Centro Universitário de Brasília – UniCEUB
Faculdade de Ciências Jurídicas e Sociais – FAJS
Curso de Bacharelado em Direito

MARIA CLARA FERREIRA SANTIAGO

A TUTELA DOS DADOS PESSOAIS DO ACUSADO NO BRASIL:
Análise da viabilidade de fornecimento do consentimento do titular dos dados para atividades de investigação e repressão de infrações penais

BRASÍLIA
2020

MARIA CLARA FERREIRA SANTIAGO

A TUTELA DOS DADOS PESSOAIS DO ACUSADO NO BRASIL:
Análise da viabilidade de fornecimento do consentimento do titular dos dados para atividades de investigação e repressão de infrações penais

Artigo científico apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais – FAJS do Centro Universitário de Brasília – UniCEUB.

Orientador (a): Professor Msc. Víctor Minervino Quintiere

BRASÍLIA
2020

MARIA CLARA FERREIRA SANTIAGO

A TUTELA DOS DADOS PESSOAIS DO ACUSADO NO BRASIL:
Análise da viabilidade de fornecimento do consentimento do titular dos dados para atividades de investigação e repressão de infrações penais

Artigo científico apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais – FAJS do Centro Universitário de Brasília – UniCEUB.

Orientador(a): Professor(a) Nome completo

Brasília-DF, de de 2020.

BANCA AVALIADORA

_____

Msc. Víctor Minervino Quintiere
Professor Orientador

_____

Professor (a) Avaliador (a)

A TUTELA DOS DADOS PESSOAIS DO ACUSADO NO BRASIL: Análise da viabilidade de fornecimento do consentimento do titular dos dados para atividades de investigação e repressão de infrações penais

Maria Clara Ferreira Santiago

RESUMO: O presente trabalho tem por objetivo estudar a efetividade da Lei Geral de Proteção de Dados Pessoais, especificamente no mecanismo de tutela das garantias do acusado submetido às intervenções penais e, por consequência, não sujeito as ingerências da lei. O trabalho irá percorrer um aspecto temporal entre as legislações vigentes no Brasil, essencialmente aquelas que versaram sobre a tutela dos dados pessoais e, também, as que se limitaram a tratar da proteção ao direito à privacidade. Prosseguindo, a pesquisa irá se dedicar sobre situações que envolveram o vazamento de dados em âmbito nacional e internacional. Passará, então, para a análise do *General Data Protection,* instituído no ordenamento jurídico europeu, e da própria Lei Geral de Proteção de Dados Pessoais. Ao final, analisará a viabilidade de fornecimento do consentimento sob a ótica do direito penal, para o acesso dos dados pessoais de um acusado, à luz das garantias constitucionais da privacidade e da não autoincriminação.

Palavras-Chave: Lei Geral de Proteção de Dados Pessoais. Tratamento de dados. Persecução. Atividades de investigação e repressão de infrações penais. Penal. Consentimento. Direito à privacidade. Direito à não autoincriminação. Garantias constitucionais. Acusado.

INTRODUÇÃO

O tratamento dos dados pessoais no ordenamento brasileiro teve ascensão tardia. Malgrado algumas normativas versarem sobre a tutela do direito e da garantia individual da privacidade, foi só com a introdução da Lei do Marco Civil da Internet que se falou, pela primeira vez, em proteção de dados pessoais na legislação.

No entanto, apenas com a Lei Geral de Proteção de Dados Pessoais, sancionada no ano de 2018, pelo presidente em exercício à época, Michel Temer, é que se deu atenção à tutela dos respectivos dados, tendo como principal inspiração no ordenamento jurídico internacional o Regulamento Geral 679/2016, da União Europeia.

A lei trouxe uma série de definições para sua melhor compreensão e diversas medidas para o tratamento dos dados pessoais, tendo como principais fundamentais aqueles dispostos em seu art. 2º, trançando como princípio basilar o respeito à privacidade. Contudo, a temática excetuou a hipótese de tutela dos dados pessoais quando voltados para atividades de investigação e repressão de infrações penais.

Nesta perspectiva é que se dá o objeto central de questionamento do presente trabalho, de modo a investigar a viabilidade de aplicação dos mecanismos da lei geral de proteção de dados pessoais à tutela de dados do acusado no âmbito do direito penal, ainda que seu art. 4º tenha restringido essa aplicação, especificamente à possibilidade de fornecimento do consentimento para o acesso e tratamento dos dados pessoais por parte daquele submetido à atividades de investigação e repressão penal.

A relevância de estudo do tema se dá pela necessidade de observância sobre como o ordenamento jurídico irá se comportar, mais precisamente, em razão da omissão da lei geral aos procedimentos de investigação de criminal a partir de sua entrada em vigor, que acontecerá no ano de 2020.

Pela recente positivação da legislação, ainda em estágio de *vacatio legis*, a originalidade do trabalho recai sobre a baixa produção acadêmica do tema e pela indispensabilidade do tratamento dos dados pessoais no ambiente criminal.

A pesquisa irá se inclinar, de início, no contexto histórico que culminou na produção da Lei Geral de Proteção de Dados Pessoais dentro do ordenamento brasileiro, desde a Constituição Federal de 1988 até a instituição da lei supramencionada. Ademais, irá abordar casos emblemáticos, a nível nacional e internacional, sobre vazamento de dados, por meio da pesquisa dogmática e histórica.

Em seu segundo capítulo, o presente trabalho analisará o Regulamento Geral da União Europeia e a Lei Geral de Proteção de Dados Pessoais, em aspectos gerais, à luz do direito comparado. Neste viés, cumpre destacar que o trabalho não pretende esgotar, de forma integral, as legislações dispostas acima e sim afunilar os principais conceitos para a concepção do objeto central do estudo. Assim, se dará especial atenção ao instituto do consentimento, um dos requisitos principais para o referido tratamento.

Para só então, no último capítulo, debruçar-se sobre o objeto central do trabalho: as questões da lei geral sob a ótica da seara penal, as implicações do consentimento e os aspectos intrínsecos ao direito à privacidade e ao direito à não autoincriminação, partindo de um método de pesquisa bibliográfica e de um método de abordagem hipotético-dedutivo para correlacionar todos os institutos estudados separadamente, chegando a uma conclusão particular.

1 CONTEXTO HISTÓRICO

A instituição de leis que tratassem da proteção de dados pessoais percorreu quatro gerações, conforme leciona Bioni (2018). A primeira geração decorreu da preocupação com o processo massivo dos dados do cidadão em meio a formação do Estado Moderno, tendo, como principal enfoque, a determinação de controle rígido da utilização da internet pelos entes governamentais.

Já na segunda geração, a atenção, que era voltada para as bases de dados pessoais estatais, estendeu sua preocupação à esfera privada, transferindo ao titular dos dados a responsabilidade de protegê-los. A terceira geração tratou, a fundo, do titular dos dados, estabelecendo sua participação no tratamento, desde a coleta até o compartilhamento de suas informações, de acordo com o mesmo autor.

A quarta geração, em que se insere a lei geral brasileira, objetivou sanar a deficiência de todas as legislações das gerações anteriores, atuando na criação de autoridades que regulassem o tratamento dos dados pessoais, além de relativizar a centralidade do consentimento, mas sem eliminar o protagonismo que lhe foi conferido (BIONI, 2018).

