEPB)

Prof. Me. José Cavalcanti dos Santos
Universidade Estadual da Paraíba (UEPB)

Dedico este trabalho ao meu pai e à minha mãe,
pelo apoio incondicional e amor sem fim.

## AGRADECIMENTOS

Aos meus queridos pais, Djacir e Da Guia, pelo exemplo de vida e dedicação à família. Por nunca terem medido esforços para me proporcionar a melhor educação possível.

Aos meus irmãos, Marcos e Pablo, pelo zelo, companheirismo e por sempre me incentivarem nos estudos.

Ao meu amor, Gisele, com quem compartilho minha vida, pelo carinho, compreensão e por ter me ajudado nos momentos que precisei.

Aos bons amigos que conquistei ao longo dessa jornada, Ramon Bahia e Juvêncio Amaral, pela convivência fraterna, por estarem sempre dispostos a me ajudar, pelas conversas descontraídas. A nossa amizade é para sempre.

Ao meu professor orientador, Antônio Silveira Neto, pela atenção, paciência, supervisão e leituras sugeridas ao longo da orientação.

Ao professor Amilton e ao professor Cavalcanti por terem aceitado participar da banca examinadora desse trabalho.

Aos demais professores e funcionários da UEPB que contribuíram na minha formação e se empenham todos os dias por uma universidade melhor.

*O ciberespaço, há não muito tempo atrás, era um espaço determinado, que nós visitávamos periodicamente, mergulhando nele a partir do nosso mundo físico. Hoje, o ciberespaço saltou para fora. Colonizou o físico.*

*William Gibson*

*Não cometa o erro de achar que você é o cliente do Facebook, você não é - você é o produto. Os seus clientes são os seus anunciantes.*

*Bruce Schneier*

**SUMÁRIO**

# ANÁLISE DOS PROJETOS DE LEI SOBRE PROTEÇÃO DOS DADOS PESSOAIS NO BRASIL À LUZ DO REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA

Júlio César de Araújo Souza Faustino[1]

## RESUMO

O presente artigo aborda o tema da proteção dos dados pessoais no Brasil haja vista o ordenamento jurídico nacional não dispor de uma lei geral que trate da proteção à privacidade dos usuários na internet. A capacidade de processamento de dados em crescente expansão pela rede de computadores configura ameaça aos direitos fundamentais da privacidade e intimidade, pela coleta e tratamento indevido dos dados pessoais tanto pelo Poder Público quanto pelas empresas privadas. O estudo analisa as principais iniciativas legislativas em discussão no Congresso Nacional com o objetivo de aprovar um regulamento geral de proteção dos dados pessoais. O método escolhido foi o indutivo amparado em pesquisa bibliográfica através de doutrinas jurídicas, artigos publicados, bem como a legislação vigente. O artigo reitera a necessidade de aprovação de norma específica a exemplo do Regulamento da União Europeia (GDPR) para consolidar o arcabouço jurídico do país na tutela de proteção aos dados pessoais.

**Palavras-Chave**: Privacidade. Internet. Proteção de dados pessoais. Projeto de lei.

## 1 INTRODUÇÃO

A proteção dos dados pessoais está na pauta do dia, a crescente evolução tecnológica dos meios de comunicação dinamizou a vida cotidiana da sociedade que se encontra cada vez mais inserida na constituição do ciberespaço. O mundo digital rompeu o paradigma das fronteiras físicas com o aumento expressivo dos fluxos de dados pessoais, transmitidos pelos usuários na *web*, estreitando as relações em níveis sociais, culturais e econômicos. As entidades públicas e sobretudo as empresas privadas armazenam e gerenciam quantidades enormes de dados pessoais para desenvolver seus serviços, ao encará-los como uma mercadoria de grande valor econômico.

Nesse contexto é evidente o surgimento de novos desafios no tocante à tutela dos dados pessoais, sendo o direito à privacidade, o mais atingido. A problematização advinda nesse cenário é como promover as garantias constitucionais do direito à privacidade e a intimidade em relação aos dados pessoais no Brasil no âmbito da rede mundial de computadores?

[1] Aluno de Graduação em Direito na Universidade Estadual da Paraíba - Campus I.
E-mail: juliocesarfaust@hotmail.com

O presente estudo tem como escopo a análise das principais iniciativas legislativas em tramitação no Congresso Nacional sobre a proteção dos dados pessoais no âmbito da *Internet*, com a finalidade de aprovar uma lei geral de proteção e tratamento dos dados pessoais coletados no Brasil inspirada nas Diretivas da União Europeia.

Como é notório pela simples análise do tema, o Brasil em pleno ano de 2018, está atrasado por ainda não possuir legislação específica que trate da proteção dos dados pessoais, deixando os cidadãos brasileiros fragilizados em relação a dinâmica da era digital, apesar da Constituição Federal tutelar o direito à privacidade, por se tratar de um direito fundamental, bem como o Código de Defesa do Consumidor e o Marco Civil. Contudo é essencial a criação de uma lei para que se possa potencializar a proteção dos usuários brasileiros dos meios digitais, assim como evitar problemas de limitação na realização do compartilhamento de dados de segurança e nas transações comerciais que envolvam o Brasil com Estados com leis de proteção de dados pessoais mais avançadas.

Países integrantes do Mercosul, a exemplo da Argentina e do Peru, respectivamente em 2000 e 2011, já sancionaram normas específicas versando sobre o assunto, o que demonstra a falta de iniciativa do legislativo nacional para a aprovação de um regulamento sobre o tema objeto. (SILVA, 2010)

Com tudo, um importantíssimo passo para a criação de uma regulação geral sobre a proteção de dados pessoais no Brasil foi dado recentemente no dia 29 de maio de 2018. A aprovação pelo Plenário da Câmara dos Deputados do PL nº 4.060/2012, do deputado Milton Monti PR-SP que, desde 2012, tramitava na Câmara. O texto prevê o tratamento de dados pessoais no país, tanto pelo poder público quanto pela iniciativa privada. A matéria foi aprovada por unanimidade e encaminhada ao Senado. O mencionado projeto de lei será abordado em momento posterior nesse estudo.

Vale ressaltar que na mesma semana em que foi aprovado o PL 4.060/2002 pela Câmara, estava em pauta em caráter de urgência no Senado, a votação do PLS 330/2013 do Senador Antônio Carlos Valadares (PSB-SE), que trata do mesmo tema de proteção à privacidade na rede, configurando dessa forma uma certa disputa entre as Casas para definição da autoria da criação da lei geral de proteção de dados pessoais no Brasil. O impulso dado as mencionadas propostas de lei pelo Congresso Nacional se relacionam ao contexto de grande relevância no cenário mundial com a entrada do novo (GDPR)[2], na sigla em inglês, o Regulamento Geral de Proteção de Dados Pessoais na União Europeia, que passou a vigorar no último dia 25 do mês

[2] General Data Protection Regulation (EU) 2016/679.

de maio e o mais recente caso de violação de dados pessoais que foi revelado ao mundo no início do ano de 2018, envolvendo a maior rede social do planeta, o Facebook, e a empresa de marketing digital, Cambridge Analytica. Diante de tais fatos, evidenciam-se cada vez mais a importância da criação de uma política de proteção e tratamento de dados pessoais no Brasil.

