CLARISSA MARIA LIMA MOURA

DADOS PESSOAIS COMO ATIVO NA ECONOMIA DIGITAL:
A tutela jurídica na legislação nacional e europeia acerca da manipulação de dados sensíveis para fins econômicos

RECIFE
2019

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE CIÊNCIAS JURÍDICAS
FACULDADE DE DIREITO DO RECIFE

DADOS PESSOAIS COMO ATIVO NA ECONOMIA DIGITAL:

A tutela jurídica na legislação nacional e europeia acerca da manipulação de dados sensíveis para fins econômicos

Monografia final de curso apresentada à banca examinadora da Faculdade de Direito do Recife, Universidade Federal de Pernambuco, como exigência parcial para obtenção do grau de bacharel em Direito.
Orientando: Clarissa Maria Lima Moura
Orientadora: Prof.ª. Eugênia Cristina Nilsen Ribeiro Barza.

RECIFE
2019

Dedico este trabalho de conclusão de curso aos meus pais, Francisco e Christiene, pelo apoio incondicional e por terem feito deste momento o maior esforço e investimento de suas vidas.

AGRADECIMENTOS

Agradeço à minha família pelo apoio e suporte durante toda a graduação, principalmente aos meus pais Francisco e Christiene e minha avó Leninha, por tudo o que fizeram e ainda fazem pela minha educação.

À minha irmã Fabiola e minha sobrinha Maria Alice, pelo companheirismo de sempre, principalmente durante a elaboração deste trabalho.

Às amizades que fiz e fortaleci durante esta graduação, por toda a parceria durante a realização deste curso.

À Felipe Pernambuco, por sempre me tranquilizar e acreditar no meu potencial.

RESUMO

O presente trabalho busca explanar uma das principais consequências da consolidação da sociedade da informação, propiciada pela crescente importância da internet e tecnologias correlatas no âmbito social, realizando a análise das repercussões jurídicas do elemento intrínseco da atividade online, qual seja a coleta de dados pessoais dos usuários, que se dá muitas vezes sem o consentimento destes, tendo estas informações inequívoco valor econômico agregado no âmbito da economia digital. Com a crescente presença da tecnologia no cotidiano, a consolidação de sua importância econômica e a divulgação de escândalos midiáticos de vazamentos de dados pessoais, delineia-se como estes podem ser usados para manipular escolhas e acesso a bens por parte de seus titulares, principalmente no que tange aos dados pessoais sensíveis, haja vista seu demarcado poder de utilização para fins discriminatórios. Demonstra-se como este cenário colocou em voga a compreensão do direito à privacidade no âmbito da economia digital, como também a necessidade de se garantir um direito a autotutela de dados pessoais por parte de seus titulares. Nesta conjuntura, realiza-se a análise de como a *General Data Protection Regularment* e a Lei Geral de Proteção de Dados editadas no contexto da União Europeia e do Brasil, respectivamente, tendo por escopo fundamental regular esta nova gama de direitos emergentes das consequências tecnológicas, equalizando este direito fundamental à proteção de dados pessoais com o desenvolvimento de atividades econômicas que utilizam dados sensíveis como insumo.

Palavras-Chave: Proteção de dados pessoais; Sociedade da Informação; Privacidade; Autotutela; Dados Sensíveis**.**

LISTA DE SIGLAS E ABREVIATURAS

ANPD - Autoridade Nacional de Proteção de Dados

AOL – American Online

ARPA- Advanced Research Agency

ARPANET - Advanced Research Projects Agency Network

BBS - Bulletin Board System

BREXIT – British Exit

EMBRATEL – Empresa Brasileira de Telecomunicações

EUA - Estados Unidos da América

FTC - Federal Trade Commission

GDPR - General Data Protection Regulation

GLBA - Gramm–Leach–Bliley Act

IBGE - Instituto Brasileiro de Geografia Estatística

LGPD - Lei Geral de Proteção de Dados

MILNET - Military Network

MUDs - Multi- User Dungeon

NSA - Agência Nacional de Segurança Nacional

NSF - National Science Foundation

OCDE - Organização para a Cooperação e Desenvolvimento Econômico

RGPD - Regulamento Geral de Proteção de Dados Europeu

TCP/IP - Transmission Control Protocol / Internet Protocol

TIC - Tecnologia da Informação e Comunicação

URSS - União das Repúblicas Socialistas Soviéticas

WWW – World Wide Web

SUMÁRIO

INTRODUÇÃO 1

1. A REVOLUÇÃO DIGITAL E PRINCIPAIS CONSEQUÊNCIAS PARA O DIREITO 3

1.1 A consolidação da sociedade da informação e os novos problemas jurídicos decorrentes 3

1.2 A massificação do acesso à internet e o desenvolvimento da economia digital 5

1.3 O dado pessoal como ativo na economia digital 10

1.4 O dado pessoal sensível 14

2. A PRIVACIDADE DE DADOS PESSOAIS SENSÍVEIS COMO DIREITO DA PERSONALIDADE E SUAS REPERCUSSÕES NO ORDENAMENTO JURÍDICO 19

2.1 A sociedade da informação e a necessidade de uma nova regulamentação legal para a proteção de dados pessoais sensíveis 19

2.2 A evolução histórica do conceito de privacidade de dados pessoais e a consolidação do direito a autotutela de dados como um direito da personalidade 20

2.3 A legislação nacional e internacional prévia para proteção de dados pessoais e sua insuficiência perante a sociedade da informação 24

2.3.1 Aspectos evolutivos da legislação internacional acerca da proteção de dados pessoais 24

2.3.2 Aspectos evolutivos da legislação nacional acerca da proteção de dados pessoais 29

3. O NOVO PANORAMA NORMATIVO TRAZIDO PELA *GENERAL DATA PROTECTION REGULATION* (GDPR) E LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) PARA A PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS E SUAS PRINCIPAIS REPERCUSSÕES ECONÔMICAS 38

3.1 A insuficiência da prévia legislação para garantir a proteção de dados pessoais e a necessidade de um novo diploma específico sobre a matéria 38

3.2 A solução normativa trazida pela General Data Protection Regulation (GDPR) para a proteção de dados pessoais sensíveis 39

3.2 A solução normativa trazida pela Lei Geral de Proteção de Dados (LGPD) para a proteção de dados pessoais sensíveis 46

3.3 O desenvolvimento da atividade econômica com base em dados pessoais sensíveis diante da atual regulamentação 49

CONSIDERAÇÕES FINAIS 52

REFERÊNCIAS 53

INTRODUÇÃO

A discussão e regulamentação jurídica acerca da proteção de dados pessoais no âmbito da sociedade da informação teve sua relevância ressaltada com a divulgação pela mídia internacional de diversos escândalos de vazamento de dados pessoais, dados estes que estavam sendo coletados e manipulados sem qualquer ciência ou autorização de seus titulares. Esta coleta e manipulação de informações pessoais careciam de uma regulamentação jurídica específica e efetiva, demonstrando-se imperiosa sua tutela jurídica no âmbito da economia digital, haja vista que estes dados estavam sendo utilizados para fins transversos sem a ciência de seus titulares, tais como para a indução de escolhas e para fins discriminatórios, com base nos dados pessoais sensíveis coletados.

Esta conjuntura apresentada demonstrou a necessidade de repensar o conceito de privacidade com a emergência das novas tecnologias e também a necessidade de o ordenamento jurídico garantir aos titulares de dados pessoais uma postura ativa perante as informações de sua propriedade que estão sendo coletadas e manipuladas, direitos estes que a *General Data Protection Regularment (GDPR)* e a Lei Geral de Proteção de Dados Pessoais se propõem a garantir.

Desta via, a temática de proteção de dados pessoais é demarcada pela multidisciplinaridade jurídica, devendo ser analisada sob a perspectiva do Direito Constitucional, haja vista sua intrínseca correlação com o direito fundamental à privacidade, mas também sob a ótica do Direito Civil, considerando-se que o novel direito à autotutela de dados pessoais é correlato aos direitos da personalidade, e também sob a perspectiva do Direito Internacional, levando-se em consideração que o fluxo de dados no âmbito da economia digital ocorre de forma transfronteiriça.

O objetivo geral deste trabalho é compreender como os dados pessoais se constituíam como um importante ativo econômico, ressaltando os aspectos jurídicos dos títulos normativos específicos sobre o tema que foram recém editados no contexto europeu e nacional, principalmente no que tange a proteção dos dados pessoais sensíveis e como as atividades econômicas que utilizam estes como insumo serão afetadas.

Desenvolvem-se os objetivos específicos do presente trabalho pela utilização do método de pesquisa bibliográfica, mediante a técnica de revisão e análise de

dados secundários e legislativos, demonstrando as principais consequências da revolução digital para o ordenamento jurídico nacional e internacional, a consolidação do direito à proteção de dados pessoais sensíveis como um direito da personalidade e pela apresentação do novel quadro protetivo para os dados pessoais sensíveis na *General Data Protection Regularment* e na Lei Geral de Proteção de Dados.

Para a condução e desenvolvimento dos objetivos gerais e específicos do presente trabalho, este foi dividido em três capítulos.

A primeiro capítulo delineia como a consolidação da sociedade da informação incorreu na insurgência de novas contendas jurídicas, ressaltando como a massificação do acesso à internet e o firmamento da economia digital contribuíram para tal, firmando-se neste contexto o dado pessoal como um ativo da economia digital e conceituando e delimitando o potencial lesivo da manipulação de dados pessoais sensíveis.

O segundo capitulo trata como o desenvolvimento da sociedade da informação demandou um novo marco legislativo para a proteção de dados pessoais sensíveis, partindo da análise da evolução histórica do conceito de proteção de dados pessoais e a consolidação do direito à autotutela de dados como um direito da personalidade, pela análise da legislação prévia para proteção de dados pessoais na conjuntura internacional e nacional e de como esta foi insuficiente para prevenir os incidentes de vazamento de dados pessoais, delimitando as principais consequências deste evento para os titulares de dados pessoais sensíveis.

O terceiro capítulo assevera como a *General Data Protection Regurlarment* e a Lei Geral de Proteção de Dados Pessoais se propõem a garantir a guarida jurisdicional aos dados pessoais sensíveis e as principais repercussões destas novas legislações na atividade econômica.

Neste interim, o presente trabalho busca asseverar, por intermédio da utilização do método de pesquisa da revisão bibliográfica, as principais consequências da coleta e manipulação de dados pessoais sensíveis no âmbito da sociedade da informação, demarcando a importância da nova legislação europeia e nacional na atividade econômica com base na utilização destes dados.

1. A REVOLUÇÃO DIGITAL E PRINCIPAIS CONSEQUÊNCIAS PARA O DIREITO

1.1 A consolidação da sociedade da informação e os novos problemas jurídicos decorrentes

A análise do panorama de proteção de dados pessoais sensíveis remonta a conceitos disruptivos, cobertos pelo ideário futurista e inovador que os dizem respeito, levando a crer que se trata de uma contenda jurídica que tomou forma apenas nas últimas décadas. Ocorre que, para se compreender o contexto em que a proteção de dados pessoais sensíveis se tornou concretamente uma preocupação jurídica, faz-se mister lançar o olhar para um breve retrospecto das históricas formas de organizações sociais e econômicas humanas.

Isso se faz necessário pois as organizações econômicas e sociais humanas, por mais díspares que sejam entre si, repetem-se sempre em um padrão de desenvolvimento, qual seja: sempre norteadas por um importante elemento que ganha relevância central na época, servindo como propulsor para a economia do período.

Desta vista, na sociedade agrícola o elemento propulsor era a terra produtiva, já na sociedade industrial o desenvolvimento econômico e social se deram em torno da eletricidade e das máquinas à vapor e, após a Segunda Guerra Mundial, ganhou força o terceiro setor, sendo a prestação de serviços o elemento central da economia do momento histórico em referência.

Hodiernamente tem-se na organização social e econômica a estruturação em torno da informação, seja na obtenção, manipulação ou apenas armazenamento desta, consolidando o que se compreende por sociedade da informação. Essa nova estruturação econômica só é possível em razão da evolução tecnológica que possibilita "mecanismos capazes de transmitir informações em uma quantidade e velocidade jamais imaginável"[1], sendo a computação eletrônica e a internet elementos intrínsecos a essa disruptiva forma de organização econômica e social.

Já anteriormente à massificação do acesso à internet pela população, na década de 70 (setenta) o escritor norte-americano Alvin Toffler[2] já destacava a

---

[1] BIONI, Bruno Ricardo. **Proteção de dados pessoais: A função e os limites do consentimento.** Rio de Janeiro. Forense, 2019. P. 34.
[2] TOFFLER, A. apud PINHEIRO, P. **Direito digital.** Saraiva Educação SA, 2016.

emergência desta organização social em torno da informação. Segundo o escritor, em metafórica explicação acerca do funcionamento da sociedade da informação, este vislumbrou que esta seria regida por dois relógios - um analógico e um digital. O relógio analógico regeria o tempo físico, tendo 24 (vinte e quatro) horas por dia e 07 (sete) dias por semana, como já convencionado. Já o relógio digital se regeria pelo tempo virtual, extrapolando os limites convencionais da hora de um dia, acumulando ações a serem realizadas simultaneamente, não importando barreiras como limite geográfico e de fuso horário, ressaltando a importância que a velocidade de tomada de decisão tem dentro desta nova organização social.

Desta maneira, compreende-se por sociedade da informação, perante a sua referência sociológica como:

> (...) um fenômeno paradigmático de transformação social e econômica. Tal paradigma é fundamentado pelo desenvolvimento de tecnologias para agir sobre a informação, cuja inserção integral nas relações sociais e nos processos de pensamento humano implica a consolidação da lógica de redes nos sistemas e processos humanos e à flexibilidade das formas e das instituições[3].

Assim, a sociedade da informação exige cada vez mais a execução de ações de maneira mais célere e o acesso a cada vez mais um volume maior de informações. Trata-se verdadeiramente de um novo modelo socioeconômico e cultural, haja vista que, o grande fluxo de informações por meio da internet acarreta uma uniformização de ideias e procedimentos em nível transnacional. Tomando tais pressupostos por base, pode-se concluir que a universalização do uso da internet foi fundamental para a globalização, que têm intrínseco em seu conceito a uniformização de conhecimento e práticas[4].

