UNIVERSIDADE DO ESTADO DO AMAZONAS
ESCOLA SUPERIOR DE CIÊNCAS SOCIAIS
CURSO DE DIREITO

JONAS SANTOS DE MELO

O DIREITO À PRIVACIDADE, AUTODETERMINAÇÃO INFORMATIVA E PROTEÇÃO DE DADOS PESSOAIS: O CONTEXTO DA LEI 13709/2018

MANAUS
2018

JONAS SANTOS DE MELO

O DIREITO À PRIVACIDADE, AUTODETERMINAÇÃO INFORMATIVA E PROTEÇÃO DE DADOS PESSOAIS: O CONTEXTO DA LEI 13709/2018

Monografia apresentada na disciplina de Monografia II na Universidade do Estado do Amazonas – UEA, como exigência parcial para obtenção do título de Bacharel em Direito.

Orientador: Prof. Msc. Neuton Alves de Lima

MANAUS
2018

Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).
Sistema Integrado de Bibliotecas da Universidade do Estado do Amazonas.

M528d MELO, Jonas Santos de
O direito à privacidade, autodeterminação informativa e proteção de dados pessoais: : o contexto da lei 13709/2018 / Jonas Santos de MELO. Manaus : [s.n], 2018.
47 f.: il.; 29 cm.

TCC - Graduação em Direito - Bacharelado - Universidade do Estado do Amazonas, Manaus, 2018.
Inclui bibliografia
Orientador: Neuton Alves de Lima

1. Direito à privacidade. 2. Autodeterminação informativa. 3. Proteção de dados pessoais. I. Neuton Alves de Lima (Orient.). II. Universidade do Estado do Amazonas. III. O direito à privacidade, autodeterminação informativa e proteção de dados pessoais:

Elaborado por Jeane Macelino Galves - CRB-11/463

UEA
UNIVERSIDADE
DO ESTADO DO
AMAZONAS

UNIVERSIDADE DO ESTADO DO AMAZONAS
ESCOLA SUPERIOR DE CIÊNCIAS SOCIAIS
CURSO DE DIREITO
TERMO DE APROVAÇÃO

JONAS SANTOS DE MELO

O DIREITO À PRIVACIDADE, AUTODETERMINAÇÃO INFORMATIVA E PROTEÇÃO DE DADOS PESSOAIS: O CONTEXTO DA LEI 13709/2018

Monografia aprovada como requisito parcial para obtenção do grau de Bacharel no Curso de Graduação em Direito, Escola Superior de Ciências Sociais, Universidade do Estado do Amazonas, pela seguinte banca examinadora:

Orientador (a): Prof. Me. Neuton Alves de Lima

Membro 2: Prof. Dr. Antonio Gelson de Oliveira Nascimento

Membro 3: Profª. Esp. Adriana Moutinho Magalhães Iannuzzi

Manaus, 14 de dezembro de 2018

A Deus, o dono da sabedoria.

À minha avó, Maria José (in memorian).

À minha mãe, Sandra Maria.

AGRADECIMENTOS

A Deus, por ter me concedido, com graça e misericórdia, força em todos os momentos e por ter me sustentado com seu amor insuperável todos os dias.

À minha avó, Maria José (in memorian), que me passou valores de fé e ética, de quem eu nunca deixarei de ter saudade.

À minha mãe Sandra Maria, companheira extraordinária em todas as horas, por todo investimento nos meus estudos e por me encorajar, mesmo quando eu não queria ser encorajado.

Aos meus irmãos Junior, Priscila e Patrícia, que nunca me abandonam.

À Sra. Raimunda Oliveira (Dona Rai), um anjo que Deus colocou na minha vida.

Aos meus amigos, em especial ao Yuri, Lucivan, André e Caio, que dispensaram momentos de lazer para somarem comigo nesta empreitada, pelo incentivo e apoio imprescindíveis em todos os momentos.

À universidade, que me oportunizou a concretização deste curso superior.

Aos meus mestres, em especial ao professor Antonio Gelson, parceiro desde antes do início do curso, e ao meu orientador, professor Neuton Lima, por compartilharem suas experiências e conhecimentos de forma tão nobre, pelo tempo que lhes coube e por cada correção, obrigado pela confiança e paciência.

A todos que colaboraram direta ou indiretamente, muito obrigado.

“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”. Tim Cook, CEO da Apple.

“Ao passo que proteção de dados constitui não apenas um direito fundamental entre os outros: é o mais expressivo da condição humana contemporânea”. (RODOTÁ, 2008, p. 21).

RESUMO

A internet coleta e processa dados a todo instante e é indispensável atualmente para o funcionamento dos mais diversos setores da sociedade. No entando, o uso indevido de dados, sobretudo dados pessoais, por empresas e organizações na rede mundial de computadores, levou alguns países à criação de normas que visam a proteção desses dados e o controle dos riscos à violação da privacidade. No Brasil, debatida por oito anos no Congresso, a recém sancionada Lei Geral de Proteção de Dados Pessoais, que altera o Marco Civil da Internet, segue essa corrente, no sentido de se normativizar o tratamento dos dados acima qualificados, que são coletados por empresas do setor público e privado, sobretudo no meio digital interconectado. Quais os ajustes e resultados esperados pela LGPD na sociedade e nos setores que tratam de dados pessoais digitais? Este trabalho se propõe a explorar, condensadamente, os conceitos de privacidade e à autodeterminação informativa na construção do direito à proteção de dados pessoais. Tendo em vista que o estudo da temática acerca do termo "proteção de dados pessoais" é atual e, ainda, incipiente no meio jurídico brasileiro, esse trabalho busca conceituar o referido termo e retratar o cenário da proteção de dados no plano internacional. Busca ainda analisar a Lei de Proteção de Dados – LGPD, sua aplicação, objetivos e impactos que ela espera alcançar na sociedade e nos setores que tratam dados no Brasil. Adotou-se para o desenvolvimento do trabalho o metodologia de pesquisa descritiva, com levantamento teórico obtido em livros, artigos e demais publicações sobre o tema. Constatou-se que as empresas e órgaos governamentais precisarão de urgência na implementação do que se estabelece a nova lei, que passa a vigorar no ano de 2020, a priori na revisão das políticas de segurança, revisão de contratos e elaboração de Relatório de Impacto de Privacidade. Por fim, concluiu-se que é necessário um amplo debate acadêmico e da sociedade como um todo acerca do tema, que afetará significativamente a forma como se executa os procedimentos referentes a coleta e processamento de dados pessoais sistematizados.

Palavras-chave: Proteção de Dados Pessoais. Autodeterminação Informativa. Direito à Privacidade. LGPD.

ABSTRACT

The internet collects and processes data at all times and is indispensable today for the operation of the most diverse sectors of society. However, the misuse of data, especially personal data, by companies and organizations in the global computer network, has led some countries to create standards that aim to protect such data and control the risks to privacy breach. In Brazil, debated for eight years in Congress, the recently enacted General Law for the Protection of Personal Data, which amends the Civil Registry of the Internet, follows this trend, in order to regulate the treatment of the data above qualified, since they are collected by public and private sector, especially in the interconnected digital medium. What are the adjustments and expected results of the LGPD in society and in the sectors that deal with digital personal data? This work proposes to explore, in a condensed way, the concepts of privacy and self-determination in the construction of the right to personal data protection. Considering that the study of the theme of the term "protection of personal data" is current and still incipient in the Brazilian legal environment, this work seeks to conceptualize the term and portray the scenario of data protection at the international level. It also seeks to analyze the Law on Data Protection - LGPD, its application, objectives and impacts that it hopes to achieve in society and in sectors dealing with data in Brazil. The methodology of descriptive research was adopted for the development of the work, with a theoretical survey obtained in books, articles and other publications on the subject. It was found that companies and government bodies will need to urgently implement the new law, which will come into force in 2020, a priori in the revision of security policies, review of contracts and elaboration of the Report of Impact of Privacy. Finally, it was concluded that a broad academic and societal debate on the subject is needed, which will significantly affect the way in which the procedures for the collection and processing of systematized personal data are performed.

Key-words: Protection of Personal Data. Informational self-determination. Right to privace. LGPD

SUMÁRIO

INTRODUÇÃO

Os avanços em tecnologia da informação e ciência da computação mudaram substancialmente a forma como as pessoas e organizações se relacionam entre si. O uso cada vez mais ampliado de sistemas informatizados que lidam com os mais variados tipos de dados é uma das consequências dos avanços tecnológicos alcançados nas últimas décadas. Diante desse panorama, a democratização e a globalização da internet foram responsáveis por uma grande transformação no que se refere ao fluxo de informações: a do mundo interconectado, onde grande parte das informações que são coletadas, processadas e propagadas se situam na rede mundial de computadores, em uma realidade em que a internet se torna indispensável no funcionamento dos mais diversos setores, sejam eles governamentais ou privados. Hospitais, bancos, escolas, empresas e uma lista infindável de organismos dependem da internet para a execução de seus respectivos procedimentos, assim como do tratamento ágil da informação requeridas por estes.

É importante salientar que para essa pesquisa não se levará em conta as diferenças terminológicas acerca dos conceitos de dado e informação, abordagem essa que fica ao encargo das ciências da informação.

Contudo, inúmeros casos de vazamentos de dados pessoais fizeram surgir a necessidade da criação de medidas que coibissem a violação da privacidade e confidencialidade dos dados dos cidadãos. Fez surgir também normativas vinculantes às instituições que detém, em suas bases de dados, informações de caráter pessoal de seus usuários, de modo a proteger direitos humanos fundamentais positivados tanto na Declaração Universal dos Direitos Humanos como na Constituição.

A Lei Geral de Proteção de Dados Pessoais, conhecida pela sigla LGPD, surge nesse cenário de controvérsia para gerenciar a utilização dos dados de pessoas físicas por empresas e órgãos públicos e a livre circulação desses dados, tecnicamente conhecida como "*free data flow"*, em face à atual concepção do direito à privacidade e à autodeterminação informativa. A LGPD possui forte influência do Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation* – GDPR), promulgado no ano de 2016 pela União Europeia, cuja busca tentou unificar a legislação acerca do tema dispersada nos países que a compõe, de modo a tornar as tarefas de consultoria e auditoria mais viáveis em seu bloco.

Com amplo debate legislativo, a LGPD ou lei nº 13709/2018, que altera a lei nº 12.965/2014 (Marco Civil da Internet) foi sancionada com vetos em agosto de 2018 e traz em seu bojo regras, princípios e sanções acerca da conduta de tratamento de dados pessoais por

empresas e instituições públicas e privadas; além disso, passará por um lapso de 18 meses para que tais instituições possam ter tempo hábil para a sua implementação e aplicação.

Trata-se, portanto, de uma lei que afetará toda a sociedade, uma vez que grande parte das pessoas, hoje, possuem algum tipo de cadastro em sistemas de informação e de base de dados em geral, sejam eles governamentais, a exemplo do DATASUS (Departamento de informática do SUS), ou privados, como *e-commerces* e redes sociais.