O Brasil se manteve silente quanto ao tema por muitos anos. Contudo, alguns marcos temporais foram relevantes para o início do tratamento: a Constituição Federal de 1988, prevendo a garantia constitucional a privacidade; os fóruns internos do MERCOSUL, em 2005, com debates intrínsecos a proteção de dados pessoais e; o debate público realizado pelo Ministério da Justiça, no ano de 2010, sobre o anteprojeto da lei de proteção de dados (DONEDA, 2018, p. 310).

A Lei Geral de Proteção de Dados Pessoais (LGPD) foi instituída no ordenamento jurídico brasileiro sob a Lei nº 13.709, de 14 de agosto de 2018. Em meados de maio de mesmo ano entrava em vigor na Europa o *General Data Protection Regulation*, o Regulamento Geral

de Proteção de Dados nº 679/2016, que influenciava diretamente na produção da legislação brasileira.

A instituição da lei geral teve início no Projeto de Lei nº 53, de 2018, no Senado Federal, e no Projeto de Lei nº 4.060, de 2012, na Câmara dos Deputados. O projeto de lei foi de iniciativa do Deputado Federal Milton Antônio Casquel Monti, integrante do Partido Liberal, antigo Partido da República.

A justificativa para a rápida mobilização em prol da aprovação do projeto de lei, em caráter de urgência, foi o vazamento de dados em países estrangeiros, onde fora constatado que "o tema mobilizou o Congresso principalmente depois do vazamento de dados dos usuários do Facebook, uma das maiores redes sociais, coletados pela empresa Cambrigde Analytica e usados nas últimas eleições nos Estados Unidos" (AGÊNCIA SENADO, 2018).

E, também, no território nacional já que, em 2018, o Ministério Público do Distrito Federal e Territórios denunciou uma suposta comercialização de dados pessoais por uma empresa pública federal de processamento de dados (AGÊNCIA SENADO, 2018).

A necessidade de tratamento sobre o tema "dados pessoais" se deu permeada por diversos episódios que culminaram em sua regulamentação em vários países. Na percepção de Quintiere (2019, p. 180):

> A proteção de dados tem relevo não apenas com a edição da referida norma, como também em outros Países. Na Europa, foi editado o General Data Protection Regulation (GDPR), o qual passou a ser obrigatório em 25 de maio de 2018 e aplicável a todos os países da União Europeia (UE). Já em solo norte-americano, foi editado o California Consumer Privacy Act of 2018 (CCPA), aprovado em 28 de junho de 2018 (AB 375).

Além das normas instituídas no cenário internacional, principalmente o Regulamento da União Europeia, que refletiu na produção da lei de proteção de dados, destacaram-se casos de relevo sobre violação de dados pessoais como o escândalo da *Cambridge Analytica*, na campanha de Donald Trump, presidente eleito nos Estados Unidos no ano de 2016, bem como a intervenção da mesma empresa no processo do *Brexit*, na Europa. Já nacionalmente, também no ano de 2018, noticiava-se o suposto vazamento de dados pessoais pelo Serviço Federal de Processamento de Dados (SERPRO).

Sobre a incidência internacional, a *Cambridge Analytica* se tornou protagonista de um dos maiores vazamentos de dados. A empresa foi fundada no ano de 2013, como sendo um

desdobramento da SCL Group, *Strategic Communication Laboratories,* que tinha como diretor executivo Alexander Nix. Além da Campanha de Donald Trump, a empresa atuou, também, no *Brexit*, saída do Reino Unido da União Europeia.

Especificamente sobre a eleição de Donald Trump, o caso da *Cambridge Analytica* foi um dos notórios que mais exigiu positivação da tutela dos dados pessoais. O escândalo que envolveu o *Facebook* foi noticiado no ano de 2018 pelos jornais estrangeiros *The Guardian* e *The New York Times.*

De acordo com o *The New York Times* (2018), a *Cambridge Analytica* adquiriu o acesso a dados de cerca de 50 milhões de usuários do *Facebook.* A coleta de dados pessoais foi o ponto chave para traçar a personalidade de propensos eleitores com base nas "curtidas", nos compartilhamentos, nas amizades e, até mesmo, nas características pessoais dos usuários, de modo a criar grupos de público-alvo a serem atingidos por publicidades específicas.

A compra de dados dos usuários do *Facebook* foi relatada por Christopher Wylie, ex-diretor de tecnologia da *Cambridge Analytica*. Segundo Wylie à Pablo Guimón, correspondente do *EL PAÍS* (2018), os dados foram obtidos por meio do aplicativo *thisisyourdigitallife*, que avaliava o perfil psicológico do usuário, desenvolvido por um pesquisador da Universidade de Cambridge. O aplicativo ainda permitia o alcance das redes de amizades dos usuários.

O ex-diretor de operações de plataforma do *Facebook*, Sandy Parakilas, que atuou na direção da rede social nos anos de 2011 e 2012 afirmou que, na época em que atuava como diretor o *Facebook*, já não se tinha controle sobre o fluxo de dados dos usuários e, muito menos, de que maneira esses dados eram utilizados. A crítica feita por Parakilas, perceptível nos anos de 2011 e 2012 foi contemporânea ao cenário do ano de 2018 (GUIMON, 2018).

Com relação ao *Brexit*, movimento de saída do Reino Unido da União Europeia, de acordo com Wylie ao *EL PAÍS* (2018), em entrevista concedida, o movimento não teria ocorrido sem a influência da empresa visto que "o referendo foi ganho com menos de 2% dos votos e muito dinheiro foi gasto em publicidade na medida certa, com base em dados pessoais".

Tais eventos acarretaram no fechamento da *Cambridge Analytica* em maio de 2018 (EL PAÍS, 2018), tendo sido registrado pedido de falência perante os Estados Unidos em decorrência dos prejuízos financeiros que a empresa sofreu após o estopim dos acontecimentos.

Já em território nacional fora noticiado, no ano de 2018, o suposto vazamento de dados por parte do Serviço Federal de Processamento de Dados, SERPRO. Teria sido apontado o repasse de informações ao site Consulta Pública, oriundas de dados da Receita Federal (COELHO, 2018).

O Ministério Público do Distrito Federal e Territórios, por meio da Comissão de Proteção dos Dados Pessoais, no ofício sob o nº 20/2018, noticiou à Procuradoria da República no Distrito Federal sobre a prática de extração de documentos de Cadastro de Pessoas Físicas (CPF) e de Cadastro Nacional da Pessoa Jurídica (CNPJ). O Despacho Ministerial ratificou que a venda de informações dos titulares dos dados era uma prática comum, feita, até mesmo, pela administração pública, direta e indireta.

Do que consta do ofício produzido pelo Promotor de Justiça, Frederico Meinberg Ceroy, a comercialização de dados pessoais pela empresa consistia na venda e disponibilização de "nome completo; número de inscrição no CPF; data de nascimento; sexo; nome completo da mãe; número do título de eleitor; endereço completo do domicílio fiscal; situação da inscrição no CPF e data do óbito" (MINISTERIO PUBLICO DO DISTRITO FEDERAL E TERRITÓRIOS, 2018).

No ano de 2019, o Ministério Público constatou novas irregularidades nos procedimentos adotados pela empresa, agora no serviço *Datavalid* envolvendo o programa de dados da Carteira Nacional de Habilitação (CNH) utilizado pelo Departamento Nacional de Trânsito, o DENATRAN (MINISTERIO PUBLICO DO DISTRITO FEDERAL E TERRITÓRIOS, 2019).