Com a emergência de novas tecnologias, a ciência jurídica, como fato social que é, deve se adequar e rever suas disposições normativas para regular as novas

---

[3] CASTELLS, Manuel apud MARTINS, Ana Paula Pereira. **Vazamento e Mercantilização de Dados Pessoais e a Fragilidade da Segurança Digital do Consumidor: um estudo dos casos Netshoes e Uber.** Disponível em: < https://www.researchgate.net/profile/Ana_Martins195/publication/327416131_VAZAMENTO_E_MERCANTILIZACAO_DE_DADOS_PESSOAIS_E_A_FRAGILIDADE_DA_SEGURANCA_DIGITAL_DO_CONSUMIDOR_um_estudo_dos_casos_Netshoes_e_Uber/links/5b8e042e299bf114b7f05bbb/VAZAMENTO-E-MERCANTILIZACAO-DE-DADOS-PESSOAIS-E-A-FRAGILIDADE-DA-SEGURANCA-DIGITAL-DO-CONSUMIDOR-um-estudo-dos-casos-Netshoes-e-Uber.pdf> Acesso em: 19 de outubro de 2019.

[4] SCHERKERKEWITZ, Iso Chaitz. **Direito e internet**. Ed. Revista dos Tribunais, 2014. Págs. 20-21

situações sociais decorrentes das inovações que a massificação do acesso à internet possibilita, sendo a coleta, tratamento e manipulação de dados pessoais sensíveis para fins econômicos um destes inovadores campos que precisam ser regulados juridicamente. É fundamental ressaltar que os avanços tecnológicos tornam também obsoletas específicas lides jurídicas, ao mesmo tempo em que criam uma nova contenda jurídica relativa à proteção de dados pessoais sensíveis que urge por regulamentação[5].

1.2 A massificação do acesso à internet e o desenvolvimento da economia digital

No ordenamento jurídico nacional, o conceito de internet é dado pelo Marco Civil da Internet (Lei 12.965/2014), que em seu artigo 5º, I conceitua a internet como: "o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes"[6].

De forma semelhante a definição dada pelo Marco Civil da Internet, a doutrina especializada define a internet partir dos seguintes conceitos: "uma rede de computadores conectados entre si compartilhando informações e disponibilizando serviços ao redor do mundo" [7], "uma rede aberta decorrente da conexão de várias redes entre si, perfazendo-se a comunicação por meio de um conjunto de protocolos, denominados *Transmission Control Protocol / Internet Protocol (TCP/IP)*"[8] e "um meio de comunicação que interliga dezenas de milhões de computadores no mundo inteiro e permite o acesso a uma quantidade de informações praticamente inesgotáveis, anulando toda distância de lugar e tempo"[9].

A partir destes conceitos, faz-se fundamental salientar a capacidade disruptiva desta tecnologia, pois suas bases estruturais possibilitaram a criação um

---

[5] LEONARDI, Marcel. **Tutela e privacidade na internet**. Editora Saraiva, 2012. P. 27.
[6] BRASIL. LEI Nº 12.965 DE 23 DE ABRIL DE 2014. **Marco Civil da Internet**. Brasília, DF, abril de 2014. Disponível em: < http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm>. Acesso em 22 de setembro de 2019.
[7] FINKELSTEIN, Maria Eugênia Reis apud SCHERKERKEWITZ, Iso Chaitz. **Direito e internet**. Ed. Revista dos Tribunais, 2014. Pág. 13.
[8] MARTINS, Guilherme Magalhães apud SCHERKERKEWITZ, Iso Chaitz. Ob. cit. Pág. 14.
[9] PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. Editora Atlas SA, 2000. Pag. 10-11

verdadeiro mundo virtual, cuja principal característica é a intangibilidade, qual seja, uma nova percepção da realidade, diferente da existência física e palpável, mas de amplo acesso popular[10].

É incontestável a importância que este referido mundo virtual tem na contemporaneidade, a julgar que, com a popularização da internet, o uso desta tecnologia virou atividade intrínseca à vida moderna e o seu uso alterou a forma de comunicação e relacionamento entre as pessoas, empresas e setor público, instituindo que aqueles que não a dominam ficam à margem de acontecimentos e debates hodiernos.

A história do desenvolvimento da internet encontra seu alicerce na capacidade que as pessoas têm de superar "metas institucionais, superar barreiras burocráticas e subverter valores estabelecidos no processo de inaugurar um mundo novo"[11] e esta demonstrou em sua validação social e histórica que a "cooperação e a liberdade de informação podem ser mais propícias à inovação do que a competição e os direitos de propriedade"[12].

Ainda que a evolução estrutural desta tenha passado por diversas etapas, uma característica se fez presente em todas essas, que foi a utilização da internet como meio de facilitação do compartilhamento de informações, que até os dias atuais se constitui como o seu escopo maior.

Ao analisar as bases históricas que serviram de alicerce para a criação da internet, remonta-se a setembro de 1969, data na qual a *Advanced Research Agency (ARPA)*[13] mobilizou uma rede de computadores para dar estrutura a *Arpanet*, que tinha por escopo fundamental a união de recursos para a pesquisa

---

[10] Aquino Júnior, Geraldo Frazão de apud SCHERKERKEWITZ, Iso Chaitz. **Direito e internet**. Ed. Revista dos Tribunais, 2014. Pág. 14.

[11] CASTELLS, Manuel. **A Galáxia Internet: reflexões sobre a Internet, negócios e a sociedade**. Zahar, 2003. p. 13.

[12] *Ibidem*., p. 13

[13] O projeto *ARPANET* foi criado em 1969 com fim exclusivamente militar, conforme política desenvolvida pelo Departamento de Defesa dos Estados Unidos que estimulava a pesquisa no âmbito da computação interativa, com o escopo de estabelecer uma inovadora forma de comunicação entre os diversos centros de pesquisa americanos e o Departamento de Defesa, com a transmissão instantânea das informações de forma segura e com proteção da comunicação na hipótese de um possível ataque nuclear. A tecnologia da *ARPANET* utilizava cabos de conexão subterrâneos, interligando os centros de pesquisa aos comandos militares, sem a definição de um centro específico ou uma rota única de informações. Em 1970 as universidades norte americanas e outras instituições ligadas à defesa do Estado obtiveram permissão para acesso à ARPANET. Em 1983, motivados por possíveis falhas de segurança da *ARPANET*, o Departamento de Defesa Norte Americano criou uma rede independente chamada *MILNET*, passando a *ARPANET* a se chamar de *ARPA – INTERNET* e ser dedicada exclusivamente à pesquisa acadêmica.

tecnológica militar, como forma de sair a frente na corrida armamentista existente à época entre os Estados Unidos da América (EUA) e a extinta União das Repúblicas Socialistas Soviéticas (URSS), dando embasamento ao momento histórico da Guerra Fria. Tal caráter foi imprescindível para o resultado hodierno da internet, como bem delineia Manuel Castells[14]:

> (...) todos os desenvolvimentos tecnológicos decisivos que levaram à Internet tiveram lugar em torno de instituições governamentais e importantes universidades e centros de pesquisa. A Internet não teve origem no mundo dos negócios. Era uma tecnologia ousada demais, era um projeto caro demais, e uma iniciativa arriscada demais para ser assumida por organizações voltadas para o lucro. (...) a Internet se desenvolveu num ambiente seguro, propiciado por recursos públicos e pesquisa orientada para missão, mas que não sufocava a liberdade de pensamento e inovação.

Muito embora este período inicial de aprimoração das bases estruturais da internet com o seu uso para finalidades militares e acadêmicas tenha sido imprescindível para seu resultado como hoje conhecido, para o estudo da proteção de dados pessoais sensíveis faz-se mister analisar tal contexto histórico a partir do momento da popularização e uso comercial da internet. Neste interim, é imperioso fazer um recorte histórico para a década de 80 do século XX, momento em que o Departamento de Defesa Americano inicializou a comercialização da tecnologia da internet, financiando fabricantes de computadores a incluir o TCP/IP - um conjunto de protocolos de comunicação entre computadores em rede - em seus protocolos.

O início dos anos 90 foi ponto de guinada para a massificação do uso da internet. Isso se deu, dentre outros acontecimentos, pela delegação pelo governo americano da administração da internet à *National Science Foundation*, em um contexto em que esta tecnologia já se encontrava dissociada do uso para fins exclusivamente militares e acadêmicos. Assim sendo, tomando por base que a tecnologia das redes de computadores já estava em domínio público e a conjuntura de desregulação das telecomunicações, a *NSF* procedeu pela privatização da internet.

Neste mesmo contexto, vários provedores de internet montaram suas próprias redes e portas de comunicação em bases comerciais, o que corroborou para o exponencial crescimento e popularização desta tecnologia. Outro acontecimento histórico significativo que propiciou a popularização da internet em nível global foi o

---

[14] *Ibidem*. p. 23-24.

desenvolvimento da *www* pelo programador inglês Tim Berners - Lee, pois foi possível a utilização de uma interface gráfica por meio desta aplicação de compartilhamento de informações, o que possibilitou a internet ser escalável a nível mundial[15].

Em sucedâneo, a companhia *Netscape Communications* desenvolveu o primeiro navegador comercial, qual seja o *Netscape Navigator*. Foi neste momento em que a até hoje gigante comercial *Microsoft* ingressou neste nicho de mercado propiciado pelo desenvolvimento e comercialização da internet, por meio do seu software *Windows 95* e seu navegador *Internet Explorer*[16].

Na conjuntura nacional, a internet teve sua estreia no ano de 1993, iniciando sua operação comercial em território brasileiro pela Empresa Brasileira de Telecomunicações (Embratel) em dezembro de 1994.

Cumpre fundamental ressaltar que este amplo acesso à internet é algo buscado pelas políticas públicas nacionais, tal como manifesto no art. 4º, I e II da Lei nº 12.965/2014 (Marco Civil da Internet)[17], abaixo transcrito. Nota-se que este referido escopo legislativo vem sendo atingido, tal como demonstram os resultados da pesquisa de Tecnologia da Informação e Comunicação (TIC) desenvolvida em 2017 pelo Instituto Brasileiro de Geografia Estatística (IBGE) que apurou que 69,8% da população brasileira têm acesso a internet, representando praticamente dois terços da população[18].

> Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:
> I - do direito de acesso à internet a todos;
> II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;

É imperioso compreender também o contexto de desenvolvimento das redes sociais, como forma de traçar uma completa perspectiva da proteção de dados pessoais sensíveis na conjuntura nacional e europeia. As redes sociais são definidas

---

[15] CASTELLS, Manuel. **A Galáxia Internet: reflexões sobre a Internet, negócios e a sociedade**. Zahar, 2003. P. 17.
[16] *Ibidem*., P. 18-19.
[17] BRASIL. LEI Nº 12.965 DE 23 DE ABRIL DE 2014. **Marco Civil da Internet**. Brasília, DF, abril de 2014. Disponível em: < http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm>. Acesso em 29 de setembro de 2019.
[18] **PNAD Contínua TIC 2017: Internet chega a três em cada quatro domicílios do país**. **IBGE, 2019**. Disponível em: < https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/23445-pnad-continua-tic-2017-internet-chega-a-tres-em-cada-quatro-domicilios-do-pais>**.** Acesso em: 29 de setembro de 2019.

como “um conjunto de participantes autônomos, unindo ideias e recursos em torno de valores e interesses compartilhados”[19], “serviços prestados por meio da internet que permitem a seus usuários criar um perfil público, alimentado por dados e informações pessoais, dispondo de ferramentas que permitam a interação com outros usuários, afins ou não ao perfil publicado”[20] e “serviços baseados na web que permitem a indivíduos: (1) construir um perfil público ou semipúblico dentro de um determinado sistema, (2) articular uma lista de outros usuários deste sistema com os quais estabelecer um relacionamento, e (3) visualizar e navegar pela sua lista de conexões e pela aquela de outros através dos sistemas ”[21].

Este cenário de criação das redes sociais fora propiciado pela consolidação do e-mail como meio de comunicação com velocidade, preço e robustez não observada em qualquer outra modalidade tradicional de comunicação. A implementação das tecnologias da informação no âmbito da comunicação pessoal remonta à década de 70, momento em que comunidades de usuários agregadas em torno das *Bulletin Board System (BBS),* software que permite a ligação via telefone a um sistema através do computador para interação*,* demonstraram a viabilidade da formação e administração de uma rede social intermediada pela tecnologia da informação.

Outro momento histórico expressivo para o fenômeno das redes sociais online se deu em 1984 com a criação da AOL – *American Online*, empresa que disponibilizou as primeiras ferramentas para criação de perfis online, em que os usuários elaboravam descrições pessoais, criavam comunidades virtuais para compartilhamento de informações e posteriormente disponibilizando um sistema de mensagens instantâneas. Ainda na década de 80 (oitenta), os jogos MUDs *(Multi-User Dungeon)*, se estabeleceram como grandes precursores das redes sociais, criando ambientes virtuais em que as pessoas se conectam e se relacionam entre si assumindo um avatar, tal como no *Second Life*.

---

[19] TOMAÉL, Maria Inês et alii. **Das redes sociais à inovação**. Disponível em: <scholar.google.com.br – scielo.br>. Acesso em 29 de setembro de 2019.

[20] Agencia Española de Protección de Datos / Instituto Nacional de Tecnologías de la Comunicación *apud* DONEDA, Danilo. **Reflexões sobre proteção de dados pessoais em redes sociais**. **Revista Internacional de Protección de Datos Personales**, n. 1, 2012. Pág. 6.

[21] DANAH BOYD, Nicole Ellison apud DONEDA, Danilo. **Reflexões sobre proteção de dados pessoais em redes sociais. Revista Internacional de Protección de Datos Personales**, n. 1, 2012. Págs. 3-4.

A expressão hodierna das redes sociais, com a interação direta entre os usuários, teve início a partir do ano de 1997, com os usuários se inscrevendo e elaborando perfis pessoais para se relacionar com demais usuários, atividade esta que pressupõe o tratamento de dados pessoais, sendo a primeira destas a rede social *Six Degrees*[22]*.* Ainda se ressalta a importância do ano de 2004 para o desenvolvimento destas redes sociais, tendo em vista que no ano em referência foram criados o *Flickr*, *Ortuk* e o *Facebook*[23]*.*

A popularização e massificação do uso das redes sociais foram imprescindíveis para a constituição do cenário hoje delineado como economia digital, que tem como pressuposto novos parâmetros de comunicação humana, de consumo e novas formas de interação política, trazendo um novo âmbito econômico a ser explorado. A constituição da economia digital consolidou a era do *Networking Intelligence,* que têm como pedra angular a digitalização da economia. Antes a esta consolidação, o fluxo de informações se dava através do papel, diferentemente da contemporaneidade, em que se há o acesso a um número quase ilimitado de informações de forma virtual e imediata.