Para elaboração do presente artigo foi adotado o método indutivo, assim como a técnica de investigação bibliográfica que se amparou na análise sistematizada de doutrinas jurídicas, artigos publicados na internet, bem como a legislação vigente.

## 2 DADOS PESSOAIS

Antes de se debruçar na temática dos desafios jurídicos de proteção ao direito constitucional da privacidade nos domínios digitais, faz-se necessário antecipar a conceituação de alguns termos específicos inerentes ao estudo dos dados pessoais.

Sendo assim, Sawaya (1999), explica que o termo *dado* se refere a números, letras, símbolos, bem como fatos que fazem referência ao descrever um objeto determinável, ideia, condição, situação ou demais fatores. No tocante a informática, são os elementos básicos fornecidos, processados ou elaborados por equipamento.

Destarte, os dados podem ser: anônimos, pessoais, cadastrais e sensíveis.

Os dados anônimos são entendidos como "dados pessoais relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento"[3] (BRASIL, 2018, p. 4).

Já os dados pessoais são acumulações de fatos e eventos que moldam a personalidade da pessoa, podendo contar precisamente a história de cada indivíduo. No passado essas informações eram constituídas através de cartas, telegramas, fotos. Nos dias atuais, através de e-mail, redes sociais. O Decreto nº 8.771/16, que regulamentou o Marco Civil, no Art. 14, I, define dados pessoais como "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa" (BRASIL, 2016).

Ainda no Decreto nº 8.771/16, temos o entendimento por dados cadastrais a filiação, o endereço e sua qualificação pessoal, através do seu nome, prenome, estado civil e profissão do usuário. (BRASIL, 2016).

[3] PLC 53/2018, art. 5º, inciso III.

Dados sensíveis são entendidos como "dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural"[4] (BRASIL, 2018, p. 4).

Nesta senda, o texto do Projeto de Lei aprovado pela Câmara dos Deputados, PL nº 4.060/2012, sobre novo número no Senado, PLC nº 53/2018, conceitua com especificidade no Art. 5º demais termos importantes, como a figura do titular a quem se refere os dados pessoais; o entendimento de banco de dados, como se vê:

> Art. 5º Para os fins desta Lei, considera-se:
> ...
> IV - banco de dados: conjunto estruturado de dados pessoais, localizado em um ou em vários locais, em suporte eletrônico ou físico;
> V - titular: a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - responsável: a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do responsável;
> VIII - encarregado: pessoa natural, indicada pelo responsável, que atua como canal de comunicação entre o responsável e os titulares e o órgão competente;
> IX - agentes do tratamento: o responsável e o operador;
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; [...] (BRASIL, 2018, p. 3-4)

Como exposto, em relação a conceituação dos termos referente aos dados pessoais, o PLC nº 53/2018 claramente se baseou no Regulamento 679/2016 da União Europeia, com redação muito próxima, tratando com clareza a definição de seus pontos. O texto do Projeto de Lei será melhor abordado neste estudo em momento oportuno.

# 3 PRIVACIDADE E ACESSO A INFORMAÇÃO NO BRASIL NO CONTEXTO DA INTERNET

## 3.1 A PRIVACIDADE

[4] PLC 53/2018, art. 5º, inciso II.

A legislação existente no Brasil sobre a Internet ainda é recente e pouco desenvolvida, o que acarreta no cenário atual dificuldades para garantir ao cidadão que utiliza o serviço, a proteção de sua privacidade na rede. Segundo Pinheiro (2013), o direto a privacidade no país não está desprotegido, o que falta são as leis vigentes serem interpretadas de forma coerente aos novos fatos, se adequando ao caso concreto.

Hoje em dia, o acesso à Internet se tornou quase que indispensável no Brasil, bem como no mundo. As pessoas, principalmente as que vivem nos grandes centros, se condicionaram e passaram a depender do seu uso. Pinheiro (2013) entende que as pessoas que utilizam a rede não estariam dispostas a deixar de usá-la gratuitamente em troca de seus dados, logo quem conseguir chefiar a tutela da privacidade sustentável, conquistará o mercado, mas antes disso devem cuidar do conteúdo das políticas de privacidades já implementadas.

Para muitos é inconcebível a ideia de deixarem de utilizar à Internet, devido aos benefícios e múltiplas aplicações oferecidas na vida cotidiana, mesmo tendo ciência da possiblidade de ofensas no tratamento de seus dados, aceitam políticas de privacidade elaboradas com diversos abusos para estarem conectadas a rede. Por tamanha relevância, no ano de 2016, a ONU (Organização das Nações Unidas) propôs reconhecer o acesso à internet como um direito do ser humano, reconhecendo a importância deste recurso em todo o planeta.

A Constituição Federal de 1988 apesar de não apresentar preceito específico sobre a privacidade, positiva diversos preceitos fundamentais no seu art. 5º, como o direito à vida, à intimidade, à vida privada, à imagem, o direito de resposta, entre outros. (BRASIL, 1988). Logo, desde a Constituição se garante o direito a individualidade e a proteção da privacidade.

Doneda (2006) afirma que a privacidade é um direito fundamental tutelado pela Constituição, ao ter como ideal máximo do ordenamento jurídico a proteção da pessoa humana. A tecnologia somada as mudanças sociais trouxeram um novo panorama no qual a informação pessoal e privacidade se entrelaçam, onde a segunda passa a estruturar a primeira, notadamente sobre os dados pessoais.

Nesse contexto de intensa evolução digital, a informação converte-se numa riqueza de extremo valor econômico para a sociedade, o usuário da rede tem seus dados coletados e armazenados diariamente em bancos de dados gerenciados pelas empresas, que ao tratarem esses dados podem exportar aspectos da personalidade, comportamentos, preferências, hábitos de cada usuário, e assim, gerar perfis de consumo, que são essenciais para a dinâmica do comércio na *Internet*. Desta forma, cabe a lei a tutela de proteção ao direito fundamental da intimidade dos usuários contra práticas abusivas que não ocasionalmente, são empreendidas pelas empresas através do uso das novas tecnologias ao coletar dados pessoais na maioria das

vezes sem o consentimento, configurando tal prática lesão a intimidade e a privacidade do usuário.

Gonçalves (2003, p. 82) afirma que:

> A utilização das novas tecnologias expande as possibilidades de recolha, tratamento e circulação de informação, virtualmente sem limites de tempo e de espaço. Confrontam-se, aqui, por um lado, o interesse do indivíduo na proteção das informações que lhe dizem respeito e, por outro, o interesse de entidades públicas ou privadas na eficiência das suas atividades. A informatização empola o grau de risco para o indivíduo na medida em que a interconexão de ficheiros e de bases de dados permite reunir informação diversa que poderá ser utilizada de modo abusivo, seja pelos poderes públicos, com intuitos repressivos, restritivos da liberdade dos cidadãos, seja por entidades privadas com fins discriminatórios (por exemplo, no recrutamento para determinados empregos) ou de mero enriquecimento (caso da venda de listas de nomes para fins de mala directa). Estas práticas podem funcionar, indirectamente, como condicionantes do próprio comportamento individual.