Embora a temática acerca do tema que será abordado no trabalho seja de grande relevo para toda sociedade, sobretudo à comunidade jurídica como um todo, tal discussão ainda é muito reservada a uma parcela de profissionais de tecnologia da informação, gestores de governança da informação e advogados atuantes na área de direito digital e *compliance*. O intuito desse trabalho visa justamente trazer uma compreensão mais abrangente sobre o que seria proteção de dados pessoais, suas causas e efeitos a um contingente mais leigo no assunto.

O primeiro capítulo fará uma breve leitura acerca do direito à privacidade, buscando conceituá-lo de forma sintética, sem levar em consideração as extensas e, ainda presentes, discussões acerca do conceito. Trará ainda a abordagem do direito à privacidade no âmbito da Constituição federal. Por fim, entrará no contexto em si da teoria da Proteção de Dados Pessoais, que nasceu dentro do campo de estudo do direito à privacidade, passando pela concepção de uma autodeterminação informativa, e se consubstanciando em uma disciplina autônoma de estudo, com várias construções dogmáticas sendo geradas ao redor do mundo sobre o tema.

No capítulo segundo, será discutido o conceito de proteção de dados de forma isolada. Inicialmente analisando o contexto internacional acerca da tutela em análise, tendo em vista que qualquer análise de uma nova perspectiva jurídica, que se proponha a ser útil e que busque contribuir para a ciência do direito no Brasil, deve, essencialmente, reconhecer a importância do direito comparado, em relação as soluções por ele propostas, que podem nos apontar tanto o que deve ser seguido, quanto o que deve ser mantido a distância. (LEONARDI, 2011). Nesse sentido. Nesse sentido, primeiro se relatará os casos recentes mais importantes acerca da violação a dados pessoais, para então se analisar o contexto jurídico internacional da proteção de dados pessoais, desde a sua concepção, no advento da revolução tecnológica iniciada na década de 1970, com destaque para conjuntura europeia, sobretudo da união Europeia, tendo em vista que essa região do mundo foi pioneira no debate de uma proteção jurídica que alcançasse os dados pessoais de seus cidadãos, e que ainda influencia os mais diversos ordenamentos jurídicos no que se refere à temática da proteção de dados, a exemplo do que será observado no estudo com relação ao Regulamento Geral de Proteção de Dados da União

Europeia, que se tornou um verdadeiro padrão normativo para a criação de diversas leis de proteção de dados no cenário global. Também se analisará com um pouco mais de detalhes a conjuntura dos Estados Unidos da América sobre a matéria em estudo, tendo em vista importantes setores da tecnologia, seja de hardware, seja de software, são de origem norte americana.

Na parte final do trabalho, Lei Geral de Proteção de Dados Pessoais será estudada de forma mais aplicada, traçando um panorama geral do quadro relativo à proteção de dados no Brasil, para então adentrar nos conceitos terminológicos da mesma, finalizando com o estudo de sua aplicação em solo brasileiro, levando em conta apenas os dispositivos mais relevantes da referida lei, devido às limitações do próprio estudo, que não ambiciona ser um compêndio doutrinário sobre o direito à proteção de dados.

Por ser um trabalho teórico, a metodologia adotada para o desenvolvimento do trabalho consiste em pesquisa descritiva, alinhado à pesquisa bibliográfica, com obtenção de dados em publicações e decisões diversas concernentes ao tema em análise. Segundo Cervo, Bervian e da Silva (2007), a pesquisa descritiva busca analisar, observar, registrar e correlacionar aspectos (variáveis) de como fatos ou fenômenos ocorrem, sem que haja uma interferência direta por parte do pesquisador, que busca descobrir a frequência desse fenômeno, bem como sua relação e conexão com outros, sua natureza e característica.

1 A PRIVACIDADE NA ERA DA INFORMAÇÃO E A AUTODETERMINAÇÃO INFORMATIVA: A CONSTRUÇÃO DO DIREITO À PROTEÇÃO DE DADOS

1.1 BREVES CONSIDERAÇÕES SOBRE O CONCEITO DE PRIVACIDADE

Um trabalho pioneiro, denominado “The right to privacy”, Warren e Brandeis (1890) discutiram a questão do direito à privacidade em face às tecnologias recentes à época, como fotografia, jornais e outros aparatos tecnológicos, e de como esses meios haviam adentrado no círculo de vida privada das pessoas. Os autores foram os primeiros a reconhecerem as ameaças à privacidade calçadas no desenvolvimento da sociedade. O debate iniciado pelos autores rompeu com a ideia de que o direito à privacidade não merecia tutela por se tratar de um mero direito subjetivo isento de relevância patrimonial. (DONEDA, 2006). Os autores buscaram então redefinir a proteção da vida privada, antes relacionada à propriedade, como uma proteção que se relaciona com a inviolabilidade da personalidade. (MENDES, 2014).

Alguns aspectos importantes foram identificados por Warren e Brandeis na formulação do direito à privacidade e seus limites, dos quais: 1. o direito à privacidade não é absoluto, de modo que o interesse público pode se sobrepor a ele; 2. a violação do direito à privacidade é excluída mediante o consentimento do afetado; 3. a veracidade da informação não afasta a violação do direito; 4. A dolo não é imprescindível na violação do direito em questão. (MENDES, 2014).

Notadamente, a fundação do direito à privacidade foi baseado no caráter individualista, com a ideia do direito de ser deixado só (*right to be let alone*), sendo um direito negativo que exige do Estado o dever de abstenção.

Como já discutido, a ideia inicial de privacidade consistia em garantir a cada indivíduo o direito de determinar os limites em que os seus pensamentos, sentimentos e emoções poderiam ser comunicados aos outros, ou seja, o direito de ser deixado só, numa espécie de isolamento do sujeito. Essa concepção inicial foi sendo modificada com a crescente consciência de que a privacidade é um meio de realização da pessoa e de sua personalidade. (DONEDA, 2006).

O artigo de Warren e Brandeis foi primordial para o desenvolvimento do conceito de privacidade, outrossim, foi essencial para o reconhecimento judicial da proteção, no âmbito do *Commom Law,* de um direito à privacidade. (LEONARDI, 2011).

Tal conotação de direito negativo do direito à privacidade vem sendo repensada no decorrer do século XX, em face as transformações sociais que o desenvolvimento tecnológico proporcionou, sobretudo a partir da década de 1970, o direito à privacidade passou da esfera

negativa para uma esfera de atuação positiva, possibilitando ao indivíduo o controle de suas próprias informações, sendo um corolário para qualquer regime democrático. (MENDES, 2014).

1.2 O DIREITO À PRIVACIDADE NA CONSTITUIÇÃO

Até 1988, no plano nacional, não havia um direito explícito acerca da privacidade. Na época, de modo que a certificação desses direitos era dada de forma indireta, através das institutos de inviolabilidade do lar e de correspondência, entre outros. A mudança aconteceu com a proclamação da Constituição da República Federativa do Brasil de 1988, ao consagrar art. 1º, inciso III, a dignidade da pessoa humana como um dos fundamentos da República. (AGUIAR, 2003).

Nesse sentido, sendo a condição de dignidade do indivíduo o estabelecimento como fundamento da ordem constitucional, não haveria como ignorar o direito à privacidade, sendo este um dos aspectos de maior valor do ser humano. De fato, foram os perigos inevitáveis causados por inovações tecnológicas que persuadiram o constituinte a promover a proteção desses direitos. (AGUIAR, 2003).

A constiuição de 1988 estabelece que:

> Art. 5º 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. (BRASIL, 2017, grifo nosso).

Deve-se ressaltar que o referido dispositivo, relacionado no Título II, Capítulo I – Dos Direitos e Deveres Individuais, possui status de cláusula pétrea, a garantir a sua plena realização e a sua máxima proteção. Qualidade essa que se extrai do dispostivo da CF88 transcrito abaixo:

> Subseção II
> Da Emenda à Constituição
> Art. 60. A Constituição poderá ser emendada mediante proposta:
> § 4º Não será objeto de deliberação a proposta de emenda tendente a abolir:
> IV - os direitos e garantias individuais. (BRASIL, 2017).

Ademais, conforme leciona Canotilho (2003), os direitos fundamentais são aqueles que foram juridicamente positivados no plano constitucional em vigor. Tais direitos fundamentais são concebidos, no ordenamento jurídico como um todo, como sendo aqueles que são inerentes

ao indivíduo. Por conta do fenômeno da constitucionalização desses direitos, os mesmos devem estar no ápice do dito ordenamento jurídico e devem ser entendidos como normas jurídicas vinculantes, o que *per se* os diferencia do conteúdo dos textos normativos.

1.3 O DIREITO À PRIVACIDADE EM FACE ÀS NOVAS TECNOLOGIAS

O resultado do desenvolvimento das tecnologias da informação e comunicação, bem como a utilização de novos métodos de automatização, tornaram possível a divulgação de fatos relativos ao círculo privado das pessoas de uma maneira inimaginável em momento anterior Conforme Barros (2017, p. 26):

> O avanço das Tecnologias de Informação e Comunicação torna premente a discussão a respeito da autodeterminação informativa e da privacidade, especialmente no momento histórico em que se torna difícil seguir uma rotina diária sem fornecer informações pessoais invariavelmente.
> (...)
> É possível afirmar que a realidade contemporânea mostra que todos são monitorados tanto por particulares quanto pelo Estado, sendo que essa invasão de privacidade é, de certa maneira, acentuada pela utilização das novas TIC.

Trata-se do plano de fundo de uma crescente discussão acerca da tutela da privacidade na chamada "era da informação"[1]. A partir da década de 70, é possível observar novos contornos em relação a vida privada dos cidadãos, com a edição de leis específicas, decisões judiciais, bem como de acordos internacionais, que demonstram a necessidade de proteção dos dados pessoais, sendo estes decorrentes da personalidade de um indivíduo. (MENDES, 2014). Trata-se de uma releitura do direito à privacidade, que consiste em uma proteção dinâmica e em uma liberdade positiva que o indivíduo possui em relação ao controle de suas informações pessoais.(BIONI, 2018). Nesse sentido:

> A esfera privada não seria algo já posto à espera de uma violação, mas um espaço a ser construído *a posteriori* e dinamicamente mediante o controle das informações pessoais. Haveria, por isso, uma mudança qualitativa representada pela transposição do eixo antes focado no trinômio "pessoa-informação-sigilo" ao eixo agora composto por quatro elementos – "pessoa-informação-circulação-controle". (BIONI, p. 96).

[1] O termo "era da informação" é analisado pelo sociólogo espanhol Manuel Castells, em sua obra A Era da Informação: economia, sociedade e cultura. Vol. I: A Sociedade em rede, e remete ao conjunto de eventos que assinalam o fim da era industrial e o surgimento de outra, advinda de uma revolução tecnológica iniciada na década de 70. Tal revolução dispõe de um paradigma organizado a partir do desenvolvimento das tecnologias da informação e da comunicação. (CASTELLS, 2000).

Cabe ressaltar que o direito à proteção de dados pessoais não deve ser entendido como uma mera evolução do direito à privacidade, mas como um novo direito da personalidade, que deve ser analisado em suas finalidades específicas, e não atrelado a outra espécie jurídica. Trata-se de um direito que requer autonomia, demandando uma ampliação normativa que o diferencie.