Reiterando a importância dos dados na economia hodierna, ao descrever os aspectos mais importantes da economia digital, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) destaca justamente a importância dos dados para este novo momento econômico, incluindo o uso do *big data* e os aspectos da conexão interpessoal, principalmente no que tange a participação de usuários e engajamento destes, que são aspectos marcantes das redes sociais e que só foram possíveis devido a massificação do acesso à internet[24].

1.3 O dado pessoal como ativo na economia digital

> Dados não são o novo ouro, dados são o novo urânio. Algumas vezes se pode fazer dinheiro a partir dele, mas este pode ser radioativo, perigoso

[22] DONEDA, Danilo. Reflexões sobre proteção de dados pessoais em redes sociais. **Revista Internacional de Protección de Datos Personales**, n. 1, 2012. Págs. 3-4.
[23] D´AQUINO, Fernando. **A história das redes sociais: como tudo começou**. Disponível em www.tecmundo.com.br. Acesso em 29 de setembro de 2019.
[24] OCDE. **Addressing the Tax Challenges of the Digital Economy, Action 1 - 2015 Final Report, OECD/G20 Base Erosion and Profit Shifting Project**. OECD Publishing, Paris, 2015. Disponível em: <http://dx.doi.org/10.1787/9789264241046-en>. Acesso em 29 de setembro de 2019.

> para estocar, tem usos militares e geralmente você não o quer em grandes quantidades e é regulado. Por que manter urânio que você não precisa?[25].

Entende-se por dado pessoal, “qualquer informação relativa a uma pessoa singular identificada ou identificável”[26], ou como “informações relativas a uma pessoa viva, identificada ou identificável, assim como o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa”’[27] e também como as “informações e metainformações criadas por e sobre as pessoas, tais como: dados oferecidos voluntariamente, dados observados e dados inferidos[28].

No estudo de dados pessoais é usual remontar a definição dada em 2006 pelo cientista de dados britânico Clive Humby de que os dados são o novo petróleo. Corrobora para este entendimento a atual configuração do cenário econômico em que as empresas com maior valor de mercado - quais sejam *Google*, *Amazon*, *Apple*, *Facebook,* e *Microsoft* - são justamente as que utilizam dados como insumo para o produto final que ofertam ao mercado consumidor, substituindo um tradicional modelo de negócios em que as empresas mais valoradas economicamente eram da tradicional indústria petrolífera.

Da mesma forma que o petróleo era na década de 80 do século XX o *commodity* que dava base aos produtos oferecidos pelas empresas melhores estruturadas economicamente no cenário anterior, na atual conjuntura, os dados são o insumo que dão suporte as novas tecnologias transformativas, quais sejam as de base com inteligência artificial, automação em múltiplos níveis, *marketing* direcionado e avançada análise preditiva. Ainda se aproveitando da definição dada por Clive Humby, de forma análoga, os dados também têm um valor inerente,

---

[25] VALSORDA, Filippo. Disponível em: <https://twitter.com/filosottile/status/1162404848073170944>. Acesso em 12 de outubro de 2019. Tradução livre da autora. Original: Data is not the new gold, data is the new uranium. Sometimes you can make money from it, but it can be radioactive, it’s dangerous to store, has military uses, you generally don’t want to concentrate it too much, an it’s regulated. Why do keep uranium you don’t need?

[26] Diretiva 95/46/CE do Parlamento Europeu e do Conselho apud SILVEIRA, Sergio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce. **A privacidade e o mercado de dados pessoais| Privacy and the market of personal data**. Liinc em Revista, v. 12, n. 2z, 2016.P. 219.

[27] **O que são dados pessoais?** Comissão Européia. Disponível em: < https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt#resposta > Acesso em 05 de outubro de 2019.

[28]WEF – World Economic Forum apud SILVEIRA, Sergio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce. **A privacidade e o mercado de dados pessoais| Privacy and the market of personal data**. Liinc em Revista, v. 12, n. 2, 2016.P. 219

fazendo-se mister o seu processamento, igualmente como o petróleo precisa do refino, para que o seu verdadeiro valor de mercado seja demonstrado.

Porém, a utilização econômica dos dados se distancia de forma latente da exploração comercial do petróleo, haja vista que os dados são uma fonte inesgotável, durável e reutilizável, podem ser replicados infinitamente e transportados ao redor do globo com a velocidade propiciada pela fibra óptica, tornando - se mais acurados a medida que são mais processados e, principalmente na sua vertente do *big data,* que são grandes volumes de dados com capacidade de retirar valor destas informações em segundos*,* podem se apresentar das mais variadas formas, quais sejam: palavras, figuras, sons, ideias, fatos, medidas, estatísticas ou qualquer outra matéria que possa ser processada por um computador e transformada em informação digital[29].

Muito embora grande parte dos serviços oferecidos por estas empresas não cobrem nenhum valor de inscrição para seus usuários, estas 05 (cinco) companhias faturaram juntas no primeiro trimestre de 2017 o valor acumulado de 25 (vinte e cinco) bilhões de dólares[30].

Para compreender como este modelo de negócios que têm por base a coleta, processamento e utilização de informações de caráter pessoal em grande volume se faz lucrativa, é imperativa a transcrição do posicionamento de Ilse Aigner, ministra do consumo da República Federal da Alemanha, *in litteris*: “Todos os que visitam um site de uma rede social devem ter consciência de que se trata de um modelo de negócio. O serviço oferecido não é gratuito. Nós, usuários pagamos por este serviço com as nossas informações privadas”[31]. Em igual sentido define também Sérgio Amadeu da Silveira:

> Gerado pelas identidades e comportamentos, pelos indivíduos em suas ações em redes digitais, os dados pessoais são a moeda paga pelo uso

[29] **Here’s Why Data Is Not The New Oil**. Bernard Marr, Forbes, 2018. Disponível em: <https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/#292b93b23aa9> Acesso em 05 de outubro de 2019.

[30] **The world’s most valuable resource is no longer oil, but data**. The Economist, 2017. Disponível em <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data >. Acesso em 05 de outubro de 2019.

[31] AIGNER, Ilse *apud* DONEDA, Danilo. **Reflexões sobre proteção de dados pessoais em redes sociais**. Revista Internacional de Protección de Datos Personales, n. 1, 2012.

> gratuito de plataformas, sites e serviços online. Dados pessoais se tornaram um importante bem econômico[32].

De acordo com o estudo *Exploring the economics of personal data: a survey of methodologies for mesuring monetary value* desenvolvido pela OCDE, a mensuração do valor monetário de mercado destes dados pode ser estimada por quatro diferentes métodos, quais sejam: a capitalização de registros de dados ou o lucro líquido por registro, os preços de comercialização dos dados nos diversos mercados, os custos da violação de dados e os preços dos dados praticados no mercado ilegal[33].

Neste mister, a exploração dos dados pessoais dos usuários se constituiu como fator vital para a consolidação da já citada economia digital, sendo usados de forma escalável e dando azo a constituição de uma fatia de mercado com base na coleta, extração, agregação, análise, codificação e monetização destes[34].

Na circunstância apresentada, os dados pessoais se formalizaram como uma nova fonte de valor econômico, tendo em vista que, uma vez que são processados e classificados, estes fornecem informações relevantes para melhorar a experiência de consumo, a eficácia de transações e qualidade de produtos, bem como identificar macrotendências em diversos setores.

Sobre a consolidação da economia da informação com base na exploração de dados, cumpre fundamental colacionar o entendimento do jurista Sérgio Amadeu da Silva[35], qual seja:

> Para obter a atenção das pessoas em uma sociedade que utiliza casa vez mais a comunicação em rede, surgem especialistas na atração dos sentidos e na formulação de estratégias nesse cenário de uma macroeconomia da atenção. Algumas companhias desenvolvem *softwares* que geram estatísticas e analisam o comportamento pessoal outras criam soluções para obter dados das pessoas e acompanhar sua navegação na internet com o objetivo de analisar suas escolhas (...). Qual a matéria-prima para a produção de uma ciência da indução do comportamento social em uma sociedade articulada pelas redes digitais? Sem dúvida, os dados pessoais são o elemento-chave para a formação de perfis de comportamento, de consumo e até de opções culturais e políticas. (...) a sociedade informacional, pós-

---

[32] SILVEIRA, Sergio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce**. A privacidade e o mercado de dados pessoais| Privacy and the market of personal data**. Liinc em Revista, v. 12, n. 2, 2016. P. 220.

[33] Organização para Cooperação e Desenvolvimento Econômico *apud Ibidem*. P. 222.

[34] BIONI, Bruno Ricardo. **Proteção de dados pessoais: A função e os limites do consentimento.** Forense, 2019. P. 39.

[35] DA SILVEIRA, Sergio Amadeu. **Tudo sobre tod@ s: Redes digitais, privacidade e venda de dados pessoais**. Edições Sesc, 2017.

> industrial, enredada por tecnologias cibernéticas modificou o mercado capitalista a ponto de torná-lo dependente de uma microeconomia da interceptação de dados pessoais.

Neste cenário, faz-se mister salientar o conceito de ubiquidade no processamento de dados, que indica que todos os âmbitos da vida moderna estão permeados pelo tratamento de dados pessoais, tendo em vista a inúmera quantidade de equipamentos eletrônicos que fazem parte do cotidiano moderno, armazenando toda e qualquer tipo de informação com estes transacionada[36].

É neste contexto que se consolidou uma economia da vigilância, em que o usuário se porta como mero expectador de suas informações[37], tendo em vista que estas, ao serem triadas por *softwares* nos bancos de dados em que são armazenadas, são agrupadas, classificadas e analisadas, inferindo todo tipo de conclusões possíveis que norteiam decisões e escolhas que podem vir perpetuar estigmas sociais[38].

Ao mesmo tempo em que a lucratividade em cima de dados pessoais se consolida como uma intromissão a privacidade individual, não existe óbice jurídico para prevenir este modelo de negócios de se expandir, apenas pela razão de ser baseado no processamento de informações pessoais[39].

1.4 O dado pessoal sensível

A conceituação de dado pessoal sensível no ordenamento jurídico nacional foi originalmente prevista no artigo 3º, § 3º, II da Lei nº 12.414/2011 (Lei de Cadastro Positivo)[40], que enuncia, *in litteris*:

> Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei. (...)
> § 3º Ficam proibidas as anotações de: (...)

---

[36] MENDES, Laura Schertel. **Privacidade e dados pessoais. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação**. Panorama Setorial da Internet. Número 2. Junho, 2019. Ano 11. P. 01.

[37] BIONI, Bruno Ricardo. **Proteção de dados pessoais: A função e os limites do consentimento.** Forense, 2019. P. 39.

[38] CASTRO, Luiz Fernando Martins. **Proteção de dados pessoais-panorama internacional e brasileiro.** Revista CEJ, v. 6, n. 19, p. 40-45, 2002. P. 41.

[39] ESTEVE, Asunción. **The business of personal data: Google, Facebook, and privacy issues in the EU and the USA**. International Data Privacy Law, v. 7, n. 1, p. 36-47, 2017. P. 36.

[40] BRASIL. LEI Nº 12.414 DE 09 DE JUNHO DE 2011. **Lei do Cadastro Positivo**. Brasília, DF, junho de 2011. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em 12 de outubro de 2019.

> II - Informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

Em sentido semelhante, o Regulamento Geral de Proteção de Dados Europeu (RGPD) amplia as hipóteses de dados pessoais sensíveis que merecem a guarida estatal, tal como se observa em seu *Chapter* 2, art. 9º, 1[41], abaixo transcrito:

> Processar dados pessoais que revelem origem étnica ou racial, opiniões políticas, religiosas ou crenças filosóficas, filiação a sindicato e o processamento de dados genéticos, dados biométricos para o propósito único de identificação da pessoa natural, dados concernentes à saúde ou dados concernentes à vida sexual de uma pessoa natural ou orientação sexual deve ser proibido.

Inspirada na legislação sobre proteção de dados europeia, a Lei Geral de Proteção de Dados Brasileira (Lei nº 13.709/2018) se orienta em sentido semelhante, incluindo mais hipóteses de dados pessoais sensíveis no ordenamento jurídico nacional por meio do artigo 5º, II da referida lei[42], qual seja:

> Art. 5º Para fins desta Lei, considera-se: (...)
> II – dado pessoal sensível: o dado pessoal sobre 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.

Cumpre fundamental relacionar que estes dados sensíveis são majoritariamente coletados com anuência concedida pelo usuário mediante aceite em termos de uso, cuja leitura não é habitual, mitigando de forma latente o poder de autodeterminação dos titulares sob estes. Nota-se uma ausência na efetividade do consentimento para a utilização dos dados, decorrendo muitas vezes em prejuízos sociais e econômicos, haja vista que estes termos de uso não são passíveis de

---

[41] UNIÃO EUROPÉIA. Regulation 2016/679 of The European Parliament and of The Council of 27 april 2016. **General Data Protection Regulation**. Disponível em: < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 12 de outubro de 2019. Tradução livre da autora. Original: Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

[42] BRASIL. LEI Nº 13.709 DE 14 DE AGOSTO DE 2018. **Lei Geral de Proteção de Dados Pessoais**. Brasília, DF, agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 12 de outubro de 2019.

negociação entre o usuário e a plataforma, tendo em vista que a sua não aceitação pelo usuário acarreta a sua impossibilidade de acesso[43].

Para ter uma melhor compreensão da sensibilidade destes dados coletados na forma acima relatada e a razão pela qual a sua proteção se faz tão imperiosa, cumpre colacionar dois casos em que a coleta, vazamento e tendenciosa manipulação destes se mostrou negativa para seus titulares.

O primeiro caso ocorreu no ano de 2016, e diz respeito ao vazamento da base de doadores da *Red Cross Blood Service*, uma prestadora de serviços de coleta de sangue para doação na Austrália. Na oportunidade do vazamento do banco de dados desta instituição, cerca de 550.000 (quinhentos e cinquenta mil) doadores tiveram informações como: nome, gênero, endereço e data de nascimento expostas à público, mas, que por si só, não se enquadravam no conceito de dados pessoais sensíveis. Ocorre que, associada a essas informações vazadas, um dado de caráter especialmente sensível do questionário respondido pelo doador também foi a público, qual seja se este tinha comportamento sexual de risco. No momento a *Red Cross Blood Service* pediu desculpas formais aos seus doadores e disponibilizou um aparato de atendimento para aqueles que tiveram seus dados violados.