Na representação apresentada perante o Tribunal de Contas da União, a Procuradora-Geral de Justiça, Fabiana Costa, afirmou que o SERPRO, através do *Datavalid*, fazia o tratamento ilegal das informações advindas do DENATRAN, que dizia respeito a dados pessoais e a, também, dados sensíveis. Nos termos da representação protocolada:

> O serviço comercializado consiste em validar a identidade das pessoas por meio de sua biometria (impressões digitais e reconhecimento facial), sendo disponibilizado a entidades públicas, privadas e de classe, tais como instituições financeiras, locadoras de veículos, aplicativos, companhias aéreas, seguradoras, *e-commerces*, empresas de tecnologia, empresas de varejo, dentre outros (MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS, 2019, p. 2).

Com a implementação da plataforma digital *Datavalid* e o fornecimento de dados da CNH sem o consentimento ou mesmo conhecimento de seus titulares, a empresa pública estaria atuando em constante violação aos ditames do Marco Civil da Internet e a da Lei Geral de Proteção de Dados Pessoais (MINISTERIO PUBLICO DO DISTRITO FEDERAL, 2019).

Apesar dos acontecimentos que envolveram a *Cambridge Analytica* e o SERPRO, terem sido os mais noticiados e servirem de motivação para a confecção da lei geral, houve vários outros que compreenderam o vazamento de dados em larga escala. O pesquisador de segurança da Avast, Martin Hron (2019), listou os 10 maiores vazamentos ocorridos no ano de 2018 ao redor do mundo. Em uma listagem crescente de afetados com os vazamentos, os números variaram entre 37 milhões e 1 bilhão.

A legislação anterior à lei geral já tinha previsão sobre o tratamento dos dados pessoais. O Marco Civil da Internet, assentado pela Lei nº 12.965, de 23 de abril de 2014, cuja revogação de alguns dispositivos deu-se com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais, tinha definido como princípio norteador da utilização da internet, em seu art. 3º, III, a proteção dos dados pessoais (BRASIL, 2014).

Em que pese o Marco Civil da Internet ter sido a primeira legislação a tratar dessa proteção, a Lei de Acesso à Informação, nº 12.527/2011, em seu art. 31, *caput*, na seção responsável por tratar das informações pessoais, dispunha sobre a necessidade de transparência e respeito à intimidade, vida privada, honra e imagem pessoal, liberdades e garantias individuais durante o tratamento das informações pessoais (BRASIL, 2011).

O Código de Defesa do Consumidor (BRASIL, 1990), previu em seu art. 43, o direito "acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes".

As normativas, anteriormente mencionadas e, recepcionadas pela Constituição Federal de 1988, buscaram abranger os dados pessoais apesar de não entrarem afundo no tema. Neste sentido, vale destacar que a Carta Magna já enunciava, à título de garantias fundamentais, a tutela da intimidade, da privacidade, bem como a inviolabilidade dos dados, de acordo com os incisos X e XII, de seu art. 5º (BRASIL, 1988).

2 DIREITO COMPARADO: ANÁLISE DAS NORMATIVAS FUNDANTES E DOS PRINCÍPIOS BASILARES DO REGULEMANTO EUROPEU E A DA LEI GERAL BRASILEIRA

A elevada ruptura à privacidade dos dados pessoais na internet exigiu, por parte dos organismos de proteção de diversos países, o tratamento do tema em seus respectivos ordenamentos jurídicos. O pioneirismo no debate aconteceu na Europa, na Diretiva 95/46/EC, relativa à proteção de dados pessoais das pessoas singulares e à livre circulação desses dados.

O *General Data Protection Regulation* ou Regulamento Geral de Proteção de Dados, foi instituído pelo Regulamento (UE) 679/2016, substituindo a Diretiva Europeia 95/46/CE. O referido regulamento "estabelece as regras relativas ao tratamento, por uma pessoa, uma empresa ou uma organização, de dados pessoais relativos a pessoas na UE" (UNIÃO EUROPEIA, 2016).

A proteção dos dados pessoais teria mais espaço nos ordenamentos jurídicos na hipótese de tratamento via tratado internacional, observando que os fluxos de dados ultrapassam fronteiras geográficas. A União Europeia, no entanto, obteve êxito em reunir, em um único regulamento, o *General Data Protection Regulation*, normativas sobre o tema, alcançando todos os seus 28 Estados-membros (PINHEIRO, 2018, p. 37).

Aprovado em 06 de abril de 2016, o Regulamento entrou em vigor no ordenamento europeu só após o período transição, estabelecido com final em 25 de maio de 2018: "para dar tempo aos Estados-Membros e às partes interessadas de se prepararem devidamente para o novo quadro jurídico", conforme preconizou a Comunicação da Comissão ao Parlamento Europeu e ao Conselho (2016).

O regulamento influenciou diretamente na produção da legislação brasileira, tendo sido sancionada, também, no ano de 2018:

> A lei brasileira possui trajetória peculiar em relação a outras leis latino-americanas de proteção de dados. Tendo sido sancionada no mesmo ano da entrada em vigor do Regulamento Europeu de Proteção de Dados (GDPR) e da revisão da Convenção 108 do Conselho da Europa, é um das primeiras normativas da região a ter sentido a influência mais direta do GDPR, ao mesmo tempo em que reflete fortemente características próprias do ordenamento jurídico brasileiro. Estes elementos derivam diretamente da forma com que a sua redação foi trabalhada desde o seu início. (DONEDA, 2018, p. 309).

Algumas diretrizes estabelecidas no Regulamento 679/2016 do Parlamento Europeu e do Conselho, ressaltaram a tutela dos dados pessoais. No considerando de nº 1, se estabeleceu que o tratamento de dados pessoais é um direito fundamental, com o devido respaldo na Carta dos Direitos Fundamentais da União Europeia e no Tratado sobre o Funcionamento da União Europeia. Ambas legislações garantiram as pessoas o direito à proteção de seus dados.

O Regulamento trouxe princípios basilares e universais para o tratamento da proteção dos dados em todo o território da União Europeia, conforme o considerando de nº 2:

> Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais.
>
> O presente regulamento tem como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares. (UNIÃO EUROPEIA, 2016).

No que tange à aplicação do *General Data Protection Regulation*, o legislador estrangeiro tangenciou seu alcance como sendo apenas para as pessoas singulares, sem abranger as chamadas pessoas coletivas. Ademais, o regulamento restringiu negativamente o tratamento dos singulares, tornando inviável a proteção de dados pessoais nas esferas pessoal e doméstica, conforme os Considerandos de nº 14 e 18.

O Regulamento 679/2016, da União Europeia, em se tratando da aplicação material, o Artigo 2º, estatuiu diversas hipóteses nas quais o regulamento não se aplicaria, uma delas a seara penal:

> 2. O presente regulamento não se aplica ao tratamento de dados pessoais:
>
> d) efetuado pelas autoridades competentes para efeitos de prevenção, investigação, detenção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública (UNIÃO EUROPEIA, 2016).

Em contrapartida, a Lei Geral de Proteção de Dados Pessoais pôde ser definida por seus cinco eixos principais: “i) unidade e generalidade da aplicação da Lei; ii) legitimação para o tratamento de dados (hipóteses autorizativas); iii) princípios e direitos do titular; iv) obrigações

dos agentes de tratamento de dados; v) responsabilização dos agentes" (DONEDA, 2018, p. 312).

A lei geral asseverou, mais especificamente, em seu art. 1º, sobre seu principal campo atuação que compreendeu o tratamento dos dados pessoais, inclusive, nos meios digitais. O referido dispositivo traçou seu objetivo fundante: a proteção dos direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL. 2018).