Nesta lógica, o cruzamento de dados nos diferentes bancos de dados, através do tratamento feito pelas empresas permite identificar com precisão cada indivíduo conectado na rede. Um banco de dados que retêm dado sensível sobre a saúde, a orientação sexual ou religiosa, que passa essa informação a uma determinada empresa pode gerar desigualdades.

Limberger (2009, p. 43) fala que "[...] um portador do vírus HIV pode não ser contratado em virtude da doença ou ser despedido. A possibilidade de a empresa escolher um trabalhador sadio, no momento da contratação, é muito grande, o que caracterizaria uma discriminação". Daí surge a necessidade de proteger juridicamente os dados pessoais, para prevenir situações discriminatórias, eliminar desigualdades, para que os dados armazenados não sejam utilizados indevidamente para prejudicar os cidadãos.

Por fim, há de se tratar, todavia, em face da proteção dos dados advindo do direito da autodeterminação informativa, que o doutrinador Mota Pinto (2000, p. 164) conceitua:

> A autodeterminação informativa é entendida como controlo sobre informação relativa à pessoa. Consiste no interesse em impedir ou em controlar a tomada de conhecimento, a divulgação ou, simplesmente, a circulação de *informação* sobre a pessoa, isto é, sobre factos, comunicações ou situações relativo (ou próximos) ao indivíduo, e que previsivelmente ele considere como íntimos, confidenciais ou reservados.

Logo, compreendido como o direito de controlar as próprias informações. Surgiu na Alemanha através do entendimento jurisprudencial de 25/12/83 do Tribunal Constitucional que anulou parcialmente a Lei de Censo da população de 1982 devido a possibilidade dos dados coletados no censo não serem apenas utilizados, pelo governo para fins estatísticos, mas também administrativos, com a eventualidade de retificação do registro civil, caracterizando a diversidade de finalidades, desta forma tornando difícil para os cidadãos alemães o

reconhecimento real do que seria feito a partir das informações coletas. Assim configurando uma das motivações da decisão que reconheceu o princípio da finalidade na coleta dos dados. Limberger (2009, p. 36) afirma que "o Tribunal extrai do direito fundamental do livre desenvolvimento da personalidade a faculdade de cada indivíduo de dispor principalmente sobre a revelação e o uso de seus dados pessoais".

Por conseguinte, Doneda (2006) em mesmo sentido afirma que, a autodeterminação informativa é direito fundamental, integrante dos direitos da personalidade, que confere ao indivíduo o controle sobre suas informações. Na tradição democrática alemã é vista como afirmação do personalismo, no entanto, associado com a dimensão da inserção social de cada indivíduo. Logo, os direitos fundamentais não são conferidos aos cidadãos somente para sua livre disposição, como também na situação de membro da comunidade e no interesse público.

## 3.2 O ACESSO À INFORMAÇÃO

A Constituição Federal de 1988 preconizou no art. 5º, inciso XXXIII, o direito de todo brasileiro à informação, mas ainda não havia uma lei especificando o acesso. (BRASIL, 1988). Em 2005 foi aprovada uma lei que garante o sigilo da maioria dos documentos e os mantêm restritos por segurança. Em 2011, o projeto de lei que regulamenta a obrigatoriedade de órgãos públicos divulgarem todas as informações de interesse nacional foi aprovado no Congresso.

> As políticas de informação adquirem uma nova dimensão entre as políticas públicas (governos de diferentes países passaram a reorientar suas estratégias com relação ao desenvolvimento da área de informação), implicando em simultâneo a redefinição de seu escopo e abrangência. (JARDIM; SILVA; NHARRELUGA, 2009, p. 8)

A Lei de Acesso a Informação é um direito de todos perante a constituição brasileira. Isso é importante para a sociedade, do qual tem direito de saber as atuações dos governos e do poder público, seja por controle social, seja por transparência na gestão do governo, ou até mesmo para inibir possíveis corrupções.

Essa lei é polêmica, pois ao mesmo tempo em que regulamenta o acesso à informação, cria uma série de arestas relativas à privacidade e ao direito individual. É preciso conciliar o direito à preservação da privacidade, a proteção dos dados pessoais dos funcionários públicos e de uma forma mais ampla a proteção dos dados pessoais de toda a população frente ao crescente tratamento automatizado dos dados pessoais e profissionais e a facilidade do seu acesso, inclusive para utilizações não autorizadas.

## 3.3 A PRIVACIDADE SOB À ÓTICA DO CÓDIGO DE DEFESA DO CONSUMIDOR E DO MARCO CIVIL DA INTERNET

Aspectos importantes sobre a proteção de dados de usuários na internet quanto aos provedores de conexão e de aplicações são garantidos pela Lei nº: 8.078/1990, o Código de Defesa do Consumidor (CDC).

O CDC é de grande aplicação prática na tutela ao consumidor, apesar de, em uma visão inicial, não abarcar todas as situações passíveis de proteção para o consumidor informacional, como a simples navegação, ou outras situações que possam não se enquadrar como de consumo, como a utilização de sites governamentais, por exemplo. Segundo Vancim e Matioli (2014), o campo de atuação do CDC é amplo, pois inclui em seu espectro protetivo, com o propósito de equilibrar as relações consumeristas, não somente os interesses individuais, mas também os individuais homogêneos, os difusos e os coletivos.

Com tudo, a Lei nº 12.965/2014, o chamado Marco Civil da Internet, é mais recente que o CDC e foi recentemente regulamentada pelo Decreto 8.771, de 11 de maio de 2016. O Marco Civil estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. É fundamentado na liberdade de expressão e privacidade, finalidade social, livre inciativa e direitos do consumidor (BRASIL, 2014). A liberdade de expressão é fundamento e princípio privilegiado na referida norma, mas ela também contempla expressamente, em seu Art. 3º, incisos II e III, a privacidade e a proteção de dados, respectivamente. O Marco Civil apresenta disposições específicas quanto à neutralidade da rede, à proteção de registros de dados pessoais de conexão e de acesso às aplicações na internet, à atuação do poder público, à responsabilidade por danos, a respeito de requisição judicial, sobre mecanismos de governança, interoperabilidade e acessibilidade, entre outros.

Conforme Teixeira (2014), além de ser uma lei principiológica, o Marco Civil estabelece regras específicas a serem cumpridas por provedores de acesso, provedores de conteúdo e outros agentes, mas não são tratados em seu texto temas importantes como comércio eletrônico, crimes de informática, propriedade intelectual, aspectos tributários ou spam, bem como não pode ser considerada uma lei de proteção de dados, por não abordar o assunto na extensão e especificidade necessárias.

# 4 CASO CAMBRIDGE ANALYTICA E O FACEBOOK

Um caso ocorrido no início do ano chamou atenção do mundo em relação ao vazamento de dados pessoais que envolveu a maior rede social do planeta, o Facebook, com a empresa

digital Cambridge Analytica. Um vazamento de dados de 87 milhões de usuários do Facebook, para uso político, o que acarretou a queda do valor da empresa e a colocou na mira das autoridades. Os dados dos usuários do Facebook foram utilizados sem o consentimento deles pela empresa britânica Cambridge Analytica para fazer propaganda política direcionada.

A empresa teria coletado os dados pessoais dos usuários ao lançar um aplicativo de teste psicológico na rede social. Aqueles usuários do Facebook que participaram do teste acabaram por entregar à Cambridge Analytica não apenas suas informações, mas os dados referentes a todos os amigos do perfil na rede social.