O segundo caso em análise trata-se de uma medida anunciada em 2014 pelo governo chinês, que declarou que implementará a partir de 2020, um sistema de crédito social ou *social scoring* obrigatório para todos os cidadãos, como maneira de verificar a fidelidade destes aos princípios e valores defendidos pela política estatal. A proposta do referido sistema de *social scoring* é categorizar e taxar os comportamentos de sua população como positivos ou negativos perante a visão do Estado, sendo elaborada uma classificação única e pública do cidadão, que servirá de requisito para o acesso à determinadas políticas públicas. O documento público de planejamento deste sistema de crédito social elucida que este forjará um ambiente de opinião pública em que manter a confiança é reconhecido

[43] MASILI, Clarissa Menezes Vaz. **Regulação do uso de dados pessoais no Brasil: papel do usuário na defesa de um direito à tutela de dados pessoais autônomo**. 2018. P. 47- 48.

positivamente, fortalecendo a sinceridade nos assuntos do governo, comércio, a sinceridade social e a construção da credibilidade judicial[44].

Em ambos os casos supra relatados, não se visa proteger unicamente a privacidade dos titulares dos dados pessoais sensíveis, mas também que estas informações não sejam utilizadas e manipuladas contra seus donos, impondo-lhes restrições de acesso a serviços públicos e privados e até mesmo o exercício de direitos.

O tratamento dos grandes volumes de dados inseridos no *big data*, uma grande base de dados que, por meio de avançadas técnicas computacionais levam a acuradas análises probabilísticas, cujos resultados concernem diretamente a interesses de um grupo social, podem retirar a capacidade de autonomia dos titulares desses dados, assim como o seu direito de acesso a consumo de bens e serviços e a determinadas políticas públicas[45].

Desta maneira, um viés protetivo especial sob as possibilidades de tratamento destes dados visa justamente garantir os fundamentos do Estado Democrático de Direito, haja vista que o uso discriminatório de dados pessoais sensíveis é uma violação latente aos direitos humanos fundamentais, dada as características e natureza dos dados pessoais sensíveis.

Neste mesmo sentido elucida o jurista Stefano Rodotà, citando os juristas L.M. Friedman e J. Rosen, *in litteris*:

> (...) coletar dados sensíveis e perfis sociais e individuais pode levar à discriminação; logo, a privacidade deve ser vista como 'a proteção de escolhas de vida contra qualquer forma de controle público e estigma social' (L. M. Friedman), como a 'reivindicação dos limites que protegem o direito de cada indivíduo a não ser simplificado, objetivado e avaliado fora de contexto'[46].

Faz-se mister salientar que, muito embora o conceito de dado pessoal seja residual ao conceito de dado pessoal sensível, esta não é uma definição estanque. Isso se dá porque identificadores comuns como: nome, número de identificação, dados de localização, identificadores eletrônicos (aparelhos, aplicações, ferramentas

---

[44] MULHOLLAND, Caitlin Sampaio. **Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18).** Revista de Direitos e Garantias Fundamentais, v. 19, n. 3,2018. p. 160 – 162.

[45] *Ibidem*.

[46] RODOTÁ, Estefano *apud* MULHOLLAND, Caitlin Sampaio. **Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18).** Revista de Direitos e Garantias Fundamentais, v. 19, n. 3,2018. p. 165.

e protocolos como o endereço de IP, *cookies* e etiquetas de identificação por radiofrequência) que, *a priori*, não são dados sensíveis sobre seus titulares podem se tornar quando combinados com outras informações que levam à dados sensíveis sobre seus titulares e ainda a definição de perfis destes.

Assim sendo, conclui-se que a linha que distingue o que se constitui como dado pessoal e dado pessoal sensível é bastante tênue, devendo se considerar que a perspectiva de análise deve ser dinâmica e não estática. Por conseguinte, é imperioso definir que são dados pessoais sensíveis todas aquelas informações que permitem que se chegue, como resultado final, a informações sensíveis a respeito de seus titulares[47].

[47] FRAZÃO, Ana. **Nova LGPD: o tratamento dos dados pessoais sensíveis**. Disponível em: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018>. Acesso em: 11 de outubro de 2019.

2. A PRIVACIDADE DE DADOS PESSOAIS SENSÍVEIS COMO DIREITO DA PERSONALIDADE E SUAS REPERCUSSÕES NO ORDENAMENTO JURÍDICO

2.1 A sociedade da informação e a necessidade de uma nova regulamentação legal para a proteção de dados pessoais sensíveis

O autor Zygmunt Bauman já enunciava a ubiquidade no conceito de privacidade na conjuntura da sociedade da informação, tal como se observa:

> (...) submetemos à matança nossos direitos de privacidade por vontade própria. Ou talvez apenas consintamos em perder a privacidade como preço razoável pelas maravilhas oferecidas em troca. Ou talvez, ainda, a pressão no sentido de levar nossa autonomia pessoal para o matadouro seja tão poderosa, tão próxima à condição de um rebanho de ovelhas, que só uns poucos excepcionalmente rebeldes, corajosos, combativos e solutos estejam preparados para a tentativa séria de resistir[48].

A discussão sobre a proteção de dados pessoais no âmbito da sociedade da informação teve seu debate impulsionado em 2013, motivada pela divulgação do esquema de vigilância massiva instaurado sobre cidadãos norte-americanos e líderes de Estado do mundo inteiro, coordenado pela Agência Nacional de Segurança Nacional (NSA) dos Estados Unidos da América (EUA), revelado a mídia internacional pelo ex agente de segurança governamental Edward Snowden.

A necessidade de uma nova compreensão do conceito de privacidade de dados pessoais e de sua proteção no novo contexto da economia digital foi impulsionado também pelo acontecimento de grande repercussão midiática envolvendo o *Facebook* e a empresa *Cambridge Analytica,* que, sem qualquer consentimento dos usuários da rede social, utilizaram de avançadas técnicas de psicometria e *marketing* direcionado como forma de favorecer a eleição presidencial norte-americana de Donald Trump, o referendo sobre a saída do Reino Unido da União Europeia (*Brexit*) e também com indícios de participação nas eleições brasileiras.

Ambos os acontecimentos foram possibilitados por um cenário traçado a partir do início do século XXI (vinte e um), momento em que o cotidiano social passou a

---

[48] BAUMAN, Zygmunt. **Vigilância Líquida**. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2014. p. 28.

ser massivamente permeado pela presença das Tecnologias da Informação (TIC). Este cenário determinou uma transformação qualitativa e quantitativa nos efeitos decorrentes da coleta de informações por meio destas tecnologias, como se demonstra em ambos os casos supracitados, tendo em conta que o vazamento e a incorreção de dados pessoais se constituem como uma nova forma de intromissão à intimidade da pessoa.

Na contemporaneidade, a internet se estabelece como um mercado e isso acarreta na transformação da privacidade de um direito fundamental a um *commodity*, a julgar que que esta tecnologia possibilita não só o acumulo de informações ilimitadas sobre o indivíduo, tais como sua condição física, mental, econômica, opiniões políticas e religiosas, mas torna possível também confrontar, agregar, rejeitar e comunicar essas informações concernentes ao indivíduo[49].

Reguladores econômicos, agentes empresariais e vasta literatura especializada já demarcam a importância da atual conjuntura econômica baseada no processamento dessas informações pessoais em larga escala (*Big Data*), cenário este que tende a demarcar o futuro econômico, corroborando para novas preocupações acerca do já conhecido problema jurídico da proteção da privacidade individual[50].

Neste interim, o contexto socioeconômico de circulação de dados informáticos em grandes volumes esvaziou o conteúdo de inúmeras e generosas leis que tutelam a privacidade, se fazendo necessário uma proteção legislativa especifica ao direito de controle sobre as próprias informações.

2.2 A evolução histórica do conceito de privacidade de dados pessoais e a consolidação do direito a autotutela de dados como um direito da personalidade

O histórico do tráfego eletrônico online de determinado usuário revela um perfil detalhado e acurado sobre a pessoa física que o detém, haja vista que este histórico é uma expressão direta de suas preferências, interesses pessoais, situação

[49] PAESANI, Liliana Miniardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil.** São Paulo: Atlas, 2000. P. 51.
[50] VALENTE, Jonas**. Privacidade em Perspectivas**. Organizadores: Sérgio Branco, Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018. P.115.

afetiva e hábitos de consumo[51], fazendo estes dados, em determinadas circunstâncias, às vezes do seu titular, em situações que em outros períodos sua presença física seria indispensável[52].

O próprio *modus operandi* da navegação da *web* pressupõe o registro de dados que *a priori* não são sensíveis, tais como: endereços de IP, *cookies* e históricos de navegação, criando este acervo verdadeiros perfis pessoais dos usuários com valor econômico agregado[53], podendo estas informações, quando combinadas a outras, revelar dados de caráter sensível sobre seu titular. Por isso que a atividade de tratamento de dados pessoais é de alto risco aos direitos fundamentais, pois estes são expressão direta da personalidade do usuário[54].

Em um contexto inicial a proteção de dados pessoais foi correlacionada diretamente com o direito à privacidade dos dados dos titulares usuários, tendo a evolução deste conceito perpassado diferentes períodos históricos e sociais, sendo a sua contemporânea compreensão uma correlação direta das peculiaridades de cada um destes momentos, sendo correlatos a este conceito de privacidade o direito à vida privada, intimidade e sigilo.

O direito em comento teve seus primeiros delineamentos no século XIX (dezenove), no contexto histórico do Iluminismo e após o fim da Revolução Francesa, momento em que houve o reconhecimento de que o ser humano tem direitos fundamentais inatos, quais sejam os direitos humanos de primeira geração, que pressupõem uma atuação negativa do Estado, ou seja, uma abstenção de atuação deste e de ingerência na esfera da liberdade, autonomia e intimidade individual, elementos que tiveram destaque com a ascensão da burguesia ao poder político.

Esboços do que se compreende por direito à privacidade eram observados nas obras políticas da época, que já destacavam a autonomia dos cidadãos para disposição de sua individualidade e seus atributos. Predominava a noção individualista, sendo a privacidade decorrente do conceito de propriedade e

---

[51] SCHERKERKEWITZ, Iso Chaitz. **Direito e internet**. Ed. Revista dos Tribunais, 2014. P. 127.
[52] DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, p. 91-108, 2011.P. 92.
[53] SCHERKERKEWITZ, Iso Chaitz. **Direito e internet**. Ed. Revista dos Tribunais, 2014. P. 127.
[54] DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, p. 91-108, 2011.P. 92

compreendida como o exercício da liberdade de ser deixado só, correlato também ao direito à intimidade[55].

Fundamental ressaltar que, neste momento histórico, a privacidade era um direito exclusivamente burguês, não alcançando integralmente a sociedade da incipiente Idade Moderna. Isso ocorria porque o exercício do direito de privacidade era associado a constituição de um local privado para a consolidação da individualidade, pois era correlacionado a um aspecto físico e tangível, conexo ao direito de propriedade, direito este que nem toda a sociedade exercia pois grande parte não tinha condições financeiras de estabelecer sua própria habitação de forma separada do ofício[56].

A privacidade passou a ter seu delineamento como direito autônomo em 1890, em decorrência da publicação do artigo *The Right to Privacy* na revista acadêmica *Harvard Law* de autoria de Louis Brandeis e Samuel Warren, motivados pelo surgimento das novas tecnologias da informação, quais sejam o jornal e a fotografia e as ainda desconhecidas consequências dos primórdios da comunicação em massa.[57] Estes autores aproveitaram da perspectiva aberta de privacidade elaborada pelo magistrado norte-americano Thomas Cooley[58], qual seja o direito de ser deixado sozinho, demonstrando que muitos dos elementos que davam guarida judicial ao conceito de privacidade já estavam positivados na lei. Deste modo, o valor da privacidade não seria medido pela vantagem econômica obtida pela sua violação, mas sim na paz mental e tranquilidade que a ausência de qualquer violação proporcionaria ao seu titular[59].

Neste interim, a tutela jurídica da privacidade passou a se desvincular da tutela de um patrimônio físico, como era compreendido no contexto de sua constituição, e passou a ser entendida como um direito de determinar se, a quem e em que medida o indivíduo quer expor seus pensamentos, sentimentos e emoções, associada também a uma proteção destas informações. Seria o direito de não tornar

---

[55] MASILI, Clarissa Menezes Vaz. **Regulação do uso de dados pessoais no Brasil: papel do usuário na defesa de um direito à tutela de dados pessoais autônomo**. 2018. P. 23 - 25.
[56] *Idem. Ibdem.*
[57] DONEDA, Danilo. **Pessoa e privacidade na sociedade da informação, Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006. p. 85.
[58] MAGRANI, Eduardo. **Direito e Tecnologia**. Rio de Janeiro: FGV, 2016. P. 23.
[59] SOLOVE, Daniel J. **Conceptualizing Privacy**. California Law Review, California, v. 90, jul. 2002. p. 1100

público o conhecimento de certos dados pessoais, demonstrando-se ainda fortemente vinculado aos ideais de autonomia e liberdade[60].

A privacidade passa a ter seu aspecto positivo reconhecido a partir do século XX (vinte), com a construção jurisprudencial dos tribunais norte-americanos que passaram a adotar a prática de anular leis com base no direito à privacidade. Isto ocorreu tomando por pressuposto o entendimento de que as normas jurídicas não poderiam adentrar a seara da liberalidade pessoal, pois acabariam ocasionando uma padronização dos indivíduos e da sociedade. Neste contexto apresentado, o direito à privacidade assegura o direito à personalidade, haja vista que se modula como um direito à autodefinição em relação a alguns aspectos da vida, não podendo o Estado impor comportamentos ou um modo de vida. Neste interim a privacidade era compreendida como o direito de não ter o curso da vida determinado pelo Estado em prol das demandas governamentais[61].

Diante do exposto, conclui-se que a privacidade é um elemento precípuo da formação da pessoa, não se tratando de mera preferência pessoal, mas consolidando-se como o que o indivíduo é de fato, ou seja, suas fronteiras e grau de interação com os demais[62].

Ocorre que, com a emergência das novas possibilidades tecnológicas propiciadas pela internet e a consolidação da sociedade da informação, o direito à privacidade por si só não era mais suficiente para estabelecer um equilíbrio na relação que se formou em torno da crescente importância financeira dada ao dado pessoal[63], pois o direito à privacidade destes pressupõe apenas o controle de acesso dessas informações pessoais. Dá-se azo ao direito à autotutela dos dados pessoais, correlato aos direitos da personalidade[64].