1.4 O DIREITO À AUTODETERMINAÇÃO INFORMATIVA

A temática acerca da privacidade e dos dados pessoais na era da informação tem alcançado notoriedade no meio jurídico e social, criando uma nova dogmática acerca dos direitos fundamentais. O conceito da autodeterminação informativa se insere nesse contexto como sendo um direito (ou um princípio) que um indivíduo tem de controlar a utilização de seus dados pessoais. (MENDONÇA, 2014).

A ideia de autodeterminação informativa (ou informacional) surge como um desdobramento do direito à privacidade, mas que devido ao massivo uso das tecnologias da informação nas últimas décadas, que lidam com armazenamento e processamento de dados pessoais, ganhou destaque em sua análise. (MENDONÇA, 2014).

As primeiras inferências acerca do direito à autodeterminação surgem no contexto europeu, mais especificamente pela União Europeia, no âmbito da revolução tecnológica de 1970, com a preocupação de uma regulamentação[2] que alcançasse os bancos de dados pessoais. Trata-se de um iminente pioneirismo no que se refere à proteção de dados.

O direito à autodeterminação afirmativa foi reconhecido pela primeira vez pelo Tribunal Constitucional Alemão, que declarou a nulidade da lei alemã do censo (*Volkszählunsgesetz*) que determinava a coleta de dados da população alemão referentes a questões pessoais, como suas práticas religiosas e políticas. A corte determinou que "O direito alemão de autodeterminação informativa protege o indivíduo da coleta, armazenamento, aplicação e transmissão dos dados pessoais". (SCHWARTZ, 1989, p. 689-690, tradução nossa).

Outrossim, a possibilidade de compartilhamento dos dados do censo suscitou a controvérsia acerca da disponibilidade indiscriminada dos dados dos cidadãos pelos entes estatais, gerando um ambiente de insegurança e temor de um Estado intrusivo da esfera privada dos cidadãos. (SCHWARTZ, 1989).

Segundo Bioni (2018, p.100):

[2] Será tratado como mais detalhes no item 2.2.1

> A relevância do julgado destaca-se por sua *ratio decidendi* sob dois aspectos: a) a proteção dos dados pessoais como um direito de personalidade autônomo e a compreensão do termo autodeterminação informacional para além do consentimento; b) a função e os limites do consentimento do titular dos dados.

Ainda segundo Bioni (2018, p. 100)

> (...) as considerações iniciais do julgado são de contumaz importância, na medida em que contextualizam como o avanço tecnológico e, principalmente, o progresso qualitativo na organização das informações impactaram significativamente as liberdades individuais.

Resumidamente, o Tribunal Constitucional Alemão delineou o direito à autodeterminação informativa/informacional com base no direito geral da personalidade, de modo que o mencionado direito à determinação informativa, que se concretiza na possiblidade do indivíduo autodeterminar seus próprios dados, como um aspecto fundamental do desenvolvimento da personalidade desse indivíduo. (BIONI, 2018).

1.5 DISTINÇÃO ENTRE PRIVACIDADE E PROTEÇÃO DE DADOS

Ainda no julgamento do caso da Lei do Censo, de 1983, o Tribunal Constitucional Alemão fez uma importante distinção acerca dos termos “privacidade” e “proteção” de dados. Conforme (SCHWARTZ, 1989, p. 675):

> O direito alemão demonstrou que a regulamentação de informações pessoais em computadores não pode depender da ideia legal de privacidade. Tentativas de definir uma base para um direito de privacidade baseado nas fronteiras do domínio "privado" ou no "sigilo" de informações pessoais não será bem-sucedido.

Conforme o autor, o *decisium* se prestou a dar atenção muito mais aos efeitos do processamento das informações e seus efeitos para a autonomia humana, do que às abordagens acerca do sigilo das informações coletadas. (SCHWARTZ, 1989).

Nessa perspectiva, enquanto a privacidade diz respeito àquilo que se quer manter em segredo, ou seja, refere-se às questões pessoais que se espera que não sejam conhecidas por outros, a proteção de dados busca proteger os indivíduos da exploração indiscriminada de suas informações, que pode gerar, dentre outras, circunstâncias discriminatórias e diferenciações ilegítimas.

2 A PROTEÇÃO DE DADOS PESSOAIS

2.1 CONSIDERAÇÕES INICIAIS

Como fenômeno oriundo da nova concepção humanista constitucional, o ser humano indivíduo e cidadão ou cidadã como fim e não mais mero meio, intensifica-se a preocupação da proteção na dimensão negativa e positiva do homem. Uma das esferas necessárias à completude humana é próprio desenvolvimento da personalidade. Assim, cada vez mais assume relevo a tutela dos direitos inerentes à subjetividade, exercida pelo indivíduo independente do comando ou do conhecimento estatal. Como exemplos de direitos de personalidade, temos o direito à vida, o direito à liberdade, o direito à integridade física e psíquica, os direitos do autor, o direito à honra (ou reputação), o direito à identidade pessoal e o direito à privacidade. Com relação ao direito à privacidade, podemos elencar uma série de garantias, o direito à imagem, à vida privada, ao sigilo e à intimidade. O direito à intimidade corresponde entre outros, a todos os fatos, informações, acontecimentos ou eventos, que a pessoa deseja manter dentro de seu foro íntimo, e que somente a ela interessa ter acesso. Neste contexto se insere a proteção de dados pessoais, que vem sendo compreendido como direito do indivíduo de autodeterminar suas informações pessoais. (BIONI, 2018).

A complexidade dos sistemas industriais, a burocratização dos setores nas esferas público e privada, os avanços tecnológicos e outras várias razões geram um volume de dados sem precedentes na história da humanidade. Registros de nascimento, casamento, escolares, dados do censo, militares, passaporte, servidores públicos e empregados, saúde, defesa civil, seguros, financeiros, telefônicos etc. A atividade de coleta e processamento de dados passou por uma verdadeira revolução na era da informação. (WESTIN, 1970).

Entende-se por dados pessoais na atualidade toda informação referente a um certo indivíduo, que não se limita apenas ao nome, sobrenome, idade e endereço, mas podendo também incluir dados mais específicos como histórico de compra, perfil de interesses comerciais, número de IP (*Internet Protocol*), dados acadêmicos e até mesmo a localização por GPS (*Global Positioning System*) em tempo real ou dos últimos lugares visitados. (PINHEIRO, 2018).

A ideia de proteger dados pessoais surge não apenas no intuito de proteção dos dados *per si*, mas também de seus detentores e titulares, como indivíduos que possuem, na sua esfera de proteção estatal, o direito à personalidade, sobretudo o direito à privacidade, o qual ganha novos contornos paradigmáticos com o advento da sociedade da informação e, a cada vez mais

frequente, transponibilidade do mundo real para o virtual. Surge dessa nova conjuntura novos riscos à violação de bens juridicamente protegidos. Os dados pessoais merecem tutela jurídica no sentido de que se constituem parcela da personalidade da pessoa. (MENDES, 2014), assim como aduz Cunha (2018, p. 17):

> Fique claro a proteção aos dados não é um fim por si só. Ela visa prevenir que surjam no meio social humano informações que tradicionalmente têm regime de sigilo, de decoro, de reserva. É um artifício da cultura jurídica para proteger o meio social humano e seus contornos informacionais e cognitivos tradicionais.

A informação, como um objeto de regulação, é um tema presente há tempos nas disciplinas jurídicas, sejam de ordem constitucional, penal ou comercial. No entanto, a revolução das tecnologias da informação e comunicação apresentou um desafio para o sistema jurídico que regula esse fenômeno. A interconectividade proporcionada pela rede mundial de computadores e a disponibilidade em massa dos meios informáticos estão presentes na vida e no cotidiano das pessoas. Fato esse que ganhou um conceito próprio chamado de "ubiquidade dos meios" ou "*ubiquituos computing"*. *Smartphones*, *web* 2.0, computação em nuvem e internet das coisas são alguns dos termos que se aplicam a essa nova realidade. Essa ampliação da conectividade das pessoas (naturais ou jurídicas) também fez com que se ampliasse as formas de controle, exposição indesejada, discriminação e de restrição à liberdade individual. (MENDES, 2014).

A combinação de técnicas automatizadas permite a obtenção, manipulação, cruzamento e distribuição de dados de forma não imaginada há pouco tempo, além de possibilitar a obtenção de informações que influenciam na tomada de decisões econômicas, políticas e sociais. (ALCALÁ, 2005).

Com efeito, a proteção da privacidade nos sistemas de comunicação e informação sofreu um grande abalo, a partir do momento em que fora revelado que tanto órgãos governamentais, como empresas privadas estariam violando a integridade e confidencialidade do fluxo das informações pessoais dos cidadãos armazenadas em seus bancos de dados, suscitando o temor do controle e vigilância através desses dados, o que vem sendo chamado de *Dataveillance.* (MENDES, 2014) (NETO; MORAIS; BEZERRA, 2017).

2.2 CASOS RELEVANTES DE VIOLAÇÃO A DADOS PESSOAIS

No ano de 2013, Edward Snowden[3], Analista de Sistemas contratado pela Agência Nacional de Segurança dos Estados Unidos da América revelou detalhes do que viria a ser um escândalo de grandes proporções acerca de espionagem da internet e de meios de comunicação, expondo-se de forma inédita os riscos à violação da privacidade dos cidadãos na era da informação. (MENDES, 2018)

Mais recentemente, agências importantes de notícias como *The Guardian, The New York Times* e *Reuters* fizeram editoriais[4] extensos acerca do uso indevido de dados pessoais pela empresa norte americana *Facebook Inc*., proprietária da rede social de mesmo nome, que conta atualmente com mais de 1 bilhão de usuários ativos. A matéria diz respeito à manipulação dos dados dos usuários a fim de influenciar o resultado das eleições presidenciais nos Estados Unidos no ano de 2016. A responsável por coletar os dados seria a empresa *Cambrigde Analytica.* Segundo os editoriais, a empresa fez uso de aplicativos de testes psicológicos de personalidade que, para serem liberados, solicitavam a permissão da coleta de dados dos usuários à plataforma do *Facebook.* Não havia, até então, ilegalidade na prática, pois tratava-se de coleta de dados para fins estatísticos ou de estudo. Ocorre que tais dados foram disponibilizados à empresa *Cambrigde Analytica,* empresa que atua no ramo de marketing eleitoral, e a partir disso pode criar propagandas personalizadas aos eleitores com base nas informações obtidas, com a intenção de promover um candidato em detrimento do outro nas eleições presidenciais dos EUA. (FONTES, 2018).

O Facebook, apesar de não ter envolvimento direto no caso, foi o responsável pela coleta inicial dos dados que foram disponibilizados para terceiros, utilizando-se brechas nos contratos de Política de Privacidade (*Privacy Policies*) e de Termos e Condições (*Terms Conditions*) que são disponibilizados para que os usuários façam adesão, mas que por serem muitas vezes extensos e de difícil compreensão, acabam sendo ignoradas pela ampla maioria dos que fazem uso de algum serviço pela internet. A repercussão do caso foi extensa e fez com que várias empresas de tecnologia alterassem seus termos de uso, tornando-os mais claros e objetivos em relação a maneira de como os dados dos usuários são coletados e tratados e para quais fins eles possam ser utilizados. (FONTES, 2018).