## 4.1 A REDE SOCIAL FACEBOOK

O Facebook, fundado em quatro de fevereiro de 2004, foi criado por Mark Zuckerberg em conjunto com mais três colegas de quarto de faculdade, Dustin Moskovitz, Chris Hughes e o brasileiro Eduardo Saverin. A criação da rede tinha o objetivo de aproximar os estudantes e os estimularem a postar fotos e a fazer novas amizades. Inicialmente, o nome do site foi intitulado de *thefacebook.com* e se tornou uma febre entre os usuários. Restrita aos alunos da Universidade de Harvard, os criadores decidiram expandir o acesso para os estudantes de Stanford, Columbia e Yale, em março do mesmo ano.

Segundo Recuero (2009, p. 171), "o foco inicial do Facebook era criar uma rede de contatos" em um momento que representava mudanças para muitos estudantes, que saiam da escola para a universidade. A autora explica que nos Estados Unidos este momento se associa não só a um novo ambiente educacional, mas, muitas vezes, a mudança de cidade.

Portanto, o Facebook é uma plataforma que oferece as pessoas se conectarem através de seu sistema criando perfis pessoais. O serviço é gratuito e a empresa gera receita por meio das propagandas divulgadas no site.

## 4.2 CAMBRIDGE ANALYTICA

Uma empresa de análise de dados que trabalhou com o time responsável para a campanha eleitoral do atual presidente republicano, Donald Trump, nas eleições de 2016 nos Estados Unidos. A empresa é em parte propriedade do bilionário do mercado financeiro Roberto Mercer e era presidida, à época, por Steve Bannon, principal assessor de Trump.

A Cambridge teria comprado acesso a informações pessoais de usuários do Facebook e usado esses dados para criar um sistema que permitiu predizer e influenciar as escolhas dos

eleitores nas urnas, segundo a investigação do jornal britânico *The Guardian* e do estadunidense, *The New York Times*.

O esquema começou em 2014, dois anos antes da eleição americana de 2016 e funcionava da seguinte maneira: as informações dos usuários do Facebook foram coletadas por um aplicativo chamado *thisisyourdigitallife*[5], que pagou a centenas de milhares de usuários pequenas quantias para que eles fizessem um teste de personalidade e concordassem em ter seus dados coletados para uso acadêmico.

O aplicativo foi desenvolvido por Aleksandr Kogan, pesquisador da Universidade de Cambridge, no Reino Unido. Ele já tinha uma pesquisa sobre como deduzir a personalidade e as inclinações políticas das pessoas a partir de seus perfis no Facebook. A Cambridge Analytica, que não tem relação nenhuma com a Universidade de Cambridge, teria comprado os dados coletados por ele.

Além da óbvia questão de que muitos usuários não leem os longos termos e condições e mal sabem que estão dando suas informações para os desenvolvedores desses testes, o grande problema foi que o aplicativo também coletou os dados de amigos das pessoas que fizeram o teste. Ou seja, se uma pessoa respondesse o quiz, estaria entregando informações privadas não apenas do seu perfil, mas de todos os seus amigos. Milhões de informações de pessoas que não deram seu consentimento tiveram seus dados manipulados para fins políticos.

Os dados teriam sido usados para catalogar o perfil das pessoas e, então, direcionar de forma mais personalizada matérias pró-Trump e mensagens contrárias à adversária dele, a democrata Hillary Clinton.

Por conseguinte, no mês de maio, a Cambridge Analytica, declarou que dará início ao processo de falência[6] no Reino Unido e o fim de suas atividades devido as intensas investigações, a perda da maioria de seus clientes, bem como o pagamento dos altos custos dos processos em decorrência dos fatos, tornando inviável a continuação de suas atividades.

## 5 COMENTÁRIOS AOS PROJETOS DE LEI EM TRAMITAÇÃO NO CONGRESSO NACIONAL

Esta etapa do estudo tem por objetivo analisar as principais iniciativas legislativas em tramitação no Congresso Nacional para a aprovação de uma tão aguardada lei geral de proteção

[5] Na tradução, essa é sua vida digital.

[6] SALOMÃO, Karin. Cambridge Analytica irá fechar depois de escândalo com Facebook. **EXAME**, São Paulo, 2 maio 2018. Disponível em: <https://exame.abril.com.br/negocios/ cambridge-analytica-ira-fechar-depois-de-escandalo-com-facebook/>. Acesso em: 6 jun. 2018.

de dados para o país, tendo em vista que no cenário muito próximo ao Brasil, a Argentina, Peru e Uruguai, como já comentado, possuem dispositivos específicos que regulam a questão da proteção das informações pessoais, notadamente na *Internet* (SILVA, 2010).

No período anterior a promulgação do Marco Civil da Internet, e após a sua regulamentação, já no ano de 2016, foram diversos os diplomas apresentados ao Congresso com o objetivo de regular de forma coerente e sistematizada a atividade do tratamento de dados pessoais (TEIXEIRA, 2014). Muitas dessas proposituras já foram arquivadas, a pesquisa focará no cenário atual, considerando os projetos mais significativos:

- Projeto de Lei nº 4.060/2012 (BRASIL, 13 jun. 2012), do Deputado Milton Monti, dispõe sobre dados pessoais de forma abrangente, o texto original não abordou quase nenhum dos principais pontos que um protejo do segmento de proteção de dados deve abordar. Era mais voltado para à livre iniciativa e manutenção da autorregulação das empresas privadas e descentralização de responsabilidade em outros órgãos, não mencionando a criação de órgão especifico. Apresentado em 13 de junho de 2012.
- Projeto de Lei n° 330/2013 (BRASIL, 2013), do Senador Antônio Carlos Valadares, dispõe sobre a proteção, o tratamento e o uso dos dados pessoais; é bastante completo e é um dos importantes projetos atualmente no Senado que trata sobre proteção de dados. Foi apresentado em 13 de agosto de 2013.
- Projeto de Lei n° 181/2014 (BRASIL, 2014 [a]), do Senador Vital do Rêgo, estabelece princípios, garantias, direitos e obrigações para a proteção de dados pessoais no Brasil; elenca os direitos do titular; determina o regime jurídico do tratamento de dados pessoais; estabelece regras para a tutela administrativa dos dados pessoais. Apresentado em 20 de maio de 2014, em tramitação no Senado.
- Projeto de Lei n° 131/2014 (BRASIL, 2014 [b]), da CPI da Espionagem do Senado Federal, dispõe sobre o fornecimento de dados de cidadãos ou empresas brasileiras a organismos estrangeiros. Foi apresentado em 16 de abril de 2014, encontrando-se em tramitação no Senado.
- Projeto de Lei nº 5.276/2016 (BRASIL, 13 maio 2016), de autoria do Poder Executivo, foi baseado em anteprojeto realizado pelo Ministério da Justiça. Teve lançada consulta pública para discussão em 28 de janeiro de 2015. De todos os textos apresentas se mostrou o mais robusto, menciona tanto dados pessoais, anônimos e sensíveis, o consentimento, criando a figura de um órgão regulador responsável pela fiscalização de tratamento de dados. Este projeto foi apresentado em 13 de maio de 2016.