Neste escopo, faz-se imperioso destacar que os direitos da personalidade se tratam de uma verdadeira cláusula geral de proteção da pessoa humana, sendo por isso dotados de elasticidade, ou seja, não se exaurem no rol dos artigos 11 a 21 do

---

[60] MASILI, Clarissa Menezes Vaz. **Regulação do uso de dados pessoais no Brasil: papel do usuário na defesa de um direito à tutela de dados pessoais autônomo**. 2018. P. 25.
[61] *Idem. Ibdem.*
[62] MAGRANI, Eduardo. **Direito e Tecnologia**. Rio de Janeiro: FGV, 2016. P. 21.
[63] DA COSTA, Mariana Monteiro. **A Era da Vigilância no Ciberespaço e os Impactos da Nova Lei Geral de Proteção de Dados Pessoais no Brasil: Reflexos no Direito à Privacidade.** Rio de Janeiro, 2018.
[64] BIONI, Bruno Ricardo. **Proteção de dados pessoais: A função e os limites do consentimento.** Forense, 2019. P. 99.

Código Civil Nacional. Estes estão constante aperfeiçoamento, cabendo o enquadramento da proteção de dados pessoais e sua autotutela como uma nova variante desta referida categoria jurídica, sendo essa tutela dinâmica uma ferramenta para proteger o desenvolvimento da pessoa humana[65].

Tomando por pressuposto que os direitos da personalidade são projeção da pessoa humana, um dado atrelado à esfera pessoal caracteriza-se verdadeiramente como uma extensão de seu titular, devendo esta nova identidade digital externar fidedignamente a singularidade do seu detentor[66] e tendo este o direito de controlá-lo e retificá-lo em hipótese de erro.

Por meio desta novel classificação dos direitos da personalidade, o indivíduo titular de dados pessoais não se porta mais como mero fornecedor destes mas tem atuação também ativa no controle de seus dados. Trata-se de um verdadeiro direito fundamental à autodeterminação informativa, tendo em vista que, embora os dados pessoais estejam em domínio público, estes também se inserem na esfera de proteção de seu titular. O exercício deste direito de autotutela independe da ofensa à privacidade, pois, como estes dados são projeção da própria personalidade, devem ser acurados independente da violação da privacidade destes[67].

2.3 A legislação nacional e internacional prévia para proteção de dados pessoais e sua insuficiência perante a sociedade da informação

2.3.1 Aspectos evolutivos da legislação internacional acerca da proteção de dados pessoais

Para delinear a progressão legislativa das normas jurídicas que se propõem a proteção e controle de dados pessoais no âmbito internacional, cumpre imperioso aproveitar-se da classificação desenvolvida por Viktor Mayer-Scöberger, sistemática esta que divide quatro gerações de evolução das normas sobre o tema, partindo de um enfoque mais técnico e restrito até a atual concepção normativa, com técnicas

---

[65] *Idem. Ibdem.*
[66] *Idem. Ibdem.* P. 97- 99.
[67] MASILI, Clarissa Menezes Vaz. **Regulação do uso de dados pessoais no Brasil: papel do usuário na defesa de um direito à tutela de dados pessoais autônomo**. 2018. P. 28-33.

mais condizentes e eficazes para a realidade da tecnologia que se visa tutelar, intrinsecamente correlacionada aos direitos fundamentais do cidadão[68].

A primeira geração de leis de proteção de dados pessoais foi reflexo direto do estado bruto em que a tecnologia se encontrava à época, assim como a restrita visão que os juristas tinham sobre estas, normatizando juridicamente os bancos de dados, assim como o Estado e suas estruturas administrativas quando no exercício da mesma função. As normas jurídicas concernentes a esta primeira geração constituíam meros permissivos jurídicos para autorização de criação de banco de dados e para o posterior controle da atividade destes por entidades públicas reguladoras[69].

Estando sistematicamente incluído na primeira geração de leis protetivas de dados pessoais, mas ainda previamente a existência dos bancos de dados informáticos, na Inglaterra a compreensão de privacidade da vida íntima e familiar remonta ao ano de 1849. Desde então vêm sendo acolhido pelas Cortes Judiciais Inglesas a ideia da quebra de confidencialidade, que pressupõe para sua configuração a divulgação de informação confidencial, a obrigatoriedade do sigilo desta e o uso não autorizado da notícia. Neste interim, consolidou-se na conjuntura legal inglesa o *Press Council*, órgão vinculado ao poder legislativo que tem por escopo normatizar princípios gerais para configuração de um direito autônomo à privacidade, estabelecendo uma genérica proibição de divulgação de dados pessoais sem o consentimento de seu titular, exceto em casos que exista um legítimo interesse público[70].

Ainda no contexto da primeira geração de leis de proteção de dados, a primeira lei editada na Europa sobre a tutela da privacidade e regulação de bancos de dados públicos e privados foi a *Datalagen,* proveniente do Parlamento Sueco em maio de 1973 e com modificações realizadas em seu teor legislativo em 1979[71].

A legislação francesa da época tinha um aspecto mais severo quanto a tutela da privacidade individual, normatizando no artigo 9º do Código Civil Francês o direito individual ao respeito à vida privada e trazendo em seu Código Penal a previsão de

---

[68] DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, p. 91-108, 2011. P. 96.
[69] *Idem. Ibdem.*
[70] PAESANI, Liliana Miniardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil.** São Paulo: Atlas, 2000. P. 49.
[71] *Idem Ibdem.*

detenção em até 01 (um) ano e multa no valor de 300 (trezentos) mil francos para aquele que atentasse contra à intimidade da vida privada alheia[72].

Em sentido semelhante a regulamentação sueca, a Constituição Portuguesa de 1977 normatizou em seus dispositivos mandamentais o direito do cidadão português de tomar conhecimento dos próprios dados pessoais utilizados por banco de dados[73].

Observa-se um teor comum encontrado nas legislações enquadradas nesta primeira geração de leis de proteção de dados pessoais, que é o receio estatal ante ao uso indiscriminado das tecnologias informáticas. Isso se dava principalmente porque os efeitos da tecnologia ainda eram desconhecidos, sendo base comum das leis do período a utilização de princípios protetivos amplos e abstratos, focados na atividade de processamento de dados pessoais e dirigidas aos responsáveis por esta. Desta forma, as normas da primeira geração tornaram-se rapidamente ultrapassadas com o crescimento dos centros de processamento de dados, que urgiam por uma sistemática mais ágil para a concessão, regulamentação e acompanhamento da autorização de funcionamento de suas atividades[74].

Neste mister, a partir de 1970 as normas de proteção de dados pessoais passaram a levar em consideração a privacidade do titular, sendo esta garantia jurídica compreendida como uma liberdade negativa a ser exercida pelo cidadão. Esta inovação jurídica é consequência direta da insatisfação popular em face da utilização de seus dados pessoais por terceiros e ante a carência de recursos jurídicos para tutelar os direitos correlatos a esta manipulação, sendo este novo momento jurídico denominado como a segunda geração de leis sobre a proteção de dados pessoais[75].

Este novo momento legislativo, com destaque ao período compreendido entre os anos de 1978 e 1981, foi demarcado pela vasta produção legislativa sobre o tema no âmbito europeu, com a adequação da legislação já existente aos princípios ora

---

[72] *Idem Ibdem.*
[73] *Idem Ibdem.*
[74] DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, p. 91-108, 2011. P. 96.
[75] *Idem Ibdem.*

norteadores da proteção de dados pessoais no âmbito jurídico da Dinamarca, Noruega, Áustria, Ducado de Luxemburgo e Irlanda[76].

Na realidade jurídica alemã à época, ainda que em sua Constituição Federal apenas fizesse previsão de direitos correlatos ao direito à proteção de dados pessoais, como valores da dignidade do homem e pleno desenvolvimento da pessoa humana, a Corte Constitucional Alemã (*Bundesverfassungsgericht*) reconheceu jurisprudencialmente o direito autônomo à privacidade, possibilitando o direito do cidadão em manter secreta a sua sexualidade, seu divórcio e o anonimato das estatísticas. Propiciado por esta criação jurisprudencial, a então Alemanha Federal foi o primeiro país europeu a legislar especificamente sobre a proteção de dados pessoais, por meio da edição do Garante Federal (*Bundesbeaufragter*) em 1977, lei esta que tutelava juridicamente a manipulação dos dados pessoais para uso não consentido[77].

Posteriormente, em 1978, na França foi promulgada a *Informatique et Libertées*, lei francesa que tratava especificamente a questão da proteção de dados pessoais[78].

Advém que, com a consolidação da sociedade da informação profundamente demarcada pela presença mais intensa das tecnologias da comunicação no cotidiano social, assentou-se que o fornecimento de dados pessoais por parte dos cidadãos se tornara requisito imprescindível para a participação social, algo que era previsto como excepcional na segunda geração de leis de proteção de dados pessoais[79].

Tomando esta conjuntura em vista, a partir da década de 80 do século XX, inaugurou-se a terceira geração de leis de proteção de dados pessoais, partindo da necessidade das normas em referência terem um viés mais centrado no indivíduo, não tutelando juridicamente apenas a liberalidade do titular de dados de fornecê-los ou não, mas também visando garantir a efetividade deste direito de escolha. A partir deste momento, a proteção de dados pessoais passou a ser tutelada juridicamente

---

[76] PAESANI, Liliana Miniardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil.** São Paulo: Atlas, 2000. P. 50.
[77] *Idem. Ibdem.*
[78] *Idem. Ibdem.*
[79] DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, p. 91-108, 2011. P. 96.

como um processo mais complexo, envolvendo a participação, ainda que tímida, do cidadão[80].

Conforme elucida Danilo Doneda[81] sobre este momento legislativo:

> O tratamento dos dados pessoais era visto com um processo, que não se encerrava na simples permissão ou não da pessoa à utilização de seus dados pessoais, porém procurava incluí-la em fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros, além de compreender algumas garantias, como o dever de informação.

Esta terceira geração legislativa da proteção de dados pessoais modulou seu aspecto protetivo sob dois eixos, quais sejam o liberal e o social protetivo.

O aspecto liberal da proteção de dados pessoais foi capitaneado pelos Estados Unidos da América (EUA), que basearam a respectiva tutela jurídica na governança de mercado e na perspectiva do titular de dados pessoais como consumidor, sendo a legislação nacional em referência demarcada por um aspecto menos intervencionista e garantista, desenvolvida segundo a concepção de mercado.

A prática adotada no país é de regulamentar a matéria de forma setorial, tal como se observa, a título exemplificativo pelo *Privacy Protection Act*[82]*, Children's Online Privacy Protection Act*[83] e pelo *Gramm–Leach–Bliley Act* (GLBA) [84]*.* Tomando por base este panorama normativo setorial, fundamental salientar a atuação da Comissão Federal de Comércio Norte Americana (*Federal Trade Commission a FTC*), que, ante a ausência de uma normativa uniformizada sobre o tratamento de dados pessoais, exerce competência fiscalizatória e executiva, levando ao Poder Judiciário Norte Americano demandas para determinar o fiel cumprimento dos dispositivos normativos setoriais[85].

Já a perspectiva de proteção de dados pessoais segundo o panorama social protetivo foi liderada pela União Europeia, sendo baseada em direitos e tendo por

---

[80] *Idem. Ibdem.*
[81] *Idem. Ibdem*.
[82] Tradução livre do original: Lei de Proteção à privacidade de 1980. Lei norte americana que protege jornalistas e redações de buscas por parte do governo, protegendo os produtos de trabalho e materiais documentais.
[83] Tradução livre do original: Lei de Proteção à Privacidade Online para Crianças. Lei norte americana que impõe requisitos aos operadores de sites ou serviços online direcionados a crianças menores de 13 (treze) anos.
[84] Tradução livre do original: Lei de Modernização dos Serviços Financeiros.
[85] MASILI, Clarissa Menezes Vaz. **Regulação do uso de dados pessoais no Brasil: papel do usuário na defesa de um direito à tutela de dados pessoais autônomo**. 2018. P. 41.

escopo a consideração de todos os aspectos da individualidade e da cidadania dos titulares.

Esta fase da regulamentação da proteção de dados pessoais teve início com Convenção de Estrasburgo do Conselho Europeu em 1981, que tinha por objetivo fundamental a proteção dos cidadãos europeus em relação à elaboração automática dos dados de caráter pessoal. Em sucedâneo e em decorrência da referida convenção emanada do Conselho Europeu, entre os anos de 1984 e 1991, numerosas leis sobre proteção de dados pessoais foram editadas na conjuntura jurídica do Reino Unido, Finlândia, Irlanda, Holanda e Alemanha.

Diante disto, é fundamental salientar as orientações do Relatório *Bangemann* elaborado em 1994, que já adiantava a necessidade de aprovação de uma normativa comum a todos os países do bloco europeu e também a Diretiva da União Europeia de Proteção de Dados nº 95/76, que tutelava a pessoa física em relação aos seus dados pessoais e sua livre circulação neste bloco econômico. Ocorre que, mesmo com toda a inovação legislativa explanada, a União Europeia lidava com efeitos jurídicos decorrentes do fortalecimento do fenômeno de coleta, armazenamento, processamento e interpretação de dados pessoais dos cidadãos[86].

Este cenário legal corroborou para a quarta e hodierna geração de leis sobre a proteção de dados pessoais, pois no cenário anteriormente delineado a autodeterminação informática do titular de dados era um privilégio exercido por uma minoria social, haja vista que o exercício deste direito era custoso socialmente e economicamente. A nova geração de leis de proteção de dados pessoais se propõe a suprir estas desvantagens existentes no enfoque individual, elevando também o padrão coletivo de proteção, não mais se baseando somente a tutela de dados pessoais na escolha individual.

2.3.2 Aspectos evolutivos da legislação nacional acerca da proteção de dados pessoais

De forma semelhante como ocorreu a evolução da legislação protetiva de dados pessoais sensíveis no panorama internacional, na conjuntura nacional, esta também se deu de forma intrinsecamente correlacionada à proteção do direito à

[86] *Idem. Ibdem*.

privacidade, por força de normas constitucionais, disposições do Código Civil (2002), Marco Civil da Internet (Lei nº 12.965/2014), Código de Defesa do Consumidor (Lei nº 8.078/1990), tratados internacionais, decretos, regulamentos e leis ordinárias espaças para situações específicas em que os dados pessoais são objeto de tratamento por terceiros.

No âmbito da Carta Magna Nacional, o tema da proteção de dados pessoais é tratado em estrita consonância ao direito fundamental de ter a intimidade preservada e demais direito correlatos a este, sendo sistematicamente localizado no Título II Dos Direitos e Garantias Fundamentais, Capítulo I Dos Direitos Individuais e Coletivos, mais especificamente no artigo 5º, incisos, X, XII e XIV[87], dando guarida legal ao direito à intimidade, sigilo de correspondência, comunicações telegráficas, telefônicas e o acesso a dados inseridos em bases governamentais.