Na delimitação material e territorial de aplicação da lei teve-se como destino, de acordo com o art. 3º, as pessoas naturais ou pessoas jurídicas, tanto aquelas de direito público como as de direito privado. Concernente à aplicação territorial buscou-se observar se as operações e atividades de tratamento, bem como os dados coletados, teriam sido obtidos em território nacional, independentemente do país de sede ou do país em que estivesse localizada a pessoa natural ou a pessoa jurídica.

O art. 4º da Lei Geral de Proteção de Dados Pessoais, elencou diversas hipóteses de exceção à aplicação do tratamento de dados pessoais. De acordo alínea "d", do rol do inciso III, do dispositivo, é inaplicável as disposição da lei quando se tratar de atividades de investigação criminal e de repressão de infrações penais (BRASIL, 2018), tal qual o ordenamento europeu.

Outro dispositivo de destaque da lei geral foi o art. 5º, que definiu, para o melhor entendimento da lei geral, uma série de conceituações. O legislador estabeleceu o dado pessoal como sendo a "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018). Partindo deste pressuposto, subdividiu os dados pessoais em dois tipos: dados sensíveis e dados anonimizados.

Os dados sensíveis nos termos do inciso I, do art. 5º, foram compreendidos como os de "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural". Já os dados anonimizados, compreenderam aqueles cuja titularidade não pode ser identificada, conforme o inciso III (BRASIL, 2018).

Sobre os sujeitos abarcados na lei, criou-se a figura do titular dos dados e a dos agentes da proteção. O titular compreendeu a pessoa natural, a qual pertence os dados pessoais a serem

tratados, já os agentes de proteção englobariam o controlador e o operador, ambos pessoas naturais ou jurídicas, de direito público ou privado, sendo o primeiro "a quem competem as decisões referentes ao tratamento de dados pessoais" e o segundo, aquele que realiza o tratamento em nome do controlador (BRASIL, 2018).

Por fim, mais um dispositivo de ênfase da lei geral foi o art. 7º que previu dez hipóteses para o tratamento dos referidos dados. A definição do consentimento foi compreendida, pela lei geral, como sendo a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", consoante o art. 5º, XII, (BRASIL, 2018).

2.1 A importância do consentimento para o tratamento dos dados pessoais

Bioni (2018) revela que na primeira versão do anteprojeto de lei da lei geral de proteção de dados pessoais, apresentado no ano de 2010, na sua primeira consulta pública, o consentimento era a única base legal de tratamento dos referidos dados. A ocorrência foi a mesma no ano de 2015, na segunda consulta pública.

Ainda de acordo com o autor:

> Após tais consultas públicas, o texto enviado ao Congresso Nacional, que depois veio a ser aprovado e sancionado, acabou por posicionar o consentimento como sendo uma das hipóteses legais e não na cabeça do dispositivo. Isso significa que, em termos de técnica legislativa, o consentimento não só deixou de ser a única base legal para o tratamento de dados, como também foi alocado topograficamente sem ser hierarquicamente superior às demais bases legais por estarem todos elas horizontalmente elencadas em incisos do art. 7º da LGPD (2018).

No entanto, o consentimento não deixou de ser o vetor mais importante para a realização do tratamento, já que a leitura dos princípios fundantes da lei geral e o corpo normativo da própria lei evidenciaram a preocupação com a participação do titular dos dados pessoais em sua capacidade de autodeterminação informacional, ou seja, no fluxo em que percorriam suas informações (BIONI, 2018).

Além de primeiro requisito consubstanciado no art. 7º, I, da Lei Geral de Proteção de Dados Pessoais, o consentimento foi o princípio basilar para o tratamento dos respectivos dados. As condições para que o consentimento fosse considerado efetivo, pela lei geral, foram previstas na sua própria definição (art. 5º, XII), devendo o mesmo ser livre, informado, inequívoco e com uma finalidade determinada (DONEDA, 2018, p. 314).

O consentimento informado para Bioni (2016, p. 44), compreendeu a ciência a respeito do uso, coleta e compartilhamento dos dados. Já a adjetivação livre, para o mesmo autor "cinge-se, assim, à concepção de um ato volitivo que deve não ser fruto de coação (física ou moral), a fim de que a autodeterminação informacional seja vetorizada de forma genuína".

A finalidade pré-determinada seria o direcionamento do consentimento, de modo que o mesmo não constituísse uma permissão genérica que embasasse qualquer tipo de tratamento de dados. Quanto ao caráter inequívoco do consentimento, em suma, referiu-se a desnecessidade de "uma ação afirmativa por parte do seu titular, mas poder ser implicitamente extraída do contexto de uma relação" (BIONI, 2016, p. 45).

Para Schermer, Bart e Hof (2014), além de todos os requisitos acima consubstanciados, seria indispensável ao titular dos dados a posse de conhecimento básico sobre as possíveis consequências que a manifestação da vontade poderia gerar.

3 ANÁLISE DA VIABILIDADE DE FORNECIMENTO DO CONSENTIMENTO DO TITULAR PARA ACESSO AOS DADOS PESSOAIS NAS ATIVIDADES DE INVESTIGAÇÃO E REPRESSÃO À INFRAÇÕES PENAIS: VIOLAÇÃO AS GARANTIAS CONSTITUCIONAIS

De acordo com Mendes, "os dados pessoais relativos à suspeita de cometimento de crimes não são de forma alguma privados ou íntimos", configurariam informações de cunho meramente pessoal, divergindo-se das esferas da privacidade e da intimidade (2014, p. 164), o que afastaria, por consequência, a concessão do consentimento. Apesar da referida posição doutrinária, os dados pessoais encontram-se ligados ao direito da privacidade e ao consentimento, mesmo nas atividades de repressão a ilícitos penais.

O direito à privacidade, positivado pelo legislador constituinte no inciso X, do art. 5º, da Carta Magna, abrangeu "o modo de vida doméstico, nas relações familiares e afetivas em geral, fatos hábitos, local, nome, imagem, pensamentos, segredos, e, bem assim, as origens e planos futuros do indivíduo" (QUINITIERE, 2019, p. 179, *apud* OLIVEIRA, 1980, p. 50). Enquanto a intimidade foi definida como uma espécie de subgênero do primeiro direito.

A necessidade do debate sobre a privacidade se deu em decorrência da utilização de novas tecnologias que propiciaram acesso e divulgação de fatos inerentes a privada no ambiente virtual (MENDES, 2014, p. 27). A difusão dos meios tecnológicos ensejou um fenômeno crescente de invasão e exposição da vida privada.

Tal fenômeno já era perceptível em 1890, em que a fotografia, jornais, entre outras tecnologias da época, eram consideradas formas de invasão da vida privada e doméstica por (WARREN & BRANDEIS, 1890, p. 195). Os mencionados autores, na defesa da privacidade, buscaram traçar seus limites de alcance, e, um deles, seria o consentimento, responsável por excluir quaisquer violações de direitos. Na lição atemporal acima transcrita, o consentimento já se alinhava aos preceitos da privacidade.

No plano nacional, ainda na fase de recém nascimento da Constituição Federal de 1988, o Supremo Tribunal Federal, em sua jurisprudência, mais especificamente no Recurso Ordinário em *Habeas Data*, o RHD 22/DF, em 1991, que tratava da requisição de acesso a dados pessoais constantes no Serviço Nacional de Informações, por meio do recurso em *habeas data*.