---

[3] Para mais informações: THE GUARDIAN. **The NSA Files:** NSA files decoded Edward Snowden's surveillance revelations explained. 2018. Disponível em: <https://www.theguardian.com/us-news/the-nsa-files>. Acesso em: 08 dez. 2018.

[4] Para mais informações: THE GUARDIAN. **The Cambrigde Analytica Files**. 2018. Disponível em: <https://www.theguardian.com/news/series/cambridge-analytica-files>. Acesso em: 08 dez. 2018.

No Brasil, o caso *Cambrigde Analytica* também teve repercussão, de modo que o Ministério Público do Distrito Federal e Territórios – MPDFT, por meio da Comissão de Proteção de Dados Pessoais e pela 1ª Promotoria de Justiça de Defesa do Consumidor, viesse a investigar, em inquérito civil público, se a referida empresa havia usado de forma ilegal os dados pessoais de milhões de brasileiros para elaboração de perfis psicográficos, a fim de que estes dados pudessem predizer: "crenças políticas e religiosas, orientação sexual, cor da pele e comportamento político". (MPDFT, 2018, p. 1). A *Cambrigde Analytica*, segundo o MPDFT (2018), opera no Brasil desde 2017 em parceria com a empresa de consultoria A Ponte Estratégia, Planejamento e Pesquisa LTDA, e tem como foco de atuação a alteração do comportamento das pessoas por meio do uso de dados.

Por fim, tem-se o processo conhecido como *Big data*[5], que orienta uma nova forma de lidar com o exponencial fluxo de dados visto nos dias hodiernos. É que que asseveram Neto; Morais; Bezerra (2018, p. 188):

> Com a massificação do acesso aos computadores nos últimos anos, o custo da tecnologia de armazenamento e processamento diminuiu drasticamente, o que tornou economicamente viável o maior armazenamento de dados por empresas e governos. Além disso, com a atual expansão do *big data*, é cada vez mais vantajoso guardar o máximo de informações possíveis; afinal, mpre podem ser descobertos novos significados a partir de um conjunto de dados aparentemente irrelevante.

Os fatos aqui debatidos que motivam a regulamentação da proteção de dados pessoais não são exaustivos, tendo em vista a veloz e constante evolução das tecnologias da informação que se utilizam da coleta e processamento de dados.

2.3 CENÁRIO INTERNACIONAL DA PROTEÇÃO DE DADOS PESSOAIS

2.3.1 União Europeia

2.3.1.1 Normas anteriores ao Regulamento Geral sobre Proteção de Dados

Após um grande esforço para harmonizar diferentes legislações sobre proteção de dados, a União Europeia aprovou, no ano de 1995, a Diretiva de Proteção de Dados Pessoais (Diretiva 95/46[6]), que trazia uma padronização dos direitos fundamentais dos cidadãos

[5] O termo será tratado com mais detalhes no item 3.3.2.3.

[6] Vide UNIÃO EUROPEIA. DIRECTIVA 95/46/CE DO PARLAMENTO EUROPEU E DO CONSELHO, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**.** 1995. Disponível em: <https://eur-lex.europa.eu/legal-

europeus e da coordenação das Autoridades de Dados Pessoais (ZANATTA, 2018). Em 2000, a Carta de Direitos Fundamentais da União Europeia[7], estabeleceu em seu artigo 8º, que:

> 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.
> 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

2.3.1.2 Regulamento Geral sobre Proteção de Dados

Os mencionados dispositivos jurídicos deram base ao que viria a ser chamado de Regulamento Geral sobre Proteção de Dados – RGPD[8], que entrou em vigor em maio de 2016, revogando a Diretiva 95/46, a qual já não alcançava a nova realidade dos fenômenos aqui já retratados, como *big data*, computação em nuvem, redes sociais etc., que nem sequer existiam na época de elaboração da respectiva Diretiva. O RGPD passou por um período para que as organizações pudessem se ajustar e viabilizar as medidas necessárias para que se enquadrassem ao regulamento supracitado. De tal forma, a regulamentação passou a ser aplicada obrigatoriamente em maio de 2018 aos países que fazem parte da União Europeia. (RAPOSO, 2018).

O RGPD é uma norma que busca harmonizar as leis de proteção de dados dos países da União Europeia, e que executa sem a necessidade de outras normas de transposição, desenvolvimento ou aplicação. As organizações que atuam na União Europeia devem, a partir de então, assumir como norma de referência o RGPD e não mais as normas de proteção de dados pessoais relativas a cada país que compõem o bloco, como estabelecia a Diretiva 95/46. Outrossim, o RGPD contém novas obrigações a serem observadas. (RAPOSO, 2018).

Um dos principais fins do RGPD é justamente a proteção da privacidade das pessoas que se encontram no território dos países membros da União Europeia, em uma realidade em

---

content/PT/TXT/?uri=celex%3A31995L0046>.

[7] Vide UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia.** 2000. Disponível em: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em: 08 dez. 2018.

[8] UNIÃO EUROPEIA. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, 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 (Regulamento Geral sobre a Proteção de Dados)**.** 2018. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 08 dez. 2018.

que as fronteiras físicas foram relativizadas e o ambiente de negócios na internet proporcionou o surgimento de um novo modelo de economia, conforme apontam Ferreira *et al* (2018, p. 01):

> Um dos principais aspectos do GDPR[9] é a preocupação em proteger a privacidade das pessoas (...). Em um ambiente de globalização e economia baseada na internet cada vez mais dependente de dados para se sustentar (*data driven economy*). O ambiente de negócios da internet traz a peculiaridade de mitigar as fronteiras físicas convencionais, produzindo grandes vantagens para a comunicação e comércio eletrônico. Entretanto, a inexistência de fronteiras do mundo digital também apresenta um grande desafio quando se trata da aplicabilidade de normas fora de uma jurisdição.

Conforme aponta estudo da Accenture (2015), 22% da economia mundial é digital[10]. e um dos elementos vitais do funcionamento dessa nova economia é justamente a utilização dos dados pessoais dos cidadãos, sendo utilizado e processado por técnicas automatizadas para definir estratégias de atuação no mercado, sobretudo no que diz respeito a publicidade direcionada. (BIONI, 2018).

Bioni cita que: "Nesse contexto, historicamente, normas de proteção de dados pessoais sempre tiveram a dupla função de não só garantir a privacidade e outros direitos fundamentais, mas também fomentar o desenvolvimento econômico". (BIONI, 2018, p. 106).

Todo esse cenário requer, de forma tão eficaz quanto, a implementação de medidas capazes de conter possíveis violações aos direitos fundamentais, especialmente os de direto da personalidade, como a vida privada, bem como para garantir o livre desenvolvimento econômico no seio da sociedade em rede.

2.3.1.3 Definição de Dados Pessoais no RGPD

O artigo 4º do RGPD traz a definição de Dados Pessoais e de Titular de Dados, ao seu entender:

> Para efeitos do presente regulamento, entende-se por:
> 1) **«Dados pessoais»,** informação relativa a uma pessoa singular identificada ou identificável («**titular dos dados**»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular. (Grifo nosso).

[9] Sigla em inglês de *General Data Protection Regulation.*

[10] Economia digital é o termo que se refere à parte da produção econômica total derivada de várias entradas digitais. Estas entradas incluem habilidades e equipamentos digitais variados. (ACCENTURE, 2015).

Nesse sentido, dado pessoal é a informação que, isoladamente, identifique uma pessoa ou seja capaz de torná-la identificável. Desse modo o RGPD busca evitar generalizações acerca do conceito de dados pessoais e de seus titulares, delimitando-os em seu próprio texto.

2.3.1.4 Princípios relativos ao tratamento de dados pessoais estabelecidos no RGPD

O RGPD lista em seu artigo 5º alguns princípios relativos a proteção de dados que merecem destaque nesse estudo. *In verbis*:

> 1. Os dados pessoais são:
> a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («**licitude, lealdade e transparência**»);
> b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.o, n.o 1 («**limitação das finalidades**»);
> c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («**minimização dos dados**»);
> d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («**exatidão**»);
> e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n.o 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («**limitação da conservação**»);
> f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («**integridade e confidencialidade**»);
> 2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.o 1 e tem de poder comprová-lo («**responsabilidade**»). (Grifo nosso).

Conforme Boardman, Mullock e Mole (2017), tais princípios valorizam ações e papeis no tratamento de dados pessoais, dos quais muitos já eram previstos na Diretiva 95/46, mas que tiveram suas definições e domínios ampliados, de modo a refletir na obtenção do consentimento dos titulares e o total esclarecimento do que é tratamento legítimo desse dados, bem como informar em quais situações será incompatível o tratamento dos dados para uma nova finalidade

diferente daquela acordada na coleta inicial. De forma que a implementação de medidas de segurança da informação dificulte os riscos da quebra de segurança dos dados.

2.3.1.5 Direito de ser esquecido

Outro tema que merece destaque e que possui alta relevância para a discussão dos direitos fundamentais e dignidade da pessoa humana no âmbito da era da informação é o "direito ao apagamento de dados", que se refere ao direito ao esquecimento, e é normatizado no RGPD em seu artigo 17, conforme transcrito abaixo:

> Direito ao apagamento dos dados («**direito a ser esquecido**»)
> 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:
> (...)
> 2. Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.o 1, toma as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos.
> 3. Os n.os 1 e 2 não se aplicam na medida em que o tratamento se revele necessário:
> a) Ao exercício da liberdade de expressão e de informação;
> b) Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento;
> c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9.o, n.o 2, alíneas h) e i), bem como do artigo 9.o, n.o 3;
> d) Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.o, n.o 1, na medida em que o direito referido no n.o 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento; ou
> e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial. (Grifo nosso).

O direito de ser esquecido é um dos pilares da regulamentação da proteção de dados, no tocante a possibilidade de os cidadãos requererem a exclusão de seus dados pessoais das organizações, desde que obedecidos os requisitos para a exclusão.

2.3.2 Estados Unidos da América

2.3.2.1 Legislação esparsa

Os Estados Unidos possuem uma ampla legislação esparsa, tanto em esfera federal como estadual, referente à proteção de dados pessoais. A ideia de regulamentação sobre dados nos Estados Unidos vem desde de a década de 1970, com o advento do *Privacy Act*[11], que estabelece normas acerca da coleta, armazenamento e tratamento das informações dos indivíduos. A referida regulamentação também estabelece a proibição da divulgação dos dados de qualquer pessoa contidos nos sistemas pelas agências detentoras desses registros, exceto pelo consentimento formal (por escrito) daquela. (FONTES, 2018).

A Lei de Privacidade de Comunicação Eletrônica – ECPA[12] (sigla em inglês), promulgada em 1986, proíbe a interceptação de mensagens por telefone ou eletrônicas, como e-mails, seja na transmissão ou no armazenamento. A lei também traz a diferenciação das informações que poderão ser obtidas pelos provedores e o que depende de ordem judicial ou mandado de busca. A referida lei veio sendo atualizada com a evolução da tecnologia da informação para abranger tanto as comunicações analógicas como as digitais. (VALENTE, 2018).