O arcabouço jurídico constitucional traçado em referência a proteção garantida aos dados pessoais é decorrência direta do disposto no artigo 1º, inciso III da Constituição Federal de 1998[88], que preceitua que a dignidade da pessoa humana é verdadeiro fundamento do Estado Brasileiro. Cumpre fundamental salientar a existência do remédio constitucional *Habeas Data*, previsto no artigo 5º, inciso LXXII do mesmo diploma jurídico[89], sendo este um instrumento jurídico que visa garantir o acesso à informação individual e retificação desta por parte do cidadão brasileiro em caso de incorreção nos bancos de dados governamentais ou de caráter público.

---

[87] 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; (...)
XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (...)
XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;

[88] Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: (...)
III - a dignidade da pessoa humana

[89] (...) LXXII - conceder-se-á habeas data:
a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

Neste mesmo interim, o Código Civil (2002) regulamenta o tema de proteção de dados pessoais, incluído em seu Capítulo II – Dos Direitos da Personalidade, tal como se observa no artigo 21[90], abaixo colacionado:

> Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma

Da leitura do supra colacionado artigo é possível aduzir que o legislador pátrio instituiu no ordenamento jurídico nacional a privacidade e a proteção de dados como liberdades negativas, sendo a sua potencial violação amparada pela tutela reparatória responsabilidade civil. Desta maneira, caberá ao juízo de adequação do magistrado em cada caso concreto para estabelecer qual o meio de reparação mais adequado para a tutela da privacidade e proteção de dados.

Da mesma forma como ocorreu no panorama internacional, a tutela dispensada pelo Código Civil Nacional não se fez completamente adequada para regular as relações concernentes à proteção de dados pessoais no âmbito da contemporânea sociedade da informação, tal como salienta Eduardo Magrini[91]:

> Consideradas, por exemplo, as particularidades dos bancos de dados informatizados, cuja utilização em larga escala faz com que a temática da privacidade mais e mais nestes esteja concentrada, faltam à responsabilidade civil os instrumentos adequados à realização da função promocional da tutela da privacidade como meio de proteção da pessoa humana e da atuação da cláusula geral da proteção da personalidade. A tutela da privacidade através da responsabilidade civil (...) não é capaz de abranger a complexidade que a proteção de dados agregou ao tema da privacidade. (...) A tutela da privacidade com uma liberdade negativa (...) desconsidera tanto a evolução tecnológica que modificou os termos nos quais a questão da privacidade se expressa, como o alcance normativo da Constituição que, ao considerar a privacidade em seu aspecto positivo, destaca a sua função promocional.

Especializada doutrina nacional defende que a atividade de coleta, tratamento, processamento e transmissão de dados pessoais tem um risco informático intrínseco, devendo esta ser amparada pelo regime da responsabilidade

---

[90] BRASIL. **CÓDIGO CIVIL**. LEI Nº 10.406 DE 10 DE JANEIRO DE 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm> .Acesso em 17 de outubro de 2019.
[91] MAGRANI, Eduardo. **Direito e Tecnologia**. Rio de Janeiro: FGV, 2016. P. 21

civil objetiva[92], conforme disposto no art. 927, parágrafo único do Código Civil Nacional[93]:

A tutela jurídica da proteção de dados pessoais é normatizada quanto ao âmbito específico das relações de consumo nos artigos 43, 72 e 73 do Código de Defesa do Consumidor (Lei nº 8.078/1990)[94], em que dispõe sobre o acesso por parte do consumidor aos seus dados pessoais e de consumo arquivados em bancos de dados.

O Marco Civil da Internet (Lei nº 12.965/2014), ao regulamentar a matéria de proteção de dados pessoais inova, trazendo uma nova gama protetiva as garantias do usuário da internet, tal como se apreende da redação dos artigos 7º, incisos I, II, III, VI, VIII, IX, e X e 8º[95].

---

[92] *Idem. Ibdem*. P. 27.

[93] Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

[94] Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
§ 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
§ 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
§ 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
§ 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
§ 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.
Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros:
Pena Detenção de seis meses a um ano ou multa.
Art. 73. Deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata:
Pena Detenção de um a seis meses ou multa.

[95] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
(...) VI - informações claras e completas constantes dos contratos de prestação de serviços, com

Observa-se que o Marco Civil da Internet é um verdadeiro ponto de mudança no panorama nacional jurídico da proteção de dados pessoais no âmbito online, haja vista que é o primeiro título legislativo brasileiro que prevê direitos e garantias dos usuários, tais como a inviolabilidade de sua intimidade e vida privada e a indenização pelo dano material e moral decorrente da eventual violação, disposições normativas em estrita consonância com o tratamento dispensado pela Constituição Federal e o Código Civil Nacional. A Lei nº 12.965/2014 garante ainda a inviolabilidade e sigilo das comunicações online e armazenadas pelos provedores, assim como a necessidade do consentimento expresso para a coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ser disposto contratualmente de forma destacada[96].

A determinação legal sobre a proteção de dados pessoais é tratada no âmbito jurídico nacional também em leis esparsas, tal como se observa na Lei de Acesso à Informação (Lei nº 12.527/2011) que define em seu artigo 4º, inciso IV a informação pessoal como "aquela relacionada à pessoa natural identificada ou identificável". De forma controversa, este dispositivo normativo autoriza que informações de caráter pessoal relativas à intimidade, vida privada, honra e imagem de pessoas físicas sejam disponibilizadas, independente de prévia autorização de seus titulares, quando existente evidente benefício de utilidade médica, cumprimento de ordem

---

detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade; (...)
VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
a) justifiquem sua coleta;
b) não sejam vedadas pela legislação; e
c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; (...)
Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:
I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou
II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil

[96] MASILI, Clarissa Menezes Vaz. **Regulação do uso de dados pessoais no Brasil: papel do usuário na defesa de um direito à tutela de dados pessoais autônomo**. 2018. P. 45-46.

judicial, defesa de direitos humanos e interesse público nesta disponibilização. O referido diploma jurídico permite ainda que essas informações, desde que garantido o anonimato de seus titulares, possam ser utilizadas para a elaboração de estatísticas e pesquisas científicas de interesse público ou geral. Esses permissivos jurídicos se constituem como de extremo risco, tendo em vista a existência de avançadas técnicas para superar o caráter anônimo de dados[97].

A proteção de dados pessoais na legislação nacional é observada ainda no Decreto nº 8.771/2016, mais especificamente em seu Capítulo III, que regulamenta os procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações na internet, assim como estabelece as medidas de transparência que devem ser adotadas na requisição de dados pela administração pública e os parâmetros para a fiscalização e apuração de infrações.

A Lei do Cadastro Positivo (Lei nº 12.414/2011) ao tratar da questão da proteção de dados pessoais, dispõe em seu artigo 5º, incisos V, VI e VII[98] sobre a possibilidade de informação ao titular de dados pessoais sobre a identidade daquele que está fazendo a gestão de seus dados, qual a finalidade deste tratamento, assim como solicitar a revisão de decisões tomadas de forma automatizada. Esta lei ainda proíbe o registro de informações excessivas e sensíveis.

Cumpre imperioso destacar também o Decreto nº 8.789/2016, que regulamenta o compartilhamento de dados entre órgãos da administração pública federal, excepcionando apenas as informações pessoais fiscais protegidas por sigilo. Esta norma visa apenas e tão somente regulamentar o compartilhamento de informações pessoais entre os órgãos da administração pública federal, haja vista que prescinde da autorização de seu titular[99]. Neste mesmo mister, o Decreto 7.962/2013, que regulamenta o comércio eletrônico, estabelece que o fornecedor

---

[97] *Idem. Ibdem.*

[98] Art. 5º São direitos do cadastrado: (...)
V - ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais;
VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; e
VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados.

[99] *Idem. Ibdem*.

deve garantir mecanismos de segurança para o tratamento de dados pessoais do consumidor[100].

Na esfera regulamentar criminal, evidencia-se a Lei nº 9.296/1996 que normatiza o procedimento de interceptação de sistemas informativos, estabelecendo que quando na instrução ou investigação de procedimentos criminais houver o pedido de interceptação de sistemas informativos, este deve ser fundamentado na razoável suspeita do cometimento de crime por parte do interceptado e sendo este o único meio para obter evidências. Já as leis nº 9.613/1998 e nº 12.850/2013, que dizem respeito respectivamente, aos crimes de lavagem de dinheiro e crime organizado, dão direito as autoridades policiais e Advocacia Geral da União a solicitar diretamente aos provedores de internet acesso aos dados armazenados, não sendo necessário ordem judicia para tal[101].

Já no que diz respeito aos tratados internacionais concernentes à proteção de dados pessoais em que o Brasil é signatário, tem-se a Convenção Internacional sobre Direitos Civis e Políticos, em que se estabeleceu que os países signatários adotariam medidas para garantir a proibição de interferências e ataques da privacidade individual e o Pacto de San Jose da Costa Rica, em que se determinou a obrigação por parte dos países signatários em impedir a ingerência arbitrária e abusiva na vida e privacidade das pessoas, muito embora o Brasil não tenha aceitado a jurisdição compulsória da Corte Interamericana de Direitos Humanos[102].

Mesmo diante do vasto panorama traçado acerca da legislação nacional que se propõe a regular a privacidade de dados pessoais, em relatório divulgado em 2016 pela *Privacy International* destacou -se que, apesar da forte militância nacional pela proteção de dados pessoais, esta preocupação não se concretiza nas medidas adotadas pelo governo brasileiro, que implementou medidas de retenção obrigatória de dados e expandiu sua capacidade institucional de vigilância.

---

[100] PRIVACY INTERNACIONAL apud MASILI, Clarissa Menezes Vaz. **Regulação do uso de dados pessoais no Brasil: papel do usuário na defesa de um direito à tutela de dados pessoais autônomo**. 2018. P. 43.
[101] *Idem. Ibdem.*
[102] *Idem. Ibdem.*

2.4 O incidente de vazamento de dados pessoais sensíveis e suas principais consequências

Ainda que o meio online conte com diversos mecanismos de proteção da integridade e privacidade dos usuários, tais como senhas e criptografia, este igualmente se encontra sujeito a variadas formas de ataque e invasões, como atividades de *hackers* e *crackers* e exposição a toda sorte de *malwares*. Neste interim, a invasão, acesso indevido, utilização ilegal e roubo de dados pessoais consolidaram-se como uma preocupação mundial no contexto da economia digital.

A coleta online de dados pessoais sensíveis de usuários da rede mundial de computadores é propiciada pelo teor abstrato e predominantemente técnico dos termos de uso, com verdadeira natureza de contratos de adesão, havendo o constante incentivo para o envio de informações pessoais, sendo esta uma verdadeira moeda de troca para o usufruto de produtos e serviços. Esta configuração prejudica o direito à autotutela de dados por parte dos usuários, haja vista que estes não conhecem os termos e condições que se submetem, legitimando a coleta, armazenamento e manipulação de dados pessoais pelas plataformas digitais[103].

Esta importância dada aos dados na contemporaneidade caracterizou o atual cenário de risco intangível e iminente do descontrole de suas próprias informações por parte dos internautas. Este quadro, associado com as crescentes falhas de segurança das plataformas online, propiciam a ocorrência dos incidentes globais de vazamento de dados (*data breach*), que são consequência da consolidação da sociedade da informação, haja vista que na atual conjuntura econômica[104] “o acesso a perfis e informações pessoais dos usuários torna-se o maior capital existente e desejável pelos Estados e empresas mundiais”[105].

A definição jurídica do incidente de vazamento de dados é:

---

[103] MARTINS, Ana Paula Pereira. **Vazamento e Mercantilização de Dados Pessoais e a Fragilidade da Segurança Digital do Consumidor: um estudo dos casos Netshoes e Uber.** Disponível em: < https://www.researchgate.net/profile/Ana_Martins195/publication/327416131_VAZAMENTO_E_MERCANTILIZACAO_DE_DADOS_PESSOAIS_E_A_FRAGILIDADE_DA_SEGURANCA_DIGITAL_DO_CONSUMIDOR_um_estudo_dos_casos_Netshoes_e_Uber/links/5b8e042e299bf114b7f05bbb/VAZAMENTO-E-MERCANTILIZACAO-DE-DADOS-PESSOAIS-E-A-FRAGILIDADE-DA-SEGURANCA-DIGITAL-DO-CONSUMIDOR-um-estudo-dos-casos-Netshoes-e-Uber.pdf> Acesso em: 19 de outubro de 2019.

[104] *Idem .Ibdem.*

[105] *Idem. Ibdem.*

> O *data breach* pode ser traduzido juridicamente como alegado fato de terceiro, em que um cracker, almejando proveito econômico criminoso, coleta dados ilegalmente em troca de pagamento em dinheiro real ou criptomoedas, ou quando um hacker "ético", com o propósito de detectar vulnerabilidades em sistemas de empresas e instituições, descobre uma falha de segurança no sistema da loja virtual que deixou exposto à ação de agentes mal-intencionados os dados de seus usuários[106].

A mineração de dados (*data mining*) é uma técnica decorrente do aprimoramento tecnológico do tratamento de informações existentes nos bancos de dados online, haja vista que estes possuem um volume cada vez maior de informações dos usuários a serem tratadas, provenientes estas das plataformas online, aplicando-se sob estes dados técnicas de *profiling*, qual seja, a organização em tendência e correlações dos dados, gerando um perfil completo do seu titular[107].

Desta maneira, quando na ocorrência do incidente de vazamento de dados, destaca Patrícia Peck Pinheiro[108]:

> A maioria das empresas virtuais que sofrem invasões não denuncia a ocorrência, haja vista que os dados furtados são de seus 'clientes' e muitas vezes serão utilizados por terceiros sem que estes percebam, pelo menos até que algo pior ocorra (...). Alguns têm medo de tornar a ocorrência pública por temerem que haja dano à marca, que passaria a imagem de ser insegura perante o universo dos consumidores.

Neste interim, é inconteste que na contemporaneidade a tecnologia tem demarcado impacto social, principalmente considerando que a captação, guarda e análise de dados é feita nos dispositivos, sistemas, aplicações e redes sociais utilizadas rotineiramente pelos indivíduos sociais. Neste contexto, quando na configuração dos incidentes de vazamento de dados, não só a privacidade é colocada em voga, mas também o bem-estar dos cidadãos, haja vista a existência de coleta de dados pessoais sensíveis, que em seu conhecimento público e processamento podem ter destinação discriminatória e lesiva aos seus titulares.