No processo citado, o Ministro Celso de Mello reconheceu a existência dos direitos à personalidade inerentes ao consentimento: "A garantia de acesso a informações de caráter pessoal, registradas em Órgãos do estado, constitui um natural consectário do dever estatal de respeitar a esfera de autonomia individual, que torna imperativa a proteção da intimidade" (BRASIL, 1991).

Na própria leitura de Mendes (2014, p. 170), a análise jurisprudencial e normativa demonstrou que existe uma rica experiência institucional em curso, que reconhece a evolução do conceito de privacidade, de modo a abarcar a proteção dos dados pessoais no ordenamento jurídico vigente.

O caminhar da jurisprudência brasileira, especificamente nos Tribunais Superiores, tangenciou seu entendimento sobre o acesso a dados e uso da tecnologia como um instrumento para efetivação, também, da tutela jurisdicional penal. O informativo nº 583, do Superior Tribunal de Justiça, entendeu como nula prova obtida por meio da extração de dados e de conversas registradas no aplicativo de mensagens *WhatsApp*, sem prévia autorização judicial (QUINTIERE, 2019, p. 183). Assim, não há que se falar em privacidade sem o fornecimento do consentimento.

Relativamente ao direito à não autoincriminação, este encontra-se consubstanciado na máxima latina *nemo tenetur se detegere*, como bem pondera Moraes (2000, p. 285):

> O direito de permanecer em silêncio, constitucionalmente consagrado, seguindo orientação da Convenção Americana sobre Direitos Humanos, que

> prevê em seu art. 8º, § 2º, g, o direito a toda pessoa acusada de delito não ser obrigada a depor contra si mesma, nem a declarar-se culpada, apresenta-se como verdadeiro complemento aos princípios do due processo of law e da ampla defesa, garantindo-se dessa forma ao acusado não só o direito ao silêncio puro, mas também o direito a prestar declarações falsas e inverídicas, sem que por elas possa ser responsabilizado, uma vez que não se conhece em nosso ordenamento jurídico o crime de perjúrio

A referida garantia à não autoincriminação encontra-se no inciso LXIII, do art. 5º, da Carta Magna. Apesar de o comando fazer alusão ao direito de permanecer calado, o direito de silêncio é uma manifestação de uma garantia muito maior, segundo a qual o sujeito a uma intervenção penal não pode sofrer nenhum prejuízo jurídico por omitir-se de colaborar em uma atividade probatória da acusação ou por exercer seu direito de silêncio quando interrogado (GESU, 2010, p. 50).

Fazendo um paradoxo do fornecimento do consentimento com o fornecimento de material genético, para fins utilização de prova no processo penal, na lição de Lopes Junior sobre o material genético (2017, p. 433) têm-se que, ao acusado, deveria ser concedido o direito à recusa do fornecimento, sem que tal recusa fosse interpretada em desfavor dele. Se tal possibilidade de recusa não é ofertada, o acusado estaria produzindo prova contra si mesmo.

Para ele, a obrigatoriedade de o investigado fornecer material genético viola o princípio do *nemo tenetur se detegere*, no entanto "havendo o consentimento do suspeito, poderá ser realizada qualquer espécie de intervenção corporal, pois o conteúdo da autodefesa é disponível e, assim, renunciável" (LOPES JUNIOR, 2017, p. 434).

Ainda sob a perspectiva de fornecimento de material genético, Sauthier (2015, p. 13), afirma que "a privacidade informacional protege as informações pessoais [...] que possam conduzir à identificação da pessoa como tal".

De igual modo, pode-se fazer, também, comparação à recusa de realização de teste alcoolemia, popularmente conhecido como bafômetro. Tal faculdade ganhou respaldo com lastro no direito à não autoincriminação:

> a recusa do condutor em submeter-se ao bafômetro ou a um exame de sangue não configura crime de desobediência nem pode ser interpretada em seu desfavor, pelo menos no âmbito criminal. Nessa linha, há precedentes do Supremo Tribunal Federal no sentido de que não se pode presumir a embriaguez de quem não se submete a exame de dosagem alcóolica: afinal, a Constituição da República impede que se extraia qualquer conclusão desfavorável àquele que, suspeito ou acusado de praticar alguma infração

> penal, exerce o direito de não produzir prova contra si mesmo (princípio do *nemo tenetur se detegere*). (LIMA, 2014, p. 87).

Assim, o consentimento informado do titular dos dados pessoais figuraria de modo a garantir que não houvesse violação do direito à privacidade e para que não houvesse a produção de provas do acusado contra si mesmo e, para que na recusa do fornecimento do consentimento, o ato não fosse interpretado prejudicialmente ao acusado, práticas vedadas constitucionalmente no ordenamento brasileiro.

3.1 Preocupações com o tema

É direito do titular dos dados pessoais, quando na pendência de uma intervenção penal, ser tutelado. A impossibilidade de aplicação da lei geral ao procedimento criminal, em verdade, resulta em uma mitigação das garantias acima previstas. Quintiere, sobre o tema, entendeu que:

> o conjunto de instrumentos e normas existentes no Brasil, em especial aquele relativo à proteção de dados, a Constituição Federal, de 1988, Código Penal, Código de Processo Penal, Lei nº 9.296, de 1998, e Lei Geral de Proteção de Dados não garantem ao Estado, mais especificamente na condição de titular da Jurisdição, condições mínimas no combate preventivo às violações aos direitos de autodeterminação informativa do réu, pela utilização de *dataveillance*, violando igualmente o princípio do *nemotenetur se detegere*.

Em atenção a necessidade de tutela dos dados pessoais durante a perseguição penal, Quintiere sugeriu uma proposta de regulamentação do tema à luz das disposições constantes na lei que disciplina a interceptação telefônica, sob o nº 9.296 de 1996 (2019, p. 187). Como enfoque específico para o art. 2º, da referida proposta, têm-se a exigibilidade de observância de alguns requisitos.

A investigação do fluxo de dados, conforme a sugestão do autor, só deverá ser admitida quando verificada a existência de indícios razoáveis de autoria ou participação em infração penal, quando a prova não puder ser obtida por outros meios disponíveis e o ilícito ser passível de sanção mínima de detenção, incabível para os fatos que constituírem contravenção penal.

Nos termos do art. 4º, *caput,* da proposta de Quintiere, o pedido para investigação do fluxo de dados terá de conter a demonstração de que a medida é essencial para a apuração do ilícito penal, indicando, ainda, os meios que serão empregados para a realização do referido tratamento.

A proposição do autor, na eventualidade de inobservância dos requisitos acima mencionados, é de que seja considerada crime a prática de investigação de fluxo de dados

discretos que não observe as disposições legais, que se proceda sem a autorização devida ou, ainda, que quebre sigilo de justiça, na linha do art. 10.

Com a mesma preocupação sobre a tutela dos dados pessoais nasceu a Proposta de Emenda à Constituição nº 17/19 que "insere a proteção de dados pessoais, incluindo os digitalizados, na lista de garantias individuais da Constituição Federal de 1988.". A referida proposta é de autoria do Deputado Federal Orlando Silva, do Partido Comunista do Brasil.

Durante o debate realizado em novembro de 2019, na Câmara dos Deputados, "especialistas defenderam que a proteção de dados pessoais, incluindo os digitalizados, deve figurar entre os direitos fundamentais previstos na Constituição" (CÂMARA DOS DEPUTADOS, 2019).