O ECPA subdivide-se em três partes: o *Wiretap Act*, que visa proteger as comunicações em trânsito; o *Stored Communications Act*, que regula os dados armazenados; e *Pen Register Act*, que alcança outros dados específicos. (MESQUITA, 2009). Alguns outros dispositivos de abrangência setorial foram criados, como a Lei de Portabilidade e Transparência de Seguros de Saúde – HIPAA[13] (sigla em inglês), que estabelece padrões de segurança para dados médicos, bem como proibir a utilização e transferência desses dados sem o consentimento do titular. Destaca-se, também, a Lei de Proteção da Privacidade de Crianças – COPPA[14] (sigla em inglês), promulgada em 1998, que estabelece regras de atuação para sites e serviços online, visando a proteção na internet da privacidade de crianças e adolescentes de até 13 anos. (VALENTE, 2018).

2.3.2.2 Lei de Privacidade do Consumidor da Califórnia

[11]Vide ESTADOS UNIDOS DA AMÉRICA. Públic Law 93-579 - Privacy Act. 31 de dezembro de 1974. Disponível em: <https://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf>. Acesso em: 9 dez. 2018.

[12] Vide ESTADOS UNIDOS DA AMÉRICA. Electronic Communications Privacy Act of 1986 (ECPA). Disponível em: <https://it.ojp.gov/privacyliberty/authorities/statutes/1285>. Acesso em: 09 dez. 2018.

[13] Health Insurance Portability and Accountability Act.

[14] Children's Online Privacy Protection Rule.

Por fim, em 28 de junho de 2018, o Estado da Califórnia promulgou a Lei de Privacidade do Consumidor da Califórnia – CCPA[15] (sigla em inglês), uma tentativa dos EUA de uma lei mais abrangente referente à proteção de dados. Ao lado do RGPD na União Europeia, o CCPA é um importante regulamento sobre a proteção de dados no plano internacional, não obstante, o Estado da Califórnia concentra a 5ª maior economia do mundo[16], se fosse um país, estaria à frente do Reino Unido e da França. Além disso, abriga a região conhecida como Vale do Silício, onde se situam empresas como *Alphabet* (Google), *Facebook*, *Apple* e várias outras importantes empresas do ramo de tecnologia, sendo, ainda, um Estado que, comumente, define tendências relacionadas à proteção de dados e privacidade nos EUA. (LA TORRE, 2018).

2.3.2.3 Definição de dados pessoais no CCPA

A definição de dados pessoais no CCPA é significativamente mais ampla que a definição de dados do RGPD. Enquanto este define dado pessoal como "informação relativa a uma pessoa singular identificada ou identificável"[17], aquele declara que

> 1798.140. Para fins deste título:
> (...)
> (o) (1) "Informação pessoal" significa a informação que identifica, descreve, diz respeito a, é capaz de ser associada, ou poderia estar razoavelmente ligada, direta ou indiretamente, a um consumidor particular ou conjunto familiar. Informações pessoais incluem, mas não estão limitadas a:
> (A) Identificadores como nome, endereço postal, identificador pessoal exclusivo, endereço IP, endereço de e-mail, nome da conta, número do CPF, número da carteira de motorista, número do passaporte ou outros identificadores semelhantes.
> (...)
> (D) Informações comerciais, incluindo registros de bens pessoais, produtos ou serviços adquiridos, obtidos ou considerados, ou outros históricos ou tendências de compra ou consumo.
> (E) Informação biométrica.
> (F) Informação de atividade na internet ou em outra rede eletrônica, não limitada a histórico de navegação, histórico de pesquisa e informações sobre a interação de um consumidor com um site da Internet, aplicativo ou anúncio.
> (G) Dados de geolocalização.
> (H) Informações de áudio, eletrônicas, visuais, térmicas, olfativas ou similares.

[15] Vide CALIFORNIA LEGISLATIVE INFORMATION. The California Consumer Privacy Act of 2018. 2018. Disponível em: <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375>. Acesso em: 09 dez. 2018.

[16] Conforme dados do Departamento do Comércio dos Estados Unidos, noticiado em: BUSSINESS INSIDER. **California's economy is now the 5th-biggest in the world, and has overtaken the United Kingdom.** 2018 Disponível em: <https://www.businessinsider.com/california-economy-ranks-5th-in-the-world-beating-the-uk-2018-5>. Acesso em: 09 dez. 2018.

[17] Vide página 15.

> (I) Informações profissionais ou relacionadas ao emprego.
> (...)
> (Tradução nossa).

Observa-se que a definição trazida pela Lei de Privacidade do Consumidor da Califórnia é significativamente mais ampla do que a concepção do Regulamento Geral de Proteção de Dados, fornecendo uma lista extensa de exemplos de informações que devem ser consideradas como pessoais.

2.3.3 Japão

No Japão, o ato nº 57 de 2003 criou o *Act on the Protection of Personal Information*, sofrendo alteração[18] em 2 de dezembro de 2016, que entrou em vigor em 30 de maio de 2017, de modo a se adequar às novas tratativas em relação à proteção de dados, sobretudo à Regulamentação da União Europeia referente ao tema. Em 6 de julho de 2017, a Comissão Europeia e o governo japonês publicaram uma declaração conjunta sobre as transferências internacionais de dados pessoais e reconheceram um ao outro, em acordo[19] firmado em julho de 2018, como países de níveis adequados de proteção de dados, de modo a viabilizar o compartilhamento de dados entre a União Europeia e o Japão.

2.3.4 China

Não existia uma lei abrangente de proteção de dados na República Popular da China. Em vez disso, as regras relacionadas à proteção de dados pessoais eram dispostas em várias leis e regulamentações, assim como ocorria no restante do mundo. No entanto, recentemente, o governo chinês lançou a versão final de um novo padrão nacional de proteção de informações pessoais[20], que passou a vigorar em 1 de maio de 2018, estabelecendo novas regulamentações sobre coleta, armazenamento e compartilhamento de dados, bem como sobre consentimento do usuário no tratamento desses dados, convergindo alguns aspectos trazidos pelo regulamento europeu. (SACKS, 2018).

---

[18] Vide JAPAN. **Amended Act on the Protection of Personal Information.** Disponível em: <https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf>. Acesso em: 09 dez. 2018.

[19] Vide EUROPEAN COMMISSION. The European Union and Japan agreed to create the world's largest area of safe data flows. 2018. Disponível em: <http://europa.eu/rapid/press-release_IP-18-4501_en.htm>. Acesso em: 9 dez. 2018.

[20] Vide CHINA. GB/T 35273-2017. Information security technology—Personal information security specification. Disponível em: <https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr>. Acesso em: 09 dez. 2018.

2.3.5 América Latina

Conforme estudo da organização argentina *Asociación por los Derechos Civiles* (ADC, 2018), Chile, Argentina e México possuem normas específicas concernentes à proteção de dados pessoais, desdobramento do direito à privacidade consagrado em suas respectivas constituições. À época do estudo, o Brasil ainda não havia editado a Lei 13709/2018.

Em comparação ao Regulamento Europeu - RGPD, as leis de Argentina e Chile se demonstram modestas no que se refere aos conceitos de dados pessoais. O mesmo não ocorre com o México, visto que contém em sua lei uma longa lista de conceitos que se aplicam à coleta e processamento de dados, como computação em nuvem, limitação de tratamento e elaboração de perfis. (ADC, 2018).

Por fim, cabe-se destacar a Proposta de Declaração de Princípios de Privacidade e Proteção de Dados Pessoais nas Américas[21], cuja adoção fora feita pela Comissão Jurídica Interamericana da Organização dos Estados Americanos - OEA. A referida Declaração elenca princípios que visam orientar a construção do sistema legal para proteção de dados dos países que compõem a OEA. (ADC, 2018).

[21] Vide OEA. Organización de Estados Americanos. Comité Jurídico Interamericano. Informe del Comité Jurídico Interamericano. Privacidad y Protección de Datos Personales. Disponível em: <http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf>. Acesso em: 10 dez. 2018.

3 LEI Nº 13907/18: LEI GERAL DE PROTEÇÃO DE DADOS

3.1 CONSIDERAÇÕES INICIAIS

Até o advento da Lei Geral de Proteção de Dados, o Brasil dispunha apenas de leis setoriais sobre o tema. Não havia padrão normativo e alguns setores importantes não eram alcançados. Segundo Bioni (2018), a ausência desse padrão normativo gerava insegurança para troca de dados entre os mais diversos ramos produtivos, que compartilham dados entre si para o desenvolvimento de novos modelos de negócios, bem como para a formulação de políticas públicas e parcerias entre órgãos públicos e entidades privadas. Outrossim, não havia uma proteção integral dos dados fornecidos pelos cidadãos aos setores públicos e privados.

A Constituição federal, no art. 170, *caput* e inciso V, estabelece como princípios da ordem econômica a proteção do consumidor e a dignidade da pessoa humana. (BRASIL, 2017). Tal orientação constitucional se reflete nos fundamentos da LGPD, que objetivam proteger os direitos fundamentais e o livre desenvolvimento da personalidade (art. 1º) e o de desenvolvimento econômico tecnológico e da inovação (art. 2º), traçando uma dialética normativa de conciliação desses elementos. (Bioni, 2018).

A materialização de tais objetivos se promove através da possibilidade do cidadão ter amplo controle sobre os seus dados pessoais, seja pelo consentimento do uso de seus dados, seja pela garantia de que o fluxo de dados pessoais atenderá às suas legítimas expectativas, preservando, sobretudo, o livre desenvolvimento da personalidade do titular dos dados.

3.2 PROCESSO LEGISLATIVO

Conforme analisa Reinaldo Filho (2018), Juiz e Doutor em direito, Ex-Presidente do Instituto Brasileiro de Direito da Informática, a entrada em vigor do Regulamento Geral de Proteção de Dados na União Europeia e das demais iniciativas acerca da proteção de dados no plano internacional, bem como o escândalo relacionado aos vazamentos de dados dos usuários do *Facebook* (caso *Cambrigde Analytica*), impulsionaram o desenrolar do Projeto de Lei 4060/2012, que já tramitava há 6 anos no legislativo, para torná-lo na Lei Ordinária 13709/2018, a Lei Geral de Proteção de Dados Pessoais - LGPD, que altera a Lei nº 12.965/2014 (Marco Civil da Internet).

Antes de ser aprovado na Câmara, o texto original da lei passou por sete emendas que foram apresentadas pela Comissão de Ciência e Tecnologia, Comunicação e Informática – CCTCI e pelo Plenário da Casa. Aprovado por unanimidade, em 10 de julho de 2018, pelo

Senado, foi transformado em norma jurídica, após emendas dos Senadores Valdir Raupp (MDB/RO) e Ricardo Ferraço (PSDB/ES), com vetos parciais, em 14 de agosto de 2018, pelo então Presidente Michel Temer, sendo, enfim, publicado no dia 15 do mesmo mês e ano. A lei terá eficácia no território nacional a partir de fevereiro de 2020, de modo que as entidades afetadas pela lei possam se adequar à nova legislação. (BRASIL, 2018a, 2018b).