---

[106] *Idem. Ibdem.*
[107] *Idem. Ibdem.*
[108] *Idem. Ibdem.*

3. O NOVO PANORAMA NORMATIVO TRAZIDO PELA *GENERAL DATA PROTECTION REGULATION* (GDPR) E LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) PARA A PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS E SUAS PRINCIPAIS REPERCUSSÕES ECONÔMICAS

3.1 A insuficiência da prévia legislação para garantir a proteção de dados pessoais e a necessidade de um novo diploma específico sobre a matéria

Diante do panorama traçado acerca das medidas protetivas que eram adotadas pelo ordenamento jurídico brasileiro e internacional para a proteção de dados pessoais e sua indiscutível ineficácia perante o quadro regulatório fático, tendo em vista a notícia de recorrentes episódios de vazamento de dados pessoais, resta claro que as instituições governamentais não foram capazes de normatizar concretamente o fenômeno jurídico decorrente do impacto da evolução tecnológica no que tange aos dados pessoais.

A atividade de manipulação de dados é intrínseca da própria natureza estrutural e operacional da internet, em que a coleta e tratamento destes se deu por longos períodos sem esbarrar em qualquer norma jurídica efetiva para seu controle e regulamentação, dando azo ao desenvolvimento de um ramo econômico com base no processamento de dados. Tal ramo econômico tem alicerce no exercício de agregação de dados isolados sobre o usuário, neste momento chamado de dados, que, passado por tratamento, se constituem como informação, formando um perfil completo a respeito do indivíduo, com os inúmeros aspectos de sua personalidade e com inequívoco valor econômico agregado.

Desta maneira, a proteção de dados pessoais na oportunidade da sociedade da informação não se dá meramente pela proteção à exposição de detalhes íntimos da vida do indivíduo, conceito correlato ao direito de privacidade, mas também para evitar a manipulação de toda e qualquer informação a este usuário concernente sem o seu consentimento ou controle de qualidade e quantidade de dados sobre si captados[109], tendo em conta que este indivíduo tem o direito também a autotutela de seus dados.

---

[109] MARTINS, Ana Paula Pereira. **Vazamento e Mercantilização de Dados Pessoais e a Fragilidade da Segurança Digital do Consumidor: um estudo dos casos Netshoes e Uber.**

Corrobora ainda para este prévio cenário de precária assistência aos direitos individuais na sociedade da informação, a consolidação do conceito de auto-regulamentação no âmbito online, em que a normatização e resolução de eventuais conflitos nesta seara se daria diretamente entre seus participantes, sem a intervenção estatal.

O conceito de auto-regulamentação no âmbito online se deu sob o pretenso fundamento de que desta maneira haveria a flexibilização adequada para a velocidade das mudanças na sociedade digital e acontecimentos no âmbito da internet, mas que na verdade endossou a ideia de que a internet seria a chamada terra de ninguém, já que não levou em consideração a ausência de possibilidade negocial dos termos de uso por parte dos usuários junto aos provedores de serviços.

Neste interim, a novel legislação no panorama nacional e internacional visa garantir a partir de suas disposições normativas a tutela dos direitos do usuário contra os riscos que ameaçam sua personalidade em face da coleta, processamento, utilização e circulação de seus dados pessoais e também a garantia de controle do fluxo desses dados na sociedade, principalmente no que tange aos dados pessoais sensíveis, haja vista o seu demarcado poder de utilização para finalidades discriminatórias ou lesivas[110].

3.2 A solução normativa trazida pela General Data Protection Regulation (GDPR) para a proteção de dados pessoais sensíveis

A *General Data Protection Regulation* foi promulgada na União Europeia em abril de 2016, entrando em vigor em maio de 2018, em substituição a 95/46/EC (Diretiva Europeia de Proteção de Dados Pessoais), sendo aplicável a todos os 28 países integrantes do bloco econômico europeu.

Este novo regulamento europeu vinculando às suas disposições toda e qualquer organização que ofereça bens ou serviços que coletem dados pessoais

---

Disponível em: < https://www.researchgate.net/profile/Ana_Martins195/publication/327416131_VAZAMENTO_E_MERCANTILIZACAO_DE_DADOS_PESSOAIS_E_A_FRAGILIDADE_DA_SEGURANCA_DIGITAL_DO_CONSUMIDOR_um_estudo_dos_casos_Netshoes_e_Uber/links/5b8e042e299bf114b7f05bbb/VAZAMENTO-E-MERCANTILIZACAO-DE-DADOS-PESSOAIS-E-A-FRAGILIDADE-DA-SEGURANCA-DIGITAL-DO-CONSUMIDOR-um-estudo-dos-casos-Netshoes-e-Uber.pdf> Acesso em: 19 de outubro de 2019.

[110] *Idem. Ibdem.*

concernentes ao bloco econômico europeu[111], consistindo o seu escopo fundamental exercer de forma mais efetiva a proteção individual, no que diz respeito ao tratamento de dados pessoais e a livre circulação destes no bloco econômico[112], tanto no âmbito online como fora deste.

O novel diploma se baseia nos princípios da licitude, lealdade, transparência, limitação das finalidades, minimização, exatidão, limitação do prazo de conservação, integridade, confidencialidade e responsabilidade quando no tratamento de dados pessoais[113].

Desta maneira, este novo marco legislativo se constitui como uma verdadeira mudança de paradigma na regulamentação da matéria em referência, tendo o escopo de modernizar e uniformizar o sistema jurídico de manipulação de dados na União Europeia, fortalecendo os direitos individuais e tratando de forma coerente e clara a regulamentação da matéria no bloco europeu.

Este diploma, embora editado na conjuntura da União Europeia, tem uma amplitude global, sendo aplicável a empresas que ofereçam bens ou serviços a titulares de dados que se encontram em quaisquer dos países da União Europeia, ainda que o tratamento se dê fora de seus limites geográficos[114], ou que de qualquer outro modo controle o comportamento de cidadãos do bloco. Há uma verdadeira extensão da jurisdição com esta regulamentação, haja vista o permissivo legal para a transferência de dados para países fora da União Europeia, desde que o país destinatário tenha similar nível de proteção aos dados pessoais[115], disposição esta que deu azo a uma onda mundial de regulamentação sobre dados pessoais.

Este novo marco regulamentar para a proteção de dados pessoais na conjuntura europeia prevê obrigações aos controladores e operadores e direitos aos

---

[111] MANGETH, Ana Lara; NUNES, Beatriz; MAGRANI, Eduardo. **Seis pontos para entender o Regulamento Geral de Proteção de Dados da EU**. ITS Rio, 2018. Disponível em: <https://feed.itsrio.org/seis-pontos-para-entender-a-lei-europeia-de-prote%C3%A7%C3%A3o-de-dados-pessoais-gdpr-d377f6b691dc>. Acesso em 26 de outubro de 2019.

[112] MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. 2ª Edição. Porto Alegre: Arquipélago Editorial, 2019. P. 119.

[113] NETO, Eugênio Facchini; DEMOLINER, Karine Silva. **Direito à Privacidade e Novas Tecnologias: Breves Considerações Acerca da Proteção de Dados Pessoais no Brasil e na Europa**. REVISTA INTERNACIONAL CONSINTER DE DIREITO Ano IV–Número VII, v. 7, 2019.

[114] NETO, Pery Saraiva; FENILI, Maiara Bonetti**. NOVOS MARCOS LEGAIS SOBRE PROTEÇÃO DE DADOS PESSOAIS E SEUS IMPACTOS NA UTILIZAÇÃO E TRATAMENTO DE DADOS PARA FINS COMERCIAIS.** Revista de Estudos Jurídicos e Sociais-REJUS ON LINE-ISSN 2594-7702, v. 1, n. 1, 2018.

[115] *Idem. Idbem.*

usuários, sendo elemento norteador da relação jurídica tutelada a função do consentimento do titular de dados para a autorização da coleta e tratamento de dados, devendo esta concordância ser expressa e inequívoca.

As regras contidas na GDPR atribuem às autoridades fiscalizatórias amplo poder para o exercício de vigilância e responsabilização daqueles que realizem a coleta e manipulação de dados pessoais em manifesto contrassenso com as disposições normativas do regulamento, podendo as sanções mais graves incorrerem em multas de até € 20 milhões ou 4% do faturamento anual da empresa transgressora.

Esta fiscalização é realizada pelas autoridades públicas já estabelecidas quando na vigência da Diretiva nº 95/46/EC, quais sejam as Autoridades de Proteção de Dados, existindo uma para cada estado membro da União Europeia. Complementa ainda este quadro fiscalizatório a figura do Encarregado de Proteção de Dados, que é o profissional responsável a prestar contas da atividade exercida pela entidade que armazena ou manipula dados pessoais, avaliando os possíveis impactos e riscos aos titulares destes, reduzindo as ameaças de abuso na coleta, tratamento, uso e transferência de dados[116].

Assim, qualquer operação realizada com dados pessoais, por meios automatizados ou não, quais sejam: a coleta, registro, organização, estruturação, armazenamento, alteração, recuperação, consulta, utilização, combinação, restrição ou destruição de dados tem o eixo de responsabilidade sob estes impostos as empresas que deles utilizam como insumo, devendo estas colocarem em prática as medidas de segurança impostas pela GDPR como forma de coibir possíveis incidentes de violação de dados, além de obrigar a adoção de práticas empresariais para notificação dos titulares e autoridades no caso de configuração do incidente[117].

Os direitos dos titulares de dados são elencados no Capítulo III da *General Data Protection Regulation*, dentre estes o direito a obter informações com transparência, possibilitando a retificação dos seus dados em caso de incorreções, o direito ao esquecimento, com a retirada de informações sobre o titular de uma

---

[116] MANGETH, Ana Lara; NUNES, Beatriz; MAGRANI, Eduardo. **Seis pontos para entender o Regulamento Geral de Proteção de Dados da EU**. ITS Rio, 2018. Disponível em: <https://feed.itsrio.org/seis-pontos-para-entender-a-lei-europeia-de-prote%C3%A7%C3%A3o-de-dados-pessoais-gdpr-d377f6b691dc>. Acesso em 26 de outubro de 2019.

[117] *Idem. Ibdem.*

plataforma, desde que esta informação não seja de interesse público, a portabilidade de dados, o direito a revisão e explicação de decisões realizadas de forma automatizada[118].

É neste contexto que o conceito de dados sensíveis encontrado no artigo 9º, (1) e (2) da GDPR[119], quais sejam as informações de cunho pessoal que revelam

---

[118] *Idem. Ibdem.*

[119] UNIÃO EUROPÉIA. Regulation 2016/679 of The European Parliament and of The Council of 27 april 2016. **General Data Protection Regulation**. Disponível em: < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 26 de outubro de 2019. Tradução livre da autora: Artigo 9. O Tratamento de categorias especiais de dados pessoais 1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. 2. O disposto no nº 1 não se aplica se se verificar um dos seguintes casos: a) Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado-Membro previr que a proibição a que se refere o nº 1 não pode ser anulada pelo titular dos dados; b) Se o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados; c) Se o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento; d) Se o tratamento for efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contatos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares; e) Se o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular; f) Se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da sua função jurisdicional; g) Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados; h) Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no nº 3; i) Se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados- -Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional; L 119/38 PT Jornal Oficial da União Europeia 4.5.2016 j) Se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n.o 1, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados. 3. Os

origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, a filiação sindical, bem como dados genéticos, biométricos e dados relativos à saúde, vida sexual e orientação sexual de uma pessoa, tem seu tratamento expressamente proibidos pela RGPD. Tal proibição é incisiva e objetiva não só assegurar o direito à privacidade de seus titulares, mas também evitar o seu potencial uso destas informações de forma a prejudicar os usuários, seja para trazer restrições de acesso a bens, serviços ou ao exercício de direitos[120].

Dada estas características dos dados pessoais sensíveis, a GDPR garante a estes uma proteção especial, haja vista sua intrínseca correlação com direitos e liberdade individuais dos cidadãos. Desta maneira, o regulamento permite excepcionalmente o tratamento de dados pessoais sensíveis na hipótese de estes terem sido coletados mediante o consentimento livre, dado sem qualquer tipo de pressão ou coação e de forma inequívoca, não pairando dúvidas quanto ao consentimento para o tratamento. Deve ainda ser informando ao titular as implicações do tratamento de seus dados, de maneira expressa, e sendo apresentada de forma clara e objetiva a concordância com o tratamento de dados pessoais sensíveis, com a necessária explicação das implicações desta coleta de dados, sendo especificado ao titular qual o propósito do tratamento[121].

O Regulamento Geral de Proteção de Dados Europeu permite ainda de forma excepcional o tratamento de dados pessoais sensíveis nas hipóteses de: cumprimento de obrigação ou exercício de direitos específicos pelo responsável pelo tratamento ou titular de dados em matéria de legislação laboral, segurança ou proteção social, para resguardar interesses vitais do titular de dados na hipótese deste estar fisicamente ou legalmente incapacitado de dar o seu consentimento,

---

dados pessoais referidos no nº 1 podem ser tratados para os fins referidos no nº 2, alínea h), se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes. 4. Os Estados-Membros podem manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde.

120 FRAZÃO, Ana. **Nova LGPD: o tratamento dos dados pessoais sensíveis**. Disponível em: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018>. Acesso em: 11 de outubro de 2019.

121 DE ANDRADE, Gustavo Piva. **O GDPR e a proteção dos dados sensíveis.** Disponível em: <https://www.migalhas.com.br/dePeso/16,MI280651,71043-O+GDPR+e+a+protecao+dos+dados+sensiveis>. Acesso em 20 de outubro de 2019.

quando na atividade de fundações, associações ou qualquer outro organismo sem fins lucrativos de finalidade política, filosófica, religiosa ou sindical apenas no que tange aos seus membros e limitado aos objetivos institucionais e quando os dados pessoais se tornam manifestamente públicos pelo seu titular.

A lei excepciona o tratamento de dados pessoais sensíveis nas hipóteses também de quando este serve como prova em procedimento judicial, por motivo de interesse público devidamente fundamentado, para efeitos de medicina preventiva ou do trabalho, avaliação da capacidade laboral do empregado, diagnóstico médico, prestação de cuidados ou tratamentos de saúde, por interesse público relativo à saúde, como a proteção contra ameaças transfronteiriças graves ou assegurar um elevado nível de qualidade e de segurança aos cuidados com a saúde, medicamentos e dispositivos médicos e para fins de investigação científica, histórica ou estatístico.