Christian Perrone, representante do Instituto de Tecnologia e Sociedade do Rio de Janeiro afirmou, durante o debate, que nos mais diversos ordenamentos jurídicos estrangeiros a proteção de dados é tida como direito fundamental, a exemplo a União Europeia. (CÂMARA DOS DEPUTADOS, 2019).

Ademais, no ano de 2020, foi aprovada a Estratégia Nacional de Segurança Cibernética, E-Ciber, na figura Decreto nº 10.222, de 5 de fevereiro de 2020. A referida normativa teve por objetivo estratégico: "Tornar o Brasil mais próspero e confiável no ambiente digital; Aumentar a resiliência brasileira às ameaças cibernéticas; e Fortalecer a atuação brasileira em segurança cibernética no cenário internacional" (BRASIL, 2020).

Apesar da iniciativa positiva em fomentar a educação e a regulamentação da segurança cibernética, as medidas de viés penal se bastaram nas ações estratégicas de combate aos crimes cibernéticos e de proteção à privacidade daqueles vítimas desses crimes. Entretanto, o decretou nada versou sobre a tutela da segurança cibernética sob à perspectiva dos direitos de um acusado.

Ainda em estágio de *vacatio legis*, cujo intervalo finda em meados de agosto de 2020, a preocupação maior se dá com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais para o ano corrente, motivada por algumas das omissões legislativas, como a concernente à esfera penal.

O Deputado Federal Carlos Gomes Bezerra Gomes, do Partido Movimento Democrático Brasileiro, propôs, por meio do Projeto de Lei sob o nº 5.762/2019, a prorrogação

da data de entrada em vigor da referida legislação como sendo para 15 de agosto de 2022 (BRASIL, 2019).

A justificativa para tanto foi de que poucas das grandes empresas brasileiras iniciaram os processos de adaptação ao cenário instituído pela lei (BRASIL, 2019, p. 2). Além disso, a preocupação do Deputado se deu, também, com a instauração da Autoridade Nacional de Proteção de Dados, sem tempo hábil para debate e tratamento da matéria.

Não obstante que o projeto não tratasse sobre a aplicação dos institutos da lei às investigações criminais, tal ausência normativa preocupou a Câmara dos Deputados. O Presidente da Casa, o Deputado Federal Rodrigo Maia, do Partido Democratas, criou uma comissão de juristas responsável pela elaboração de anteprojeto de lei sobre proteção de dados pessoais para fins de segurança pública, defesa nacional e atividades de investigação de infrações penais (CÂMARA DOS DEPUTADOS, 2019).

A comissão de juristas que tem como presidente o Ministro Nefi Cordeiro, do Superior Tribunal de Justiça, conforme a literalidade de seu art. 1º, é "destinada a elaborar anteprojeto de legislação específica para o tratamento de dados pessoais no âmbito de segurança pública, infrações penais e repressão de infrações penais", e terá 120 dias para conclusão dos trabalhos, desde a data de sua instalação, com a possibilidade de prorrogação do período quando solicitado pelo presidente.

O referido ato do Presidente, do dia 26 de novembro de 2019, teve por consideração o caráter personalíssimo dos dados pessoais, combinado à necessidade de preservação da privacidade do indivíduo, especialmente quando esses dados estiverem intimamente ligados à probabilidade de privação da liberdade daquele submetido as investigações penais.

Durante encontro do colegiado, promovido em 03 de fevereiro de 2020, os integrantes fizeram um levantamento inicial, por meio de pesquisas acadêmicas, principalmente na União Europeia, de modo a destacar alguns assuntos como: "proteção de dados pessoais; aspectos constitucionais; cooperação jurídica internacional; e processo penal". Com o próximo encontro marcado para março de 2020, a comissão irá proceder a oitiva de especialistas no assunto (CÂMARA DOS DEPUTADOS, 2020).

CONSIDERAÇÕES FINAIS

De início, constatou-se que o cenário imbuído na tutela dos dados pessoais na legislação brasileira percorreu diversos marcos temporais legislativos, cujo primórdio se deu na Constituição Federal, por meio da tutela da privacidade e da intimidade, até a instituição da Lei Geral de Proteção de Dados Pessoais.

Em que pese o tratamento expresso dos dados pessoais ter ocorrido apenas na lei geral de proteção, o tema já era objeto de atenção por outras legislações, como o Marco Civil da Internet, a Lei de Acesso à Informação e o Código de Defesa do Consumidor.

Os fenômenos ocorridos, a níveis nacional e internacional, como o escândalo da *Cambridge Analytica* na campanha eleitoral de Donald Trump e no *Brexit* e o vazamento de dados pelo SERPRO, foram os maiores responsáveis pela positivação da proteção dos referidos dados no Brasil.

Passando, no segundo capítulo, pela análise do direito comparado, teve-se como espelho para a construção da legislação no ordenamento brasileiro o Regulamento da União Europeia 679/2016 que, em verdade, já era pioneira do tema desde a Diretiva Europeia 95/46/CE. O regulamento europeu, ao contrário da norma brasileira, estabeleceu a tutela dos dados pessoais como um direito fundamental.

Ambas as legislações definiram seus princípios basilares como sendo o tratamento e proteção de dados pessoais e restringiram seu alcance: nenhuma das leis buscou tutelar os dados pessoais no âmbito da persecução penal. Ainda assim, buscou-se analisar alguns dos principais institutos da lei geral para sua melhor compreensão, como as conceituações definidas e os requisitos para o tratamento de dados.

O primeiro requisito consubstanciado para o referido tratamento na lei geral foi o consentimento. O protagonismo do consentimento, como visto no primeiro capítulo, percorreu quatro gerações de lei, em algumas atuava como vetor principal e, em outras, era restringido.

No próprio anteprojeto da lei geral, a única hipótese de tratamento desses dados era sob o fornecimento do consentimento. Apesar de a lei ter sido sancionada com outras nove hipóteses de tratamento, divergindo-se do projeto inicial, o consentimento não perdeu sua importância, em decorrência da preocupação com a autodeterminação informacional.

Para entender o instituto, conforme a conceituação do art. 5º, XII, da lei geral, foi necessário definir o que seria o consentimento livre, informado, inequívoco e com finalidade determinada.

Apesar da restrição de alcance da lei geral aos procedimentos criminais, buscou-se analisar sobre a viabilidade de aplicação do instituto do consentimento aos procedimentos de cunho criminal. Isto, para entender se é possível que o titular dos dados pessoais, ora investigado, possa ter ingerência sobre o acesso e tratamento de seus dados.

Para tanto, no último capítulo, tratou-se do consentimento e da privacidade e da não autoincriminação. A posição de Mendes ainda revelava certo distanciamento dos dados pessoais de um acusado da tutela da lei geral, pautando-se em que tais informações consistiram em meras informações, excluindo a privacidade a intimidade.

Contudo, na linha da mesma posição doutrinária, foi demonstrada a necessidade de debate sobre a privacidade, principalmente com o fenômeno crescente de invasão e exposição da vida privada, já perceptível em 1980, por Warren e Brandeis que consideraram que a única maneira de não se violar a privacidade era por meio do consentimento.

O Ministro Celso de Mello, no julgamento do RHD 22/DF, em 1991, reconheceu que o acesso a informações de caráter pessoal exigiam a proteção e o respeito estatal da autonomia individual e da intimidade.