Dos textos apresentados no Congresso, o elaborado pelo Ministério da Justiça, a partir das discussões e contribuições populares que compuseram o anteprojeto, foi o mais completo até agora, em relação a criação de medidas protetivas para os dados pessoais e a privacidade dos usuários.

Vale salientar que quando da apresentação do anteprojeto à Câmara, tornando-se o PL 5.276/2016, apresentou diferenças em relação ao texto que constava na *Internet*, havendo retrocesso no que diz respeito a temática do consentimento, diretamente relacionado a autodeterminação informativa do usuário.

Como já salientado no início deste artigo, neste ano de 2018 a Câmara dos Deputados aprovou por unanimidade o PL nº 4.060/2012[7] de autoria do deputado Milton Monti PR-SP, que tramitava há seis anos na Câmara, no dia 29 de maio. Sob condução do deputado Orlando Silva PT-SP que apresentou novo texto com grandes contribuições do PL 5.276/2016 que também tramitava na Câmara. Em decorrência disso, o referido Projeto de Lei foi arquivado pela Câmara e o novo PL nº 4.060/2012 foi encaminhado para o Senado. Ao chegar no Senado, já neste mês de junho, recebeu nova numeração, agora como PLC 53/2018 e teve o PLS 330/2013 apensado[8] ao seu texto. A matéria segue em análise no Senado.

Desta forma, o estudo se focará na análise do texto do PLC 53/2018 elencando suas principais disposições. O Projeto conta com 65 artigos e está dividido em dez capítulos.

No Capítulo I, referente às Disposições Preliminares, apresenta no Art. 1º seu objeto, a proteção de direitos fundamentais em relação aos dados pessoais, e são enunciados em seu Art. 2º os seus fundamentos. O Art. 3º especifica o escopo do tratamento de dados a que se destina, ao se referir ao tratamento de dados no território nacional. Deixa claro em seu parágrafo único que considera os dados como coletados no território nacional quando o seu titular ali se encontrar no momento da coleta.

Já o Art. 4º aborda os casos em que a lei não se destina, no seu § 3º faz menção a um órgão competente quanto ao assunto da proteção de dados. No seu Art. 5º, como já comentado anteriormente, lista termos bastante completo, dando suplementação a falta de alguns conceitos não abordado no Código de Defesa do Consumidor, no Marco Civil e em seu Decreto

---

[7] PIOVESAN, Eduardo. Câmara aprova projeto que disciplina tratamento de dados pessoais. Câmara notícias, Brasília, 29 maio 2018. Disponível em: <http://www2.camara.leg.br/ camaranoticias/noticias/politica/558252-camara-aprova-projeto-que-disciplina-tratamento-de-dados-pessoais.html>. Acesso em: 1 jun. 2018.

[8] RONCOLATO, Murilo. O que diz o projeto de lei de proteção de dados que tramita no Senado. Nexo, São Paulo, 7 jun. 2018. Disponível em: <https://www.nexojornal.com.br/ expresso/2018/06/07/O-que-diz-o-projeto-de-lei-de-prote%C3%A7%C3%A3o-de-dados-que-tramita-no-Senado>. Acesso em: 7 jun. 2018

regulamentador. No Art. 6º é apresentada os princípios pelos quais deve-se pautar a atividade de tratamento de dados.

O Capítulo II, Requisitos para o Tratamento de Dados Pessoais, apresenta o Art. 7º enumera as hipóteses em que o tratamento de dados poderá ser realizado. O Art. 8º regulamenta quanto às informações necessárias que devem ser disponibilizadas ao usuário, referentes ao tratamento de seus dados.

Já o Art. 11 trata da vedação ao tratamento dos dados sensíveis, exceto uma série de situações, que podem se transformar em qualquer situação, dependendo apenas de consentimento, em alguns casos. Em geral, são dados que podem ser usados para causar dano ao titular, como dados sobre raça, religião, sexualidade, opinião política, dados genéticos e biométricos. O Art. 13, trata dos dados anonimizados que foram revertidos ou que possam ser revertidos ao estado inicial, assim como os dados utilizados para formação de perfil comportamental de uma determinada pessoa natural, identificada. A temporalidade dos dados, é tratada no Art. 15, que dispõe sobre as hipóteses do término do tratamento dos dados pelo responsável, e o Art. 16 complementa o dispositivo.

O Capítulo III, Dos Direitos do Titular, começa com o Art. 17 já assegurando a toda pessoa natural a titularidade dos seus dados, e o Art. 18 dá complemento ao artigo anterior, em que tem direito de obter, em relação a seus dados, o titular dos dados pessoais.

O Art. 19 aborda a confirmação da existência ou o acesso aos dados pessoais pelo titular, e também explicita os formatos em que poderão ser solicitadas as informações. O Art. 20 trata do direito à revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses. O Art. 21 diz que os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo. Já o Art. 22 fala da possibilidade de tutela individual e coletiva dos direitos dos titulares de dados, como visto em outras situações.

O Capítulo IV, Do Tratamento de Dados pessoais pelo Poder Público, vai do Art. 23 ao Art. 30, tratando da administração direta e indireta em relação aos dados pessoais.

O Capítulo V, Da Transferência Internacional de Dados, começa com o Art. 33 ao tratar as hipóteses de possibilidade de transferência de dados pessoais a outros países, que levará principal em consideração o nível de proteção de dados do país que receberá os dados. No Art. 35, entre outros pontos, que o órgão competente poderá elaborar cláusulas contratuais padrão ou homologar dispositivos que constem em documentos ou realizadas diligências de verificação quanto às operações em andamento que fundamentem a transferência internacional de dados, que podem ser requeridas informações suplementares.

O Capítulo VI, Dos Agentes do Tratamento de Dados, vai do Art. 36 a 40, que tratam que estes agentes são o Responsável e o Operador, onde este último deverá realizar as operações de acordo com as instruções repassadas pelo Responsável, que deverá verificar a observância de suas próprias instruções e da legislação aplicável, e que a comunicação de dados entre eles deve ser autorizada pelo titular, salvo hipóteses de dispensa de consentimento previstas.

Nesta senda, do Art. 42 ao Art. 44 é tratado a questão da responsabilidade e ressarcimento de danos, falando sobre a obrigatoriedade de reparação de danos causados a outrem em vista da atividade de tratamento de dado pessoais, da possibilidade de inversão do ônus da prova, que eventual dispensa de consentimento não dispensa as demais obrigações previstas nesta lei, e da obrigação solidária entre cedente e cessionário, observadas exceções previstas.

O Capítulo VII, Da Segurança e das Boas Práticas, em sua primeira seção, que vai do Art. 45 ao Art. 49, trata sobre a segurança e sigilo de dados, das medidas técnicas e administrativas que o operador deve tomar na prevenção de acidentes e ilícitos, que o órgão competente poderá dispor sobre padrões técnicos e organizacionais para as tarefas, e que deverão obedecer ao estado atual da tecnologia, principalmente no caso de dados sensíveis. A segunda seção das boas práticas, que podem ser formuladas individualmente pelas empresas ou por associações, tendo em vista o escopo, natureza, finalidade do tratamento dos dados, e a probabilidade/gravidade dos riscos dos danos aos titulares, e o órgão competente estimulará a adoção de padrões técnicos que facilitem o controle dos titulares sobre seus dados pessoais.