Dentre os dispositivos da referida Lei que foram vetados pelo Poder Executivo está o inciso II do artigo 23, que estabelecia o seguinte:

> II - sejam protegidos e preservados dados pessoais de requerentes de acesso à informação, nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), vedado seu compartilhamento no âmbito do Poder Público e com pessoas jurídicas de direito privado.

As razões do veto se dão em razão de que o compartilhamento de informações, especialmente àquelas que são definidas na LGPD, são fundamentais para a implementação de diversas atividades e políticas públicas, a exemplo do banco de dados da Previdência Social e do Cadastro Nacional de Informações Sociais, que se utilizam de informações compartilhadas por diversos outros órgãos públicos para o reconhecimento do direito de seus beneficiários e alimentados. Outrossim, o inciso afeta diretamente a viabilidade de investigações no âmbito do Sistema Financeiro Nacional. (BRASIL, 2018a).

O art. 28 da LGPD foi outro dispositivo da referida Lei que sofreu veto. O artigo dispunha que: "a comunicação ou o uso compartilhado de dados pessoais entre órgãos e entidades de direito público será objeto de publicidade, nos termos do inciso I do *caput* do art. 23 desta Lei". O veto foi realizado em razão de que a publicidade irrestrita do compartilhamento de dados pessoais entre os órgãos da administração pública poderia acarretar na dificultação do exercício regular de ações de fiscalização, controle e poder de polícia. (BRASIL, 2018a).

Outro importante veto diz respeito à criação de um órgão regulador nomeado Autoridade Nacional de Proteção de Dados – ANPD, estabelecido nos arts. 55 ao 59. Dentre alguns aspectos trazidos pelos artigos relacionados à ANPD, consta que o órgão seria "integrante da administração pública federal indireta, submetida a regime autárquico especial e vinculada ao ministério da justiça", art. 55, *caput*. Dentre as atribuições da ANPD, elencadas no art. 56, estariam:

> I - zelar pela proteção dos dados pessoais, nos termos da legislação;
> II - zelar pela observância dos segredos comercial e industrial em ponderação com a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;

> III - elaborar diretrizes para Política Nacional de Proteção de Dados Pessoais e da Privacidade;
> IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
> V - atender petições de titular contra controlador;
> VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
> VII - promover estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;
> VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, que deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;
> IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;
> X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, observado o respeito aos segredos comercial e industrial;
> XI - solicitar, a qualquer momento, às entidades do Poder Público que realizem operações de tratamento de dados pessoais, informe específico sobre o âmbito e a natureza dos dados e os demais detalhes do tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento desta Lei;
> XII - elaborar relatórios de gestão anuais acerca de suas atividades;
> XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, assim como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco para a garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;
> XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante, assim como prestar contas sobre suas atividades e planejamento;
> XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; e
> XVI - realizar ou determinar a realização de auditorias, no âmbito da atividade de fiscalização, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluindo o Poder Público.

A observância de possíveis inconstitucionalidades foi a razão do veto à criação da ANPD, tendo em vista que a criação de órgão dessa natureza é de iniciativa privativa do Presidente da República, conforme entendimento do Art. 61, § 1, inc. II, "e", da Constituição Federal de 1988 (BRASIL, 2017), e também pela matéria retratada ser de competência de lei complementar, conforme Art. 37, XIX da CF88.

3.3 CONCEITOS BÁSICOS

3.3.1 Dado pessoal, dado pessoal sensível e dado anonimizado

O inciso I do artigo 5º da LGPD conceitua dado pessoal como “toda informação relacionada a pessoa natural identificada ou identificável”. O conceito é semelhante ao trazido pelo RGPD, não se limitando a nome, idade, endereço físico ou virtual, dados acadêmicos, perfis de compra, ou outro dado qualquer que posso identificar uma pessoa natural viva. (PINHEIRO, 2018).

Já dados pessoais sensíveis (art. 5º, II) são aqueles que estão relacionados a alguma característica individual da personalidade de um indivíduo e suas preferências pessoais, tais como raça ou etnia, religião, posição política, dados de saúde ou vida sexual, dados genéticos ou biométricos, vinculados a uma pessoa natural. (PINHEIRO, 2018).

No art. 5º, III, define-se dado anonimizado como aquele “dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento”.

Segundo Neto; Morais e Bezerra (2017, p. 194):

> Trata-se de uma classificação que cria três níveis de proteção distintos: os dados sensíveis gozarão da maior proteção dentre todos, seguidos pelos dados pessoais e, por fim, pelos dados anônimos. Esses últimos gozam de menor privilégio, uma vez que, supostamente, não seriam capazes de identificar os indivíduos aos quais se referem.

As técnicas de interpretação de dados, geralmente, utilizam dados anonimizados, sendo estes os de maior preponderância nas organizações que se utilizam de dados. Contudo, conforme asseveram Neto; Morais e Bezerra já na análise do anteprojeto da LGPD, a classificação não se justifica no contexto das técnicas de processamento de dados atuais, como Mineração de Dados e *Big Data.* Nesse sentido, os dados não se limitariam a uma classificação delimitada, pois podem assumir características de pessoal, sensíveis ou anônimos, a depender do tipo de análise e aplicação. (NETO; MORAIS e BEZERRA, 2017).

3.3.2 Tratamento de dados

3.3.2.1 Considerações legais

LGPD considera como tratamento de dados (art. 5º, IX):

> 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;

Nesse sentido, tratamento de dados é toda a operação técnica realizada sobre um dado pessoal, em ambiente informatizado ou não. Os responsáveis pelo controle e operacionalização do tratamento de dados são nomeados de "agentes de tratamento" (art. 5º, IX).

3.3.2.2 Mineração de dados

No ambiente informatizado de tratamento (de dados), os dados geralmente são organizados por conjuntos lógicos estruturados em sistemas de bancos de dados, de modo a torná-los mais acessíveis e de fácil utilização. Embora os bancos de dados possam ser manuais (arquivos físicos), o risco de violação dos dados é bem maior quando residem em ambiente informatizado, devido às incontáveis técnicas automatizadas de processamento de dados. (MENDES, 2014).

Uma das técnicas mais utilizadas hoje é a mineração de dados, ou *data mining*, que consiste no processo de transformar dados de difícil compreensão em informações valiosas para empresas, utilizando cominação de dados e estatística. (MENDES, 2014).

Segundo Mendes (2014), a técnica de mineração de dados tem um grande potencial discriminatório, a depender do seu modo de utilização e das tomadas de decisão dos agentes de tratamento, na medida em que a referida técnica pode promover a classificação de pessoas a partir dos dados pessoais armazenados.

Outro aspecto importante é que a técnica de mineração de dados pode converter informações dispersas sobre um indivíduo em dados pessoais sensíveis que orbitam na esfera da intimidade dessa pessoa, dos quais ele esperava que se mantivessem em sigilo. (MENDES, 2014).

Portanto, a legitimidade da técnica dependerá, além do consentimento[22] do usuário, da legitimidade dos fins aos quais ela espera alcançar, respeitando, dentre outros, os direitos à privacidade e autodeterminação informativa.

3.3.2.3 Big Data

A tecnologia da informação possibilitou o acúmulo de um volume descomunal de dados. Hoje em dia é possível armazenar todo o acervo digitalizado da biblioteca de uma escola, por exemplo, em um simples *pendrive.*

O termo *Big Data* (Grandes Dados, em tradução literal) consiste na tecnologia que possibilita que um grande conjunto de dados variados possam ser interpretados para as mais

[22] Abordado no item 2.3.5 desse capítulo.

variadas finalidades, representando o ápice do progresso quantitativo e qualitativo da gestão da informação. (BIONI, 2018).

Uma grande evolução do *big Data,* em comparação com outras metodologias de tratamento de dados, é que o mesmo não necessita que os dados estejam previamente estruturados para serem tratados, eliminando a etapa de estruturação e organização dos dados tornando o processo de tratamento mais veloz. (BIONI, 2018).

Com a aplicação da metodologia do *Big Data,* é possível, por exemplo, construir padrões de reconhecimento para indicar a probabilidade de uma consumidora estar grávida, levando em conta que uma determinada lista de compras é comumente adquirida por clientes gestantes. (LERMAN, 2013).

As redes sociais são responsáveis pela criação de um exponencial volume de dados, especialmente dados pessoais. Cada vez mais as pessoas expõem seus dados e hábitos nesses meios, construindo um grande arcabouço de dados para análise. Nesse panorama, a *Big data,* associado à outras técnicas de estudos comportamentais e estatísticos, é um método que possibilita a construção dos mais variados perfis, sendo de grande valor para aplicação publicitária e outras abordagens. (BIONI, 2018).

3.3.2.4 Proteção de dados sensíveis

Dentre as questões a serem confrontadas pela Lei de Proteção de dados, em relação à mineração de dados e *Big Data,* estão justamente àquelas que poderiam afetar o respeito à privacidade (art. 2º, I), a autodeterminação informativa (art. 2º, II), a inviolabilidade da intimidade, da honra e da imagem (art. 2º, IV), bem como dos direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (art. 2º, VII), construindo um conjunto jurídico de proteção integral das pessoas em relação aos seus dados.

As técnicas de tratamento de dados disponíveis podem identificar dados sensíveis acerca da individualidade das pessoas, tais como raça, orientação sexual e estado de saúde, o que pode pode suscitar práticas discriminatórias ou de diferenciação de um indivíduo. A título de exemplo, um estudo[23] realizado pela Universidade de Cambrigde foi capaz de identificar, com base no número de curtidas em uma determinada rede social, a porcentagem exata de usuários

[23] Vide KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. 2013. Disponível em: <http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf+html>. Acesso em: 10 dez. 2018.

negros e brancos, usuários homossexuais e heterossexuais, e ainda se estes usuários teriam alguma ligação partidária.

> Exatamente por esse motivo leis de proteção de dados pessoas, incluindo a brasileira, dedicam um regime jurídico mais protetivo em relação a dados sensíveis com o intuito de frear práticas discriminatórias. Tal tutela jurídica procura assegurar que o titular dos dados pessoais possa se relacionar e se realizar perante a sociedade, sem que eventuais práticas frustrem tal projeto. (BIONI, 2018, p. 85).

A possibilidade de discriminação ou diferenciação de um indivíduo pelos aspectos de sua personalidade é um importante enfrentamento das normativas acerca de proteção de dados, incluindo a lei em estudo, que se constitui no impedimento do tratamento e exploração de dados pessoais sensíveis de um indivíduo de forma inconsentida e ilegítima.

3.3.3 Anonimização

O inciso XI do art. 5º da LGPD traz o conceito de anonimização para os fins da Lei como sendo o meio adequado para impossibilitar ou dificultar a identificação de um indivíduo por um dado seu, tornando esse dado anonimizado.

Bioni aborda, em seu trabalho intitulado “Proteção de Dados Pessoais - A função e os Limites do Consentimento” (2018, p. 70), as técnicas de “supressão” e “generalização” para ilustrar as implicações normativas de uma possível dicotomia entre dados anonimizados e dados pessoais. Nesse sentido, a “supressão” do CPF seria adequada para diferenciar pessoas que possuem o mesmo nome. Já a “generalização” do nome completo, fazendo uso apenas do prenome, seria uma forma de evitar que um nome pudesse ser associado a um indivíduo, conforme exemplo ilustrado na Tabela 1.