Mendes reconheceu a evolução da jurisprudência no que concerne à proteção dos dados pessoais à luz do direito à privacidade. Conforme demonstrou Quintiere, o acesso a dados e tecnologia, especificamente no âmbito penal, efetivou a tutela jurisdicional penal. Assim, o consentimento e privacidade caminharam juntos, a forma de não violar a garantia constitucional da privacidade se deu por meio do fornecimento do consentimento expresso do titular dos dados para sua utilização.

Na análise do consentimento à luz do direito à não autoincriminação, consubstanciada no brocado *nemo tenetur se detegere*, em comparação ao fornecimento de material genético e a realização do teste de alcoolemia, o direito de recusa deveria ser ofertado, caso contrário haveria violação da máxima acima, conforme destacou Lopes Junior. O mencionado autor considerou que o consentimento afastaria tal violação.

Quintiere, em proposta de regulamentação do tema, em razão da lei geral ter esquivado de tratá-lo, sugeriu que a investigação de dados só deve ocorrer quando houver indícios razoáveis de autoria ou participação delitiva, quando a prova não puder ser obtida por outros meios e para delitos de sanção mínima de detenção. A obediência de tais requisitos relativizaria a mitigação da autoincriminação e da privacidade.

Ainda nesse contexto surgiu a proposta de emenda constitucional para englobar os dados pessoais como sendo um direito fundamental, tal medida seria eficaz para tutelar os dados de um acusado, pois não haveria proteção seletiva apenas de possíveis vítimas.

Apesar de ter sido aprovada a Estratégia Nacional de Segurança Cibernética, a referida legislação manteve-se silente quanto à medidas de proteção penais de um acusado, tratando apenas como preocupação, a criminalização de condutas virtuais ilícitas.

Em que pese a celeridade com que o Congresso Brasileiro buscou estatuir a lei geral, a rápida positivação desencadeou questionamentos inerentes à proteção dos dados no âmbito do direito penal, inclusive ensejou a criação de uma comissão para tratar do tema em específico.

Assim, verificou-se que não deverá ser considerada a possibilidade de exclusão da tutela jurisdicional da lei geral ao direito penal, mesmo que a referida lei se esquive de tal tratamento, em respeito aos princípios e garantias constitucionais da privacidade e da vedação à autoincriminação, a tutela deve ser efetivada, ainda que mediante alteração legislativa da lei geral ou da instituição de uma nova lei que aborde o tema.

Em que pese isto, é indispensável que seja considerado o caráter personalíssimo dos dados pessoais e que seja ofertada a possibilidade do direito de consentimento ou mesmo do direito de recusa, por parte de um acusado para o referido tratamento e, posteriormente, modificação da Lei Geral de Proteção de Dados Pessoais.

O ordenamento jurídico brasileiro deverá aguardar a normatização do tema pela Comissão de Juristas criada pelo presidente da Câmara dos Deputados, dando preferência para oferta do direito ao fornecimento ou da recusa e, se esses direitos não forem considerados, que o acesso e tratamento de dados pessoais de acusado esteja submetido a tutela do poder judiciário e ao contraditório e à ampla defesa.

REFERÊNCIAS

AGÊNCIA SENADO (Ed.). **Projeto de lei geral de proteção de dados pessoais é aprovado no Senado.** 2018. Disponível em: https://www12.senado.leg.br/noticias/materias/2018/07/10/projeto-de-lei-geral-de-protecao-de-dados-pessoais-e-aprovado-no-senado. Acesso em: 22 out. 2019.

AVAST. **Os últimos 10 maiores vazamentos de dados**. 2019. Disponível em: https://blog.avast.com/pt-br/os-ultimos-10-maiores-vazamentos-de-dados . Acesso em: 13 out. 2019.

BIONI, B. R. **Proteção de dados pessoais :** a função e os limites do consentimento. [s. l.], 2018. Disponível em: http://search.ebscohost.com/login.aspx?direct=true&db=edsmib&AN=edsmib.000013124&lang=pt-br&site=eds-live. Acesso em: 15 out. 2019.

_____. **Xeque-mate:** o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. USP- Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação. Relatório de Pesquisa, 2016.

BRASIL. Câmara dos Deputados. **Projeto de Emenda à Constituição nº 17 de 2019**. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/133486. Acesso em: 15 out. 2019.

BRASIL. Câmara dos Deputados. Projeto de Lei n° 5.762 de 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2227704. Acesso em: 18 jan. 2020.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4.060 de 2012**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: 15 out. 2019.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 53 de 2018.** Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/133486. Acesso em: 15 out. 2019.

BRASIL. **Constituição da República Federativa do Brasil.** Brasil, 5 outubro 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17 out. 2019.

BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: 20 fev. 2020.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº

11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 17 out. 2019.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 19 out. 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 out. 2019.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 10 out. 2019.

BRASIL. Supremo Tribunal Federal. **Recurso Ordinário em Habeas Data n. 22/DF**, Pleno, j. 19-9-1991, m.v., rel. Min. Marco Aurélio, rel. p/ acórdão Min. Celso de Mello, DJ 1º-9-1995.

CÂMARA DOS DEPUTADOS (Brasil). **Comissão de juristas vai ouvir especialistas sobre uso de dados pessoais em investigações**. [*S. l.*]: Da Redação - MO, 4 fev. 2020. Disponível em: https://www.camara.leg.br/noticias/634101-comissao-de-juristas-vai-ouvir-especialistas-sobre-uso-de-dados-pessoais-em-investigacoes/. Acesso em: 6 fev. 2020.

CÂMARA DOS DEPUTADOS (Brasil). **Especialistas defendem legislação que coloque proteção de dados como direito fundamental**. [*S. l.*]: Ana Chalub, 6 nov. 2019. Disponível em: https://www.camara.leg.br/noticias/610575-especialistas-defendem-legislacao-que-coloque-protecao-de-dados-como-direito-fundamental/.Acesso em: 2 jan. 2020.

CÂMARA DOS DEPUTADOS (Brasil). **Maia cria comissão de juristas para propor lei sobre uso de dados pessoais em investigações**: Colegiado terá 120 dias para elaborar o anteprojeto que, depois, será analisado pelo Congresso. [*S. l.*]: Natalia Doederlein, 27 nov. 2019. Disponível em: https://www.camara.leg.br/noticias/618483-maia-cria-comissao-de-juristas-para-propor-lei-sobre-uso-de-dados-pessoais-em-investigacoes/. Acesso em: 17 dez. 2019.

CÂMARA DOS DEPUTADOS (Brasil). **PEC transforma proteção de dados pessoais em direito fundamental**. [*S. l.*]: Natalia Doederlein, 9 ago. 2019. Disponível em: https://www.camara.leg.br/noticias/565439-PEC-TRANSFORMA-PROTECAO-DE-DADOS-PESSOAIS-EM-DIREITO-FUNDAMENTAL. Acesso em: 16 jan. 2020.

COELHO, Gabriela. **MP-DF acusa empresa pública de vender dados pessoais de brasileiros**. **Revista Consultor Jurídico**, 31 de maio de 2018. Disponível em: < https://www.conjur.com.br/2018-mai-31/mp-df-acusa-empresa-publica-vender-dados-brasileiros#top. Acesso em: 29 out. 2019.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico *Journal of Law* [EJJL], v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 10 out. 2019

DONEDA, Danilo; SCHERTEL, Laura Mendes. **Um perfil da nova Lei Geral de Proteção de Dados brasileira**. *In*: BELLI, Luca et al. Governança e regulações da Internet na América Latina: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. FGV Direito Rio, 2018. Disponível em: http://hdl.handle.net/10438/27164. Acesso em: 10 ou 2019.