O Capítulo VIII, Da Fiscalização, é considerado muito importante, porque estabelece em seu Art. 52 as sanções administrativas para as infrações realizadas pelas pessoas jurídicas de direito privado, aplicáveis pelo órgão competente, que serão aplicadas fundamentadamente, isolada ou cumulativamente, de acordo com o caso concreto.

O Art. 53 dispõe sobre as atribuições do órgão competente para a fiscalização do disposto na lei, bastante extensas, incluem, entre outras, a elaboração de uma Política Nacional de Dados Pessoais e Privacidade, realizar auditorias nos tratamentos de dados pessoais, e estabelecer normas complementares para as atividades de comunicação de dados pessoais e sobre proteção de dados pessoais e privacidade.

O capítulo IX, Da Autoridade Nacional de Proteção de dados e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, que vai do Art. 55 ao Art. 59, aborda a criação dos órgãos que devem aplicar e fiscalizar a lei de proteção de dados. O Art. 55 indica a competência do referido Conselho, que inclui fornecimento de subsídios para a formação da Política Nacional de Proteção de Dados Pessoais e da Privacidade, assim como elaborar

relatórios anuais e avaliação das ações desta sugestão de ações a serem tomadas pelo órgão competente, realização de estudos e debates sobre o tema, e a disseminação de conhecimento sobre proteção de dados e privacidade à população em geral. O Art. 58 trata da composição do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade sendo formado por 23 representantes titulares e seus suplentes.

E por último, o capítulo X trata das Disposições Finais e Transitórias, indo do Art. 60 ao 65. O último artigo estabelece que a lei tem dezoito meses para entrar em vigor após a sua aprovação.

Nesta senda, o estudo passa a abordar os direitos a privacidade do titular dos dados pessoais, elencados no Projeto de Lei, expressamente relacionados nos incisos do Art. 18 do PLC 53/2018, assim como termos referentes ao desenvolvimento do estudo.

***Direito de acesso***: Art. 18, inciso II - acesso aos dados. O titular pode acessar os dados e receber informações sobre o tratamento e suas finalidades. O artigo 9º do PLC, detalha o acesso aos dados da seguinte forma (BRASIL, 2018):

> O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva, acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> [...]

***Direito de correção dos dados***: Art. 18, inciso III - "correção de dados incompletos, inexatos ou desatualizados" (BRASIL, 2018). O responsável tem a obrigação de retificar dados a pedido do titular.

***Direito de portabilidade***: Art. 18, inciso V - "portabilidade dos dados pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão responsável" (BRASIL, 2018). É o direito do titular dos dados de transferi-los de um serviço para outro.

***Direito ao esquecimento***: O PLC 53/2018 não traz expressamente em seus artigos o direito ao esquecimento. É entendido como o direito de uma pessoa não ter exposto ao público um fato que, mesmo verídico, possa lhe causar transtornos e sofrimento. O novo (GDPR) Regulamento Geral de Proteção de Dados Pessoais 2016/679[9], que entrou em vigor no último

[9] UNIÃO EUROPEIA. Regulamento 2016/679 de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://eur-lex.europa.eu/legal content/PT/TXT/PDF/?uri= CELEX:32016R0679&from=EN>. Acesso em: 6 jun. 2018.

dia 25 de maio na União Europeia, revogando a Diretiva 95/46/CE, passou a prever expressamente o direito a ser esquecido em seu Art. 17, nº 1. O titular dos dados tem o direito de solicitar ao responsável pelo tratamento de dados que sejam excluídos seus dados sem demora injustificada quando não forem mais necessários para a finalidade que motivaram sua coleta. Bem como quando o titular remove seu consentimento sobre o tratamento de dados e passa a não existir mais fundamento jurídico para seu tratamento. Vale ressaltar que o direito ao esquecimento não tem aplicação obrigatória ao entrar em choque com o direito da liberdade de expressão e da informação, razão de interesse público ou para o cumprimento de obrigação legal prevista pelo direito da União Europeia ou por Estado-Membro ao qual esteja sujeito.

***Direito de saber se os dados pessoais foram hackeados***: O Art. 48 do PLC trata dos casos de riscos de segurança aos dados dos titulares. Nos casos de vazamentos ou falhas de segurança que evidenciem riscos aos dados pessoais deve o responsável comunicar ao titular e ao órgão competente em prazo razoável, que avaliará e decidira os próximos passos e caso necessário, para salvaguarda dos direitos dos titulares, divulgar a falha em meios de comunicação e medidas para reverter os danos causados. Já em relação ao Regulamento da União Europeia, nos casos de vazamentos de dados, obrigatoriamente cabe ao responsável pelo tratamento avisar a Autoridade de Controle, o mais tardar 72 horas após ter conhecimento do ocorrido, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades individuais. A notificação à autoridade de controle é acompanhada de uma justificação fundamentada caso não seja feita no prazo de 72 horas. Acrescente-se a obrigatoriedade de informar o titular dos dados quando a violação dos dados pessoais for suscetível de implicar um elevado risco para seus direitos e liberdades.

***Consentimento***: O Art. 5º, inciso XII, do PLC 53/2018 define o que vem a ser consentimento: "Art. 5º, Inciso XII - manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, 2018). É um dos requisitos para o tratamento dos dados pessoais do titular pelo Poder Público e pelas empresas. (Art. 7º, Inciso I, do PLC). O Art. 8º trata das formalidades do consentimento. Deve ser, se de acordo com o Art. 7, Inciso I, fornecido por escrito ou outro meio que demon0stre a manifestação de vontade do titular; se fornecido por escrito, deverá demonstrar cláusula destacada das demais; O titular pode retirar seu consentimento, pedir a exclusão ou a portabilidade dos seus dados pessoais; Exigência de consentimento de pais ou responsável legal para o tratamento de dados de crianças. Uma vez em mãos, a empresa ou órgão público fica impedida de repassá-los a terceiros sem nova autorização. "O consentimento deverá referir-se a finalidades determinadas e serão nulas as autorizações genéricas para o

tratamento de dados pessoais". "É vedado o tratamento de dados pessoais mediante vício de consentimento" (BRASIL, 2018, p. 10). O consentimento na Diretiva 95/46/CE sofreu mudança com a entrada novo Regulamento da União Europeia. Segundo o Art. 4 é necessário que o consentimento seja obtido por uma resposta afirmativa do titular indicando sua manifestação de vontade livre, específica, inequívoca e informada, no sentido de que concorda que seus dados pessoais sejam objeto de tratamento. A obtenção do consentimento deve ser feita de forma explícita, numa linguagem clara e simples. Nos casos em que o tratamento sirva para diversas finalidades, deverá ser dado um consentimento para todas elas.

***Compartilhamento dos dados pessoais***: A definição do termo podemos encontrar no dispositivo do PLC 53/2018 abaixou descrito:

> Art. 5º, Inciso XVI - a comunicação, a difusão, a transferência internacional, a interconexão de dados pessoais ou o tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre estes e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados. (BRASIL, 2018, p. 5)

Em relação aos dados sensíveis, o Art. 11 afirma que é vedada a comunicação ou o uso compartilhado entre responsáveis de dados sensíveis referentes à saúde com o objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular. De acordo com o Art. 9º, Inciso V, o titular dos dados tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva sobre informações acerca do uso compartilhado de dados pelo responsável e sua finalidade.