Tabela 1 – Banco de dados relacional com dados anonimizados

Nome	CPF	Faixa etária	Classificação/ segmentação
1. Bruno dos ~~Santoss~~	~~87625362726~~	18>	Jovem Hipster
2. Brunodes ~~Santoss~~	~~12323434545~~	18>	Jovem poupador
3. Brunodes ~~Santoss~~	~~32435678989~~	18>	Jovem consumista
4. Bruna ~~Souza~~	~~34876543243~~	60<	Idosa com rentabilidade
5. Bruna ~~Souza~~	~~23423442344~~	60<	Idosa sem rentabilidade
6. Bruna ~~Scboftdeff~~	~~23242342344~~	60<	Idosa com rentabilidade
7. Maria ~~Souza~~	~~23234242346~~	18<	Adulto desempregado
8. Maria ~~Souza~~	~~53453453456~~	18<	Adulto perfil executivo
9. Maria ~~Sósteness~~	~~54534676588~~	18>	Jovem hipster

Fonte: (BIONI, 2018). Adaptada.

Contudo, segundo o autor, o processo de anonimização de dados tem se mostrado falho, conforme estudo dos pesquisadores Narayanan e Shmatikov (2010). Os pesquisadores criaram um algoritmo que foi capaz de reconhecer dados anonimizados de usuários da plataforma de *streaming* Netflix, na base de dados do site IMDB, que classifica filmes de acordo com as impressões e notas dadas por seus usuários. Os pesquisadores puderam, através do cruzamento dos dados anonimizados da Netflix e de dados do IMDB, por meio das avaliações dos filmes e seus *scorings*, revelar a identidade dos usuários da Netflix.

Portanto, segundo Bioni (2018), o critério da razoabilidade deve ser considerado na classificação de um dado, de modo que a partir do momento que o esforço para resultar um dado anonimizado em dado pessoal se torne irrazoável, não há porquê defini-lo como dado pessoal.

3.3.4 Titular

Conforme o art. 5º, V, da LGPD: "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento".

Segundo Mendes (2014, n.p[24]), na obra "Privacidade, proteção de dados e defesa do consumidor – Linhas Gerais de um novo direito fundamental" as normas que versam sobre proteção de dados no mundo compartilham de uma "concepção procedimental", pela qual "a regulamentação estatal somente deve estabelecer princípios e procedimentos para o tratamento dos dados pessoais, devendo o conteúdo desse direito ser estabelecido pelo titular dos dados pessoais", e continua:

> A garantia de controle do indivíduo sobre as próprias informações é, de fato, uma característica generalizada das diversas legislações nacionais sobre o tema, conforme se percebe a partir das expressões "autodeterminação informativa", consolidada no direito alemão, e "liberdade informática", utilizada no direito espanhol, que expressam a importância que a dimensão da autonomia alcançou na temática da proteção de dados pessoais.

A LGPD estabelece no seu art. 18 os direitos subjetivos que o titular possui em relação aos controladores de seus dados, tais como acesso, correção, anonimização, elimininação (quando cabível), informação sobre compartilhamento, informação sobre a possibilidade de o usuário não fornecer consentimento e suas consequências, revogação do consentimento e outros.

[24] A paginação da obra não é convencional. O excerto foi retirado do item 1.2 – "Regime jurídico de proteção de dados pessoais" do capítulo 1 da parte 1.

3.3.5 Consentimento

Definido pela LGPD como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", art. 5ª, XII. O art. 7, I, estabelece que o tratamento de dados pessoais só poderá ser realizado mediante o fornecimento de consentimento pelo usuário. A dispensa da exigência de consentimento é disciplinada no § 4º do art. 7º, e se refere àqueles dados tornados manifestamente públicos pelo titular. A dispensa de consentimento não desobriga os agentes de tratamento de dados das obrigações impostas pela LGPD (art. 7º, § 6º). O referido consentimento deve ser fornecido pelo titular de forma escrita ou por outro meio que demonstre a manifestação de vontade do titular (art. 8º, *caput*).

O consentimento é um importante vetor da disciplina de proteção de dados, que confere ao indivíduo o poder de autodeterminação informativa, possibilitando ao mesmo a expressão de sua vontade no que diz despeito aos seus dados. Nesse ambiente, o consentimento apresenta diversos aspectos a serem considerados, tais como o não consentimento do indivíduo resultar na exclusão do mesmo do mercado de consumo e da sociedade; da violação dos dados após o consentimento do tratamento; e no que se refere ao consentimento ao tratamento de dados sensíveis. Os problemas citados levam em conta especialmente a possibilidade de que alguns direitos relacionados à personalidade, como a privacidade, serem violados em face ao vício de consentimento, bem como acerca do aspecto de indisponibilidade de alguns desses direitos, sobretudo quando se trata de dados sensíveis, que podem ter carácter potencialmente discriminatório. (MENDES, 2014).

De acordo com Calo (2011), em artigo denominado *Against notice skepticism in privacy (and elsewhere),* o debate em torno do consentimento tem mostrado que o mesmo tem sido um instrumento pouco eficiente no empoderamento dos cidadãos acerca do controle de seus dados, tendo em vista as práticas pouco transparentes e, por vezes manipuladoras, em que os consumidores são submetidos ao consentirem com o tratamento de seus dados. Reflexão que se mantém atual.

Ao analisar a questão do consentimento, no âmbito da LGPD, Bioni (2018, p. 196-197), menciona que:

> Qualquer declaração de vontade deve ter um direcionamento, já que não se consente no vazio e de forma genérica. Seria o equivalente a emitir uma espécie de "cheque em branco" que esvaziaria qualquer esfera de controle do cidadão sobre seus dados. práticos, o famoso "para fins de melhorar a sua experiência", constante de inúmeras políticas de privacidade, deve ser abandonado.

Nesse viés, a LGPD, ao trazer as concepções de “inequivocabilidade” e “finalidades determinadas do consentimento”, busca evitar que o cidadão, ao conceder consentimento para o tratamento de dados, em termos pouco claros e genéricos, esteja de algum modo permitindo o uso desses dados de forma indiscriminada por agentes de tratamento.

3.4 APLICAÇÃO DA LGPD NO PLANO NACIONAL

A LGPD se aplica a organizações públicas ou privadas, pessoas físicas ou jurídicas que executam tratamento de dados pessoais, independentemente do meio e técnica, manual ou automatizada, que possa envolver, ao menos um dos seguintes elementos (art. 3º):

> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

O art. 4 estabelece as hipóteses que não de aplicação da lei, que dizem respeito ao tratamento de dados pessoais realizado para fins exclusivamente particulares e não econômicos, ou aqueles que são de caráter jornalístico e artístico (art. 4º, II, a), acadêmicos (art. 4º, II, b), e , por fim, aqueles para fins exclusivos de segurança nacional (art. 4º, III, a), e defesa nacional (art. 4º, III, b).

Como observado, a exigência de uma lei explícita sobre Proteção de Dados Pessoais em âmbito nacional é consequência do atual plano de ação da sociedade, no qual os dados pessoais são amplamente explorados pelo mercado, em virtude do seu alto valor para a economia digital. (PINHEIRO, 2018).

LGPD também tem alcance fora do território nacional, isto é, impactos no âmbito internacional, visto que se aplica adicionalmente a informações tratadas fora do Brasil, mas que foram coletadas no plano nacional, ou mesmo quando a oferta de um bem ou serviço a pessoas no domínio nacional ou em trânsito no solo brasileiro. Dessa maneira, mesmo os dados pessoais armazenados fora do país (serviços de nuvem, por exemplo), serão tutelados pela Lei de Proteção de dados Brasileira.

CONSIDERAÇÕES FINAIS

A terceira revolução industrial, ou revolução tecnológica, em meados do Sec. XX, foi um marco para o avanço tecnológico que conhecemos atualmente, ao passo que passou a utilizar a tecnologia conjuntamente com sistemas informáticos a fim de ajudar na produção industrial. De tal maneira, nos dias hodiernos, o principal advento da tecnologia é a internet, advento que nos traz informações de maneira impar das mais diferentes vertentes e modos.

Com a senilidade da internet ao passar dos tempos, diversos foram os mecanismos descobertos para que uma população conseguisse aproveita-la de forma que os seus componentes pudessem interagir entre si, de tal maneira, que o fluxo de informações interconectados foi aumentando exponencialmente com o avançar da tecnologia da informação, possibilitando o armazenamento em massa de dados.

Essa realidade foi impactada significativamente pelo advento das redes sociais na internet, que compreendem um conjunto de pessoas (ou empresas ou qualquer outra entidade socialmente criada) que se interligam entre si em conjunto de relações sociais, tais como amizade, relações de trabalho, trocas comerciais ou de informações (SILVA e FERREIRA, 2007). A partir desta concepção, e não única, não é difícil que um indivíduo, ao compartilhar seus dados pessoais, em uma esfera gigante de informações, seja surpreendido pelo uso indevido dessas informações, em um quadro de grave afronta à sua privacidade e à autonomia do desenvolvimento de sua personalidade.

Uma das esferas necessárias à completude humana, além da própria personalidade, são os direitos inerentes à subjetividade, exercida pelo indivíduo independente do comando ou do conhecimento estatal. De tal maneira, a própria Carta Magna de 1988, garante o direito à vida, o direito à liberdade de expressão, à liberdade religiosa, o direito à identidade pessoal e o direito à privacidade – intimidade – de maneira que transgredir informações, acontecimentos ou eventos, que a pessoa deseja manter dentro de seu foro íntimo e que somente a ela interessa ter acesso, viola um direito fundamental do indivíduo. Com isso, insere-se a proteção de dados, sendo explicada como o direito do próprio indivíduo de autodeterminar suas informações pessoais.

No Brasil, promulgada em 2018, a Lei Geral de Proteção de Dados Pessoais – LGPD, que modifica a Lei do Marco Civil, visa proteger os dados pessoais de usuários das mais diferentes plataformas digitais. Nesse contexto, a LGDP busca adequar de forma harmônica a proteção de dados no país, visto que embora já existisse um sistema de proteção à privacidade,

ele era fragmentado e ultrapassado em mais de 40 normas jurídicas do setor financeiro, de saúde, de credito e telecomunicações. (LIMBERGER, 2008).

De tal maneira, a LGDP suprime lacunas existentes no sistema jurídico brasileiro, advindas da fragmentação das normas de proteção aos dados pessoais em leis e da falta de harmonização em uma legislação unificada. Por conta disso, torna-se um dispositivo impar para os usuários, visto que o contexto de desenvolvimento de novas tecnologias e de transformação digital tem estado em contexto e sendo consolidada ao longo dos anos. Com isso, por prever mecanismos de tutela e uma Autoridade Nacional, a LGDP, traz segurança jurídica, desenvolvendo novos mercados no Brasil e colocando o país em níveis considerados adequados para cooperações econômicas e transições que envolvam o compartilhamento de dados.