FAZZALARI, Elio. ***Istituzioni di Diritto Processuale***. Cedam, 1992.

GESU, Cristina Di. **Prova penal & falsas memórias**. Rio de Janeiro: Lumen Juris, 2010.

GUIMÓN, Pablo. Cambridge Analytica, empresa pivô nível no escândalo do Facebook, é fechada. **El País,** 02 maio 2018. Disponível em: https://brasil.elpais.com/brasil/2018/05/02/internacional/1525285885_691249.html. Acesso em: 31 out. 2019

_____. O 'Brexit' não teria acontecido sem a Cambridge Analytca. **El País**, 26 março 2018. Disponível em: https://brasil.elpais.com/brasil/2018/03/26/internacional/1522058765_703094.html>. Acesso em: 29 out. 2019

LIMA, Renato Brasileiro de. **Manual de processo penal**. 2. ed. Salvador: Juspodivim, 2014.

LOPES JUNIOR, A. **Direito processual penal**. *[s. l.]*, 2017. Disponível em: http://search.ebscohost.com/login.aspx?direct=true&db=edsmib&AN=edsmib.000012596&lang=pt-br&site=eds-live. Acesso em: 5 fev. 2020.

MARTÍ, Silas. Entenda o escândalo do uso de dados do Facebook. **Folha de São Paulo**, 22 mar. 2018. Disponível em: https://www1.folha.uol.com.br/mercado/2018/03/entenda-o-escandalo-do-uso-de-dados-do-facebook.shtml. Acesso em: 27 out. 2019.

MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor :** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. ISBN 9788502218987. Disponível em: http://search.ebscohost.com/login.aspx?direct=true&db=edsmib&AN=edsmib.000005030&lang=pt-br&site=eds-live. Acesso em: 27 jan. 2020.

MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS. Fabiana Costa Oliveira Barreto. Procuradoria-Geral de Justiça. **Representação,** Brasília, DF, 10 de junho de 2019. Disponível em: http://www.mpdft.mp.br/portal/pdf/comunicacao/junho_2019/Representacao_TCU_-_SERPRO_-_PGJ.pdf. Acesso em: 05 nov. 2019.

MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS. Frederico Meinberg Ceroy. Comissão de Proteção de Dados Pessoais. Ofício 20/2018 – CPDP/MPDFT. **Despacho Ministerial,** Brasília, DF, 30 de maio de 2018. Disponível em: https://www.conjur.com.br/dl/oficio-mpf-base-dados.pdf. Acesso em: 04 nov. 2019.

MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS. Ministério Público representa contra o Serpro no TCU. Assessoria Especial de Imprensa, Brasília, DF, 19 de junho de 2019. Disponível em: http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10987-mpdft-representa-contra-o-serpro-no-tcu. Acesso em: 04 nov. 2019.

MORAES, Alexandre de. **Direitos humanos fundamentais**. 3. ed. São Paulo: Atlas, 2000.

PARLAMENTO EUROPEU E CONSELHO, **Diretiva 95/46/CE, 24 de outubro de 1995**, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoas e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046. Acesso em: 31 out. 2019.

PELLEGRINI GRINOVER, Ada; SCARANCE FERNANDES, Antônio e GOMES FILHO, Antônio Magalhães. **As nulidades no processo penal**. 2. ed. São Paulo, Malheiros, 1992.

PINHEIRO, P. P. **Proteção de dados pessoais :** comentários à Lei n. 13.709/2018 (LGPD). [s. l.], 2018. Disponível em: http://search.ebscohost.com/login.aspx?direct=true&db=edsmib&AN=edsmib.000013416&lang=pt-br&site=eds-live. Acesso em: 31 out. 2019.

POZZI, Sandro. EUA multam Facebook em 5 bilhões de dólares por violar privacidade dos usuários: Empresa é punida com multa recorde pelo vazamento de dados no caso Cambridge Analytica. **El País**, 13 jul 2019. Disponível em: https://brasil.elpais.com/brasil/2019/07/12/economia/1562962870_283549.html. Acesso em: 22 out. 2019

QUINTIERE, Víctor Minervino. Questões controversas envolvendo a tutela jurisdicional penal e as novas tecnologias à luz da lei geral de proteção de dados (LGPD) Brasileira: Dataveillance. **Revista ESMAT**, v. 11, n. 17, p. 175-188, 2019. Disponível em: http://dx.doi.org/10.34060/reesmat.v11i17.290. Acesso em: 10 out. 2019.

SAUTHIER, R. **A identificação e a investigação criminal genética à luz dos direitos fundamentais e da Lei 12.654/12**. Curitiba, PR: CRV, 2015.

SCHERMER, B. W.; CUSTERS, Bart; HOF. S, van der. ***The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection (February 25, 2014)***. *Ethics and Information Technology.* DOI: 10.1007/s10676-014-9343-8, Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418. Acesso em out. 2017.

THE GUARDIAN. ***Five things we learned from Mark Zuckerberg's European parliament appearance***. 2018. Disponível em:

https://www.theguardian.com/technology/2018/may/22/five-things-we-learned-from-mark-zuckerbergs-european-parliament-appearance. Acesso em: 18 out. 2019

THE GUARDIAN**.** ***The key moments from Mark Zuckerberg's testimony to Congress*****.** 2018. Disponível em: https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments. Acesso em: 17 out. 2019.

THE NEW YORK TIMES. **How Trump Consultants Exploited the Facebook Data of Millions**. 2018. Disponível em: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. Acesso em: 14 jun. 2018.

UNIÃO EUROPEIA. **Comunicação da Comissão ao Parlamento Europeu e ao Conselho. Bruxelas**, 24 jan 2018. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A52018DC0043&qid=1517578296944&from=EN. Acesso em: 04 nov. 2019.

UNIÃO EUROPEIA. Para que serve o Regulamento Geral sobre a Proteção de Dados (RGPD)?. **Jornal Oficial da União Europeia**, 2016. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_pt. Acesso em: 01 nov. 2019.

UNIÃO EUROPEIA. **Regulamento (EU) 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). Jornal Oficial da União Europeia, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em: 01 nov. 2019.

WARREN, Samuel; BRANDEIS, Louis. *The Right to Privacy*, *In*: ***Harvard Law Review***, Vol. 4, No. 5, 1890. Disponível em: http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 15 dez. 2019.

AGRADECIMENTOS

“Não há caminho fácil da terra às estrelas”. É nesta lição de Sêneca que tenho pautado meus esforços diários durante toda a graduação. Com a conclusão de mais este passo, encontro-me cada vez mais perto do encerramento de todo um ciclo que, por óbvio, não seria possível sem os coprotagonistas da minha história.

Em primeiro agradeço a Deus por ter me concedido saúde, coragem e dedicação para esta graduação.

À minha família que não poupou esforços para me proporcionar uma oportunidade de estudo de qualidade, que me apoiou a cada dia da graduação e batalhou comigo durante toda a minha formação.

Aos meus colegas de curso por todo o companheirismo, paciência e reciprocidade durante todo o curso, principalmente nos momentos mais desafiadores e difíceis pelos quais passamos juntos.

Ao meu orientador, o Professor Víctor Minervino Quintiere, por todo apoio, paciência e confiança que me conferiu durante a elaboração deste trabalho.

Por fim, a todos os demais professores que me incentivaram e me ensinaram, diariamente, com maestria e dedicação ao saber.