***Privacidade por defeito***: É um termo que se refere a uma medida técnica para explicar que as empresas devem oferecer, por defeito, sistemas que protejam seus clientes. Isto significa assegurar que são colocados em prática, dentro de uma organização, mecanismo para garantir que, por defeito, apenas será recolhida, utilizada e conservada para cada tarefa, a quantidade necessária de dados pessoais. O Art. 25, nº 2 do Regulamento da União Europeia expressa a significação do termo:

> O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares. (UNIÃO EUROPEIA, Regulamento 2016/679, p.48)

O PLC 53/2018 não traz especificamente dispositivo que regule a medida técnica, apenas menciona no Art. 6º o princípio da necessidade e Art. 46, no capítulo de segurança e boas práticas, demanda aos agentes a adoção de medidas de segurança, técnicas administrativas para proteger os dados pessoais.

***Sanções administrativas***: O PLC trata das sanções aos agentes no capítulo VIII - Da Fiscalização, sendo aplicadas pelo órgão competente. Estão previstas no Art. 52. São: suspensão das atividades da empresa por seis meses, prorrogável por igual período; multa simples ou diária de até 2% do seu faturamento ou no máximo R$ 50 milhões por infração. Quanto ao Regulamento 2016/679 da União Europeia, as sanções são aplicadas pelos Estados-Membros. É previsto no Art. 83º, n. 5. O valor da multa pode chegar até €20.000.000 ou 4% do volume de negócios anuais da empresa.

***Órgão/Conselho competente*:** O PLC no capítulo IX, cria a Autoridade Nacional de Proteção de Dados, que é submetida a regime autárquico e vinculada ao Ministério da Justiça, com previsão no Art. 55; caracterizada por independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes e autonomia financeira, sendo previsto no Art. 55. § 3º. A Autoridade será gerida por três conselheiros que formam o Conselho Diretor, Art. 55, § 2º, nomeados por decreto. Logo abaixo do Conselho Diretor, a Autoridade terá o Conselho Nacional de Proteção de Dados Pessoais, Art. 58, composto por 23 representantes, O Projeto ainda prevê, a participação de quatro membros de instituições científicas e tecnológicas Art. 58, VIII, e quatro membros da sociedade civil com atuação comprovada em proteção de dados pessoais Art. 58, II. A Autoridade Nacional de Proteção de Dados tem como funções, fiscalizar e aplicar sanções, zelar pela proteção dos dados pessoais, elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, entre outras. Fica evidente após essa exposição que o PLC 53/2018 prevê a constituição de um órgão regulador aos moldes do europeu, com funções de conselho, controle, exercendo autoridade para tratar da proteção dos dados pessoais.

Da análise do Projeto de Lei aprovado da Câmara, o texto felizmente agregou muitos pontos do PL 5.276/2016 que se originou nas discussões do anteprojeto, assim como no Regulamento da União Europeia, atual paradigma de norma sobre a proteção de dados pessoais no mundo.

# 6 CONSIDERAÇÕES FINAIS

Devido aos avanços tecnológicos e o advento da *Internet*, a sociedade atual se reconfigurou a partir da expansão do ciberespaço, sendo impossível para um país nos dias de hoje não tratar de maneira específica as implicações surgidas com a evolução desse ambiente virtual. O direito à privacidade compõe um dos direitos fundamentais de qualquer indivíduo e tem previsão constitucional expressa na Carta de 1988, bem como no Código Civil de 2002, apesar disso, essa tutela é de natureza muito genérica e limitada aos ambientes físicos, revelando ineficácia para proteção dos dados pessoais no contexto da *Internet*, como consequência todos os dias violações a esse direito são constatadas. O usuário brasileiro encontra-se em total vulnerabilidade em decorrência das práticas de mercado adotadas pelas empresas, que utilizam os dados pessoais como moeda de troca, satisfazendo seus interesses privados, deixando o interesse público em segundo plano.

Foi a Lei 12. 965/14, o Marco Civil, a primeira em nossa legislação que se dedicou a tratar do funcionamento da *Internet* e mais recente o Decreto 8.771/16 que fez sua regulamentação. O Marco Civil da Internet apesar de ter sido um grande avanço na tentativa de regular o ambiente informacional do país, não tratou especificamente da proteção de dados pessoais na rede, positivando em seu art. 3, III, que lei singular aprofundaria o tema.

Diante destas constatações, o presente estudo entende que para a solução da problemática é necessário a aprovação de uma lei geral e específica de proteção de dados pessoais que esteja em consonância com os desafios jurídicos advindos com a implantação do espaço informacional e que esta se aproxime das diretivas da União Europeia, ao apresentar princípios e conceitos gerais precisos, assim como a criação de órgão autônomo, encarregado de aplicar e fiscalizar o cumprimento da lei, garantindo assim, a salvaguarda efetiva da proteção dos dados pessoais dos usuários da *Internet* no Brasil.

Do exame dos projetos de lei que foram apresentados, o PL nº 4.060/2012 que foi aprovado pela Câmara dos Deputados, agregando em seu texto pontos do PL nº 5.276/2016, se aproxima do ideal de norma sobre a proteção de dados ao tratar, embora não completamente, os interesses públicos do Estado bem como das empresas privadas.

Em última análise, o Brasil se vê prestes a aprovar uma lei geral de proteção de dados pessoais, tendo em vista que o PL nº 4.060/2012 foi aprovado pela Câmara no mês passado já com o novo texto incorporando aspectos do PL nº 5.276/2016. O texto foi encaminhado ao Senado e apensado ao PLS 330/2013 para discussão. Caso o texto não sofra nenhuma alteração pelos senadores, será enviado ao Presidente para sanção.

# ANALYSIS OF THE LAW PROJECTS ON PROTECTION OF PERSONAL DATA IN BRAZIL UNDER THE LIGHT OF GENERAL RULES ABOUT DATA PROTECTION OF EUROPEAN UNION


## ABSTRACT

This paper is about the issue of personal data protection in Brazil concerning to the national legal regulation that does not dispose of a general law that deal with the protection of users privacy on the Internet. The data processing ability increases widely by computers network and it shows a threat to fundamental rights of privacy and intimacy through collecting and improper treatment of personal data by both Public Power and private companies. This study analyzes the main legislatives initiatives in discussion in National Congress of Brazil that aims to approve a general regulation of personal data protection. It was chosen the inductive method based in bibliographic research through legal doctrine, published articles as well as the present legislation. This work reaffirms the necessity of specific rule approval, for example, as the European Union Regulation, that has the General Data Protection Regulation (GDPR) and so it makes possible the consolidation of the country legal framework in custody of personal data protection.


**Keywords**: Privacy. Internet. Personal data protection. Law project.

# REFERÊNCIAS


ARAUJO, Luiz Ernani Bonesso; CAVALHEIRO, Larissa Nunes. **A proteção de dados pessoais na sociedade informacional brasileira**: o direito fundamental a privacidade entre a autorregulação das empresas e a regulação protetiva do internauta. Revista do Direito Público, Londrina, v. 9, n. 1, p. 209-226, jan./abr. 2014. DOI: 10.5433/1980-511X.2014v9n1p209.