REFERÊNCIAS

ACCENTURE. **Digital disruption: The growth multiplier**. 2015. Disponível em: <https://www.accenture.com/t00010101T000000Z__w__/br-pt/_acnmedia/PDF-14/Accenture-Strategy-Digital-Disruption-Growth-Multiplier-Brazil.pdf>. Acesso em: 09 dez. 2018.

ADC. Asociación por los Derechos Civiles. **El Sistema de Protección de Datos Personales en América Latina. Volume 1**. 2017. Disponível em: <https://adcdigital.org.ar/wp-content/uploads/2017/06/Sistema-proteccion-datos-personales-LatAm.pdf>. Acesso em: 10 dez. 2018.

ALCALÁ, Humberto Nogueira. Autodeterminación informativa y hábeas data em Chile en información comparativa. **Anuario de Derecho Constitucional Latinoamericano**, México, tomo II, 2005. Disponível em: <https://revistas-colaboracion.juridicas.unam.mx/index.php/anuario-derecho-constitucional/article/view/30267/27321>. Acesso em: 10 dez. 2005.

AGUIAR, Rodrigo Goulart. A nova face dos direitos à intimidade e à vida privada na ordem jurídica nacional: os primeiros passos rumo à tutela de dados e à autodeterminação informativa. A&C: **Revista de Direito Administrativo e Constitucional**, Belo Horizonte, a. 3, n. 11, jan./mar. 2003.

BARROS, Clarissa Teresinha Lovatto. **Direito à informação x proteção de dados pessoais**: a publicação de decisões judiciais em casos de pornografia envolvendo crianças e adolescentes. 2017, 113 f. Dissertação (Mestrado em Direito) - Universidade Federal de Santa Maria, Santa Maria, RS, 2017.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2018.

BOARDMAN, Ruth; MULLOCK, James; MOLE, Ariane. **Bird & Bird & guide to the General Data Protection Regulation**. 2017. Disponível em: <https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf>. Acesso em: 8 dez. 2018.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**: texto constitucional promulgado em 5 de outubro de 1988, com as alterações determinadas pelas Emendas Constitucionais de Revisão nºs 1 a 6/94, pelas Emendas Constitucionais nºs 1/92 a 96/2017 e pelo Decreto Legislativo nº 186/2008. Brasília, DF: Senado Federal, Coordenação de Edições Técnicas, 2017.

_____. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). 2018a. Disponível em: <http://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-publicacaooriginal-156212-pl.html>. Acesso em: 10 dez. 2018.

_____. Projeto de Lei da Câmara n° 53, de 2018. 2018b. Disponível em: < https://www25.senado.leg.br/web/atividade/materias/-/materia/133486>. Acesso em: 10 dez. 2018.

BUSSINESS INSIDER. **California's economy is now the 5th-biggest in the world, and has overtaken the United Kingdom**. 2018 Disponível em: <https://www.businessinsider.com/california-economy-ranks-5th-in-the-world-beating-the-uk-2018-5>. Acesso em: 09 dez. 2018

CALIFORNIA LEGISLATIVE INFORMATION. **The California Consumer Privacy Act of 2018**. 2018. Disponível em: <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375>. Acesso em: 09 dez. 2018.

CALO, Ryan. Against notice skepticism in privacy (and elsewhere). **Notre Dame lawreview**, v. 87, n. 3, march, 2011. p. 1027-1072.

CASTELLS, Manuel. **A Era da Informação**: economia, sociedade e cultura. Vol. I: A Sociedade em rede. Trad.: Klauss Brandini Gerhardt e Roneide Venâncio Majer. 2. ed. São Paulo: Paz e Terra, 2000.

CERVO, A. L.; BERVIAN, P. A.; SILVA, R. **Metodologia científica. 6. ed**. São Paulo: Pearson Prentice Hall, 2007.

CHINA. GB/T 35273-2017. **Information security technology—Personal information security specification**. Disponível em: < https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr>. Acesso em: 09 dez. 2018.

CUNHA, Mauro Leonardo. **Comentários à Lei Geral de Proteção de Dados**: Essencial para Profissionais do Mercado, do Mundo da TI e, da Gestão de Riscos e Seguros, da Comunidade de ... Brasileiro Livro 1) (Locais do Kindle 331-334). Edição do Kindle.

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

EUROPEAN COMMISSION. **The European Union and Japan agreed to create the world's largest area of safe data flows**. 2018. Disponível em: <http://europa.eu/rapid/press-release_IP-18-4501_en.htm>. Acesso em: 9 dez. 2018.

FERREIRA, Ricardo Barretto et al. **Entra em vigor o Regulamento Geral de Proteção de Dados da União Europeia**. 2018. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI281042,81042-Entra+em+vigor+o+Regulamento+Geral+de+Protecao+de+Dados+da+Uniao>. Acesso em: 08 dez 2018.

FONTES, José Igor Alves**. Dados pessoais digitais e seu tratamento no ordenamento jurídico brasileiro**. 2018, 47 f. Monografia (Graduação em Direito) – Universidade Federal do Rio Grande do Norte, Natal, 2018.

JAPAN. **Amended Act on the Protection of Personal Information**. Disponível em: <https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf>. Acesso em: 09 dez. 2018.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. **Private traits and attributes are predictable from digital records of human behavior**. 2013. Disponível em: <http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf+html>. Acesso em: 10 dez. 2018.

LA TORRE, Lydia de. **GDPR matchup:** The California Consumer Privacy Act 2018. 2018. Disponível em: <https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/>. Acesso em: 09 dez. 2018.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011.

LERMAN, Jonas. Big Data and Its Exclusions. **Stanford Law Review Online**, v. 66, Sept. 2013. Disponível em: <http://ssrn.com/abstract=2293765>. Acesso em: 11 dez. 2018.

LIMBERGER, TÊMIS. Proteção dos dados pessoais e comércio eletrônico: os desafios do século XXI. **Revista de Direito do Consumidor: RDC**, São Paulo, v. 17, n. 67, p. 217-241, jul./set. 2008

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDONÇA, Fernanda Graebin. **O direito à autodeterminação informativa: a (des)necessidade de criação de um novo direito fundamental para a proteção de dados pessoais no brasil.** 2014. Disponível em: <https://online.unisc.br/acadnet/anais/index.php/sidspp/article/viewFile/11702/1571>. Acesso em: 11 dez. 2018.

MESQUITA, Rodrigo Octávio de Godoy Bueno Caldas. **A proteção da privacidade nas comunicações eletrônicas no Brasil**. 2009, 333 f. Dissertação (Mestrado em Direito) –

Universidade de São Paulo – USP, São Paulo, 2009.

MPDFT. Ministério Público do Distrito Federal e Territórios. **MPDFT investiga uso ilegal de dados pessoais de brasileiros disponíveis no Facebook**. Disponível em: <http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/noticias/noticias-2018/9910-mpdft-vai-investigar-uso-ilegal-de-dados-de-brasileiros-disponiveis-no-facebook-por-empresa-americana>. Acesso em: 10 dez. 2018.

MORGADO, Laerte Ferreira. O cenário internacional de proteção de dados pessoais. Necessitamos de um Código Brasileiro? **Âmbito Jurídico**, Rio Grande, XII, n. 65, jun. 2009. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=6336>. Acesso em: 09 dez 2018.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Myths and Fallacies of "Personally Identifiable Information". **Ċommunications of the ACM,** v. 53, n. 06, p. 24, June 2010. Disponível em: <www.cs.utexas.edu/~shmat/shmat_cacm10.pdf>. Acesso em 10. dez. 2018.

NETO, Elias Jacob de Menezes; MORAIS, Jose Luis Bolzan de; BEZERRA, Tiago José de Souza Lima. O projeto de lei de proteção de dados pessoais (PL 5276/2016) no mundo do big data: o fenômeno da *dataveillance* em relação à utilização de metadados e seu impacto nos direitos humanos. **Rev. Bras. Polít. Públicas**, Brasília, v. 7, nº 3, 2017 p. 184-198

OEA. Organización de Estados Americanos. Comité Jurídico Interamericano. **Informe del Comité Jurídico Interamericano. Privacidad y Protección de Datos Personales**. Disponível em: <http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf>. Acesso em: 10 dez. 2018.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais - Comentários à Lei n. 13.709/2018 LGPD**. São Paulo: Saraiva 2018.

RAPOSO, Jorge Nunes. **O novo regime de proteção de dados pessoais na união europeia**. 2018. Disponível em: <https://books.google.com.br/books?id=bwdMDwAAQBAJ&printsec=frontcover&hl=pt-BR>. Acesso em: 08 dez. 2018.

REINALDO FILHO, Demócrito. Lei de proteção de dados pessoais aproxima o Brasil dos países civilizados. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 23, n. 5498, 21 jul. 2018. Disponível em: <https://jus.com.br/artigos/67668>. Acesso em: 11 dez. 2018.

RODOTÀ, Stefano. **A vida na sociedade da vigilância** (coord. Maria Celina Bodin de Moraes). Rio de Janeiro: Renovar, 2008.

SACKS, Samm. **New China Data Privacy Standard Looks More Far-Reaching than**

GDPR. 2018. Disponível em: <https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr>. Acesso em: 09 dez. 2018.

SCHWARTZ, P. The Computer in German and American Constitucional Law. **American Journal of Comparative Law**. v. 37, p. 675-705, 1989. Disponível em: <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1865&context=facpubs>. Acesso em: 11 dez. 2018.

SILVA, A.; FERREIRA, M. Gestão do conhecimento e capital social: as redes e sua importância para as empresas. **Informação & Informação**, Londrina, v. 12, n. esp., 2007.

THE GUARDIAN. **The Cambrigde Analytica Files**. 2018. Disponível em: <https://www.theguardian.com/news/series/cambridge-analytica-files>. Acesso em: 08 dez. 2018

_____. **The NSA files:** NSA files decoded Edward Snowden's surveillance revelations explained. Disponível em: <https://www.theguardian.com/us-news/the-nsa-files>. Acesso em: 08 dez. 2018.

UE. União Europeia. **Carta dos Direitos Fundamentais da União Europeia.** 2000. Disponível em: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em: 08 dez. 2018.

_____ Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**.** 1995. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>.

_____. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, 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 (Regulamento Geral sobre a Proteção de Dados). 2018. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 08 dez. 2018.

UNITED STATES OF AMÉRICA. **Electronic Communications Privacy Act of 1986 (ECPA)**. Disponível em: <https://it.ojp.gov/privacyliberty/authorities/statutes/1285>. Acesso em: 09 dez. 2018.

_____. **Públic Law 93-579 - Privacy Act. 31 de dezembro de 1974.** Disponível em: <https://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf>. Acesso em: 9 dez. 2018.

VALENTE, Jonas. **Legislação de proteção de dados já é realidade em outros países.** 2018. Disponível em: <http://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises>. Acesso em: 09 dez. 2018.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, vol. IV, n. 5, p. 193-220, Dec. 1890.

WESTIN, Alan. **Privacy and freedom**. New York: Atheneum, 1970.

ZANATTA, Rafael A. F. **Proteção de dados pessoais como regulação do risco**: uma nova moldura. 2017. Disponível em: <http://www.redegovernanca.net.br/public/conferences/1/anais/ZANATTA,%20Rafael_2017.pdf>. Acesso em: 11 dez. 2018.