ARTIGO19. **Proteção de dados pessoais no Brasil**: Análise dos projetos de lei em tramitação no Congresso Nacional. Disponível em: <http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Prote%C3%A7%C3%A3o-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf>. Acesso em: 7 jun. 2018

BRASIL. Câmara dos Deputados. **Ficha de tramitação do Projeto de Lei nº 5.276/2012**. Disponível em:<http://www.camara.gov.br/proposiçõesWeb/ fichadetramitacao?idProposicao =2084378>. Acesso em: 5 jun. 2018.

_____. Câmara dos Deputados. **Projeto de Lei nº 4.060/2012**. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. 2012. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=4673F89CFB5E66C0E6B323A589909C2D.proposicoesWebExterno1?codteor=1001750&filename=PL+4060/2012>. Acesso em: 4 jun. 2018.

_____. **Código Civil**. Brasília, 10 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/2002/l10406.htm>. Acesso em: 7 jun. 2018.

_____. Constituição (1988). **Constituição da República Federativa do Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 6 jun. 2018.

_____. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm>. Acesso em: 7 jun. 2018.

_____. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. **Acesso à Informação**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 7 jun. 2018.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Código de Defesa do Consumidor**. Disponível em: <http:// www.planalto.gov.br/ccivil_03/Leis/l8078.htm>. Acesso em: 7 jun. 2018.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Marco Civil da Internet**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 7 jun. 2018.

_____. Senado Federal. **Projeto de Lei da Câmara n° 53, de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. 2018. Disponível em: < https://legis.senado.leg.br/sdleg-getter/documento?dm=7738646&ts=1528477863709 &disposition=inline&ts=1528477863709>. Acesso em: 8 jun. 2018.

_____. Senado Federal. **Projeto de Lei do Senado n° 181, de 2014**. Estabelece princípios, garantias, direitos e obrigações referentes à proteção de dados pessoais. 2014. Disponível em: < https://legis.senado.leg.br/sdleg-getter/documento?dm=2925965&ts=1528478318592& disposition=inline&ts=1528478318592>. Acesso em: 5 jun. 2018.

_____. Senado Federal. **Projeto de Lei do Senado n° 330, de 2013**. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. 2013. Disponível em: < https://legis.senado.leg.br/sdleg-getter/documento?dm=2931559&ts=1528478375763 &disposition=inline&ts=1528478375763>. Acesso em: 5 jun. 2018.

CARVALHO, Ana Paula Gambogi. **O consumidor e o direito à autodeterminação informacional**: considerações sobre os bancos de dados eletrônicos. Revista de direito do consumidor, v. 46, p. 77-119, 2003.

CRAVO, D. C. **Proteção à privacidade na internet**: aplicação "Territorial" pela União Europeia do direito ao esquecimento? Revista Brasileira de Direitos Humanos, São Paulo, v. 75, n. 14, p. 26-47, jul./set. 2015.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

GEHRKE, Daniel Bender. **A necessidade de lei de proteção de dados no brasil**. 2016. 84f. Monografia (apresentada como exigência parcial para a obtenção do título de bacharel em Direito) - Faculdade de Direito, Universidade Federal do Rio Grande do Sul, Porto Alegre. Disponível em: < http://hdl.handle.net/10183/157685>. Acesso em: 7 jun. 2018.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 5. ed. São Paulo: Atlas, 1999.

GONÇALVES, Maria Eduarda. **Direito da Informação**: novos direitos e formas de regulação na sociedade da informação. Coimbra: Almedina, 2003.

LIMBERGER, Têmis. **Da evolução do direito a ser deixado em paz à proteção dos dados pessoais**. Novos Estudos Jurídicos, Itajaí, v. 14, n. 2, p. 27-53, 2009. Disponível em: <https://siaiap32.univali.br/seer/index.php/nej/article/download/1767/1407>. Acesso em: 12 jun. 2018.

MOTA PINTO, Paulo Cardoso Correia da. **A proteção da vida privada**. Boletim da Faculdade de Direito, vol. LXXVI, Universidade de Coimbra, 2000.

O escândalo que fez o Facebook perder US$ 35 bilhões em horas. **BBC**, São Paulo, 20 mar. 2018. Disponível em: <https://www.bbc.com/portuguese/internacional-43466255>. Acesso em: 7 jun. 2018.

O que sabemos do escândalo do Facebook e por que você deve se preocupar. **UOL**, São Paulo, 21 mar. 2018. Disponível em: <https://tecnologia.uol.com.br/listas/o-que-sabemos-do-escandalo-do-facebook-e-por-que-voce-deve-se-preocupar.htm>. Acesso em: 7 jun. 2018.

PINHEIRO, Patrícia Peck. **Direito digital**. São Paulo: Saraiva, 2013.

PIOVESAN, Eduardo. Câmara aprova projeto que disciplina tratamento de dados pessoais. **Câmara notícias**, Brasília, 29 maio 2018. Disponível em: <http://www2.camara.leg.br/camaranoticias/noticias/politica/558252-camara-aprova-projeto-que-disciplina-tratamento-de-dados-pessoais.html>. Acesso em: 1 jun. 2018.

RECUERO, Raquel. **Redes sociais na internet**. Porto Alegre: Sulina, 2009.

RONCOLATO, Murilo. O que diz o projeto de lei de proteção de dados que tramita no Senado. **Nexo**, São Paulo, 7 jun. 2018. Disponível em: <https://www.nexojornal.com.br/expresso/2018/06/07/O-que-diz-o-projeto-de-lei-de-prote%C3%A7%C3%A3o-de-dados-que-tramita-no-Senado>. Acesso em: 7 jun. 2018

SALOMÃO, Karin. Cambridge Analytica irá fechar depois de escândalo com Facebook. **EXAME**, São Paulo, 2 maio 2018. Disponível em: <https://exame.abril.com.br/negocios/cambridge-analytica-ira-fechar-depois-de-escandalo-com-facebook/>. Acesso em: 6 jun. 2018.

SAWAYA, Márcia Regina. **Dicionário de informática e internet**. São Paulo: Nobel, 1999.

SILVA, Rosane Leal da. As tecnologias da informação e comunicação e a proteção de dados pessoais. In: ANAIS DO XIX ENCONTRO NACIONAL DO CONPEDI, 19, 2010, Fortaleza. **Anais**... Fortaleza, 2010. p. 3907-3918.

SILVA, S. A; NHARRELUGA, R. S; JARDIM, J. M. **Análise de Políticas Públicas**: uma abordagem em direção às políticas públicas de informação. Perspectivas em Ciência da Informação. (Impresso), v. 14, p. 2-22, 2009.

TEIXEIRA, Tarcísio. **Curso de direito e processo eletrônico**: doutrina, jurisprudência e prática. 2. ed. São Paulo: Saraiva, 2014.

UNIÃO EUROPEIA. **Diretiva (UE) 2016/680 de 27 de abril de 2016**. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=PT>. Acesso em: 5 jun. 2018.

UNIÃO EUROPEIA. **Regulamento 2016/679 de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 6 jun. 2018.

VANCIM, Adriano Roberto; MATIOLI, Jeferson Luiz. **Direito & internet**: contrato eletrônico e responsabilidade civil na Web. Franca, SP: Lemos & Cruz, 2014.