Desta maneira, estabelecem o Considerando número 51 e 52 do *General Data Protection Regulation*, em tradução literal[122]:

> (51) Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas. O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular. Tais dados pessoais não deverão ser objeto de tratamento, salvo se essa operação for autorizada em casos específicos definidos no presente regulamento, tendo em conta que o direito dos Estados-Membros pode estabelecer disposições de proteção de dados específicas, a fim de adaptar a aplicação das regras do presente regulamento para dar cumprimento a uma obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento. Para além dos requisitos específicos para este tipo de tratamento, os princípios gerais e outras disposições do presente regulamento deverão ser aplicáveis, em especial no que se refere às condições para o tratamento lícito. Deverão ser previstas de forma explícita derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por exemplo, se o titular dos dados der o seu consentimento expresso ou para ter em conta necessidades específicas, designadamente quando o tratamento for efetuado no exercício

[122] UNIÃO EUROPÉIA. Regulation 2016/679 of The European Parliament and of The Council of 27 april 2016. **General Data Protection Regulation**. Disponível em: < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 26 de outubro de 2019

> de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais. (52) As derrogações à proibição de tratamento de categorias especiais de dados pessoais deverão ser igualmente permitidas quando estiverem previstas no direito da União ou dos Estados-Membros e sujeitas a salvaguardas adequadas, de forma a proteger os dados pessoais e outros direitos fundamentais, caso tal seja do interesse público, nomeadamente o tratamento de dados pessoais em matéria de direito laboral, de direito de proteção social, incluindo as pensões, e para fins de segurança, monitorização e alerta em matéria de saúde, prevenção ou controlo de doenças transmissíveis e outras ameaças graves para a saúde. Essas derrogações poderão ser previstas por motivos sanitários, incluindo de saúde pública e de gestão de serviços de saúde, designadamente para assegurar a qualidade e a eficiência em termos de custos dos procedimentos utilizados para regularizar os pedidos de prestações sociais e de serviços no quadro do regime de seguro de saúde, ou para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos. Uma derrogação deverá também permitir o tratamento desses dados pessoais quando tal for necessário à declaração, ao exercício ou à defesa de um direito, independentemente de se tratar de um processo judicial ou de um processo administrativo ou extrajudicial.

O regulamento estabelece ainda considerações específicas quando nas exceções que permitem o tratamento de dados sensíveis no contexto do setor de saúde e social, tanto privado quanto público, no processamento por autoridades oficiais para objetivos de reconhecimento de comunidades religiosas e no processamento de opiniões políticas por partidos políticos.

Neste interim, como forma de garantir efetividade a este quadro regulamentar europeu, principalmente no que tange aos dados pessoais sensíveis, o próprio Órgão Europeu Supervisor de Proteção de Dados recomenda: a imposição das normas de proteção de dados pessoais, a priorização por parte dos reguladores de um diagnóstico coletivo sobre o incidente de vazamento de dados pessoais ou outra contende jurídica correlata, a cooperação dos diversos setores sociais, tanto público como privado, o desenvolvimento de códigos próprios para específicos quadros de regulamentação, desde que tomando por base os princípios mínimos estabelecidos na GDPR e o estímulo aos cidadãos para exercer suas prerrogativas concernentes à proteção de dados pessoais, inclusive as ações coletivas[123].

[123] EUROPEAN DATA PROTECTION SUPERVISOR, **Opinion 3/2018. EDPS Opinion on online manipulation and personal data**. Março de 2018. Disponível em: <https://edps.europa.eu/shttps://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdfites/edp/files/publication/18-03-19_online_manipulation_en.pdf>. Acesso em 20 de outubro de 2019.

3.2 A solução normativa trazida pela Lei Geral de Proteção de Dados (LGPD) para a proteção de dados pessoais sensíveis

Em manifesta inspiração no promulgado Regulamento Geral de Proteção de Dados da União Europeia, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) foi editada no contexto brasileiro em 14 de agosto de 2018, passando os seus 65 artigos a ter força normativa apenas em agosto de 2020, haja vista o seu período de *vacatio legis*.

A nova legislação estabelece um regime geral de proteção de dados pessoais, consolidando-se como um marco normativo da sociedade da informação, em complementação a prévia legislação que exercia uma regulação da matéria de forma setorial, sendo aplicável de maneira horizontal ao setor público e as empresas nacionais ou estrangeiras que ofertam produtos ou serviços no mercado brasileiro ou que monitorem o comportamento de titulares de dados localizados em solo nacional, independentemente da nacionalidade ou local de residência destes[124].

Tomando por base que os dados pessoais são meio de representação da pessoa na sociedade e estão em intrínseca correlação com a personalidade de seus titulares, a nova legislação reconhece a possibilidade de violação de direitos fundamentais caso estes sejam manipulados para fins transversos, tais como a violação à liberdade de expressão e comunicação, privacidade, honra, imagem, autodeterminação informativa e livre desenvolvimento da personalidade[125]. Isto significa dizer que o referido diploma normativo nacional prevê em seu artigo 2º, inciso VII[126] a efetivação e promoção de direitos humanos fundamentais como justificativa para a tutela de dados pessoais[127].

Neste interim, a promulgação da Lei Geral de Proteção de Dados Pessoais brasileira visa harmonizar os interesses legítimos de titulares de dados em face das empresas que os utilizam como insumo para a sua atividade, tendo por escopo

---

[124] MENDES, Laura Schertel. **Privacidade e dados pessoais. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação**. Panorama Setorial da Internet. Número 2. Junho, 2019. Ano 11. P. 02.

[125] *Idem. Ibdem.*

[126] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: (...) VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

[127] MULHOLLAND, Caitlin Sampaio. **Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18).** *Revista de Direitos e Garantias Fundamentais*, 2018, 19.3: 159-180.

fundamental não frear o desenvolvimento tecnológico, mas sim compatibilizar este com os direitos e expectativas dos titulares de dados pessoais, viabilizando o tratamento legítimo destes. Este diploma visa ainda colocar o Brasil no parâmetro internacional dos países que conferem segurança jurídica aos dados pessoais, haja vista a crescente exigência internacional deste status para a realização da transferência internacional de dados.

Orientam a lei em comento os princípios da finalidade, adequação, necessidade livre acesso, qualidade dos dados, transparência, segurança, prevenção não discriminação, responsabilização e prestação de contas nas atividades que tenham acesso a dados pessoais, consolidando que o tratamento destes só poderá se dar na conjuntura nacional caso enquadrado em uma das hipóteses autorizativas da Lei Geral de Proteção de Dados nacional.

A LGPD estabelece uma nova gama de direitos conferidos aos titulares de dados pessoais para exercerem o controle do fluxo de seus dados, que são taxados na lei em comento como: o direito ao acesso e confirmação de tratamento de seus dados, o direito à retificação de dados incompletos, inexatos ou desatualizados, a restrição de uso de suas informações pessoais, a possibilidade de recusa em fornecer o consentimento, o cancelamento ou exclusão de dados em tratamento, o direito a portabilidade de seus dados, a informação de quais informações estão sendo tratadas, revogação do consentimento, a oposição e a explicação[128].

A Lei nº 13.709/2018 estabelece ainda um quadro de responsabilização dos agentes coletores de dados pessoais na hipótese de configuração de incidentes de vazamento, cuja responsabilidade poderá ser apurada tanto no âmbito cível como administrativo. De forma análoga como estabelecido na legislação europeia, na conjuntura nacional cria-se também a figura da Autoridade Nacional de Proteção de Dados (ANPD) e do Encarregado de Tratamento de Dados Pessoais.

Desta forma, a normativa de proteção de dados nacional estabelece que, na configuração do incidente de segurança, o encarregado é obrigado a comunicar a ANPD, podendo esta determinar a adoção de medidas de mitigação ou a ampla divulgação para a sociedade. Desta forma, a ANPD pode dar uma advertência,

---

[128] MENDES, Laura Schertel. **Privacidade e dados pessoais. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação**. Panorama Setorial da Internet. Número 2. Junho, 2019. Ano 11. P. 02

determinando a adoção de medidas corretivas ou arbitrar multas no valor de até 2% do valor de faturamento da empresa (limitado ao valor de R$ 50.000.000,00 por infração), podendo também sancionar pelo arbitramento de multas diárias, determinando a publicidade da infração e o bloqueio ou eliminação de dados pessoais a que se referem a informação. Assim a infração será sancionada tomando-se em consideração a gravidade e a natureza desta, os direitos pessoais infringidos, a boa-fé do infrator, a vantagem econômica auferida e a condição econômica deste, a reincidência e cooperação do infrator, a adoção de mecanismos e procedimentos para minimizar os danos e de políticas de boas práticas e de governança adotadas pela empresa que incorreu em infração.

O art. 5º, inciso II da Lei nº 13.709/2018 define como dado pessoal sensível como o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou 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.

Estão intrinsecamente correlacionados à proteção de dados pessoais sensíveis os princípios da finalidade e o da não discriminação. O princípio da finalidade determina que os dados devem ser tratados apenas para o propósito que foram concedidos, devendo as razões da coleta de dados pessoais sensíveis serem objetivas e limitadas, sendo imprescindível existir uma "comunicação preventiva ao interessado sobre como serão usadas as informações coletadas; e para algumas categorias de dados especialmente sensíveis estabelece que a única finalidade admissível é o interesse da pessoa considerada"[129]. Já o princípio da não discriminação, veda a utilização dos dados pessoais para fins discriminatórios ilícitos ou abusivos[130].

Dada as características destes dados, é possível ao seu detentor ao tratá-los traçar um perfil fidedigno da pessoa que o detém, possibilitando um uso potencialmente lesivo, em decorrência da capacidade discriminatória que tais informações podem vir a gerar.

---

[129] RODOTÁ, Estefan *apud* MULHOLLAND, Caitlin Sampaio**. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18).** *Revista de Direitos e Garantias Fundamentais*, 2018, 19.3: 159-180.

[130] *Idem. Ibdem.*

Assim sendo, de maneira semelhante como normatizado o tema na *General Data Protection Regularment*, a Lei Geral de Proteção de Dados Brasileira permite o tratamento de dados pessoais sensíveis de forma excepcional, sendo imprescindível a manifestação livre, informada, inequívoca por parte de seu titular e ainda de forma específica e destacada. “Reconhece-se que o consentimento do titular de dados sensíveis deve ser qualificado, na medida em que estamos diante de uma ‘contratante vulnerável’, caracterizado justamente pela ausência de liberdade substancial no momento da determinação da vontade”[131].

Por conseguinte, na conjuntura jurídica do ordenamento pátrio, podem ser tratados dados pessoais sensíveis nas hipóteses de este ser prescindido pelo consentimento do titular, de formar específica e destacada, para finalidades específicas. Quando no cumprimento de obrigação legal ou regulatória de seu *controller.* Para a execução de políticas públicas pela Administração Pública. Quando no exercício regular de direito, inclusive em contratos e processo judicial, administrativo e arbitral. Na proteção da vida ou da incolumidade física do titular ou de terceiros. Na tutela da saúde, em procedimento realizado por profissionais da área. E na prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

Neste interim, é possível aduzir que o tratamento de dados pessoais sensíveis se faz indispensável em algumas situações concretas específicas, mas que esta deve ser realizada com cautela, respeito e segurança, haja vista tais informações, seja por sua natureza ou por suas características, quando violadas podem incorrer em riscos significativos em relação aos direitos e às liberdades fundamentais da pessoa[132].

3.3 O desenvolvimento da atividade econômica com base em dados pessoais sensíveis diante da atual regulamentação

É fundamental salientar que, muito embora a *General Data Protection Regularment* e a Lei Geral de Proteção de Dados Brasileira tenham por escopo fundamental salvaguardar os direitos dos sujeitos informacionais, estes dispositivos

---

[131] *Idem. Ibdem.*

[132] PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. Saraiva Educação SA, 2018.

normativos precisam equalizar suas disposições com os interesses econômicos e comerciais correlatos à economia baseada em dados.

Esta ponderação de direitos é imprescindível, haja vista que estes se encontram em mesmo nível hierárquico constitucional, quais sejam o direito fundamental a dignidade humana e da livre iniciativa econômica. Desta forma, ainda que o mercado de dados seja uma das principais fontes de receita para algumas das grandes corporações da economia informacional[133], é necessária cautela na utilização destes dados que dinamizam e tornam a gestão econômica mais eficiente no bojo da economia digital.

Previamente a promulgação dos marcos normativos de proteção de dados no contexto europeu e brasileiro, os dados pessoais eram coletados e manipulados muitas vezes de forma ilícita, sem a ciência e a autorização de seus titulares. Desta forma, diante da flagrante ilegalidade em que o cenário econômico com base em dados se consolidava, assentou-se que, ainda que os dados pessoais sejam novos insumos da economia digital, o tratamento e manipulação destes precisam se equalizar com a proteção da privacidade e identidade pessoal dos usuários, sendo imprescindível na consolidação da sociedade informacional que este titular possa também exercer sua autodeterminação informativa.

Neste bojo, dá-se azo a consolidação do conceito de *privacy by design,* que determina que os princípios fundamentais da privacidade devem ser aplicados em todo o processo de desenvolvimento de um sistema ou atividade econômica, assim como o conceito de *privacy by default,* que determina que os produtos e serviços oferecidos no âmbito da sociedade informacional sejam ofertados com as configurações mais avançadas de privacidade como padrão[134].

Cumpre salientar que os novos diplomas normativos protetivos de dados pessoais não tem o objetivo de inviabilizar o exercício de atividades econômicas que tenham por base a captura, processamento e análise de dados, mas sim que esta atividade econômica seja exercida tomando por base os novos padrões protetivos de direitos individuais estabelecidos pela GDPR e LGPD, devendo estas serem

---

[133] FRAZÃO, Ana. **Nova LGPD: principais repercussões para a atividade empresarial.** Disponível em: <https://www.ab2l.org.br/nova-lgpd-principais-repercussoes-para-a-atividade-empresarial/>. Acesso em: 26 de outubro de 2019.

[134] MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. 2ª Edição. Porto Alegre: Arquipélago Editorial, 2019. P. 128.

levadas em consideração quando em decisões negociais e parcerias comerciais, motivem a revisão e adequação de processos internos de empresas que tratem dados pessoais e desenvolvimento de novos produtos e serviços em adequação aos referidos diplomas normativos. Por conseguinte, é possível equalizar direitos individuais com o fomento à inovação, segundo tratamento legítimo de dados pessoais pautado em boas práticas de governança.

CONSIDERAÇÕES FINAIS

O contexto socioeconômico de circulação de dados informáticos em grandes volumes esvaziou o conteúdo de inúmeras e generosas leis que se propunham a tutelar a privacidade, se fazendo necessário uma proteção legislativa especifica ao direito de controle sobre as próprias informações, levando-se em conta que a atividade de tratamento de dados pessoais é de alto risco aos direitos fundamentais, pois estes são expressão direta da personalidade do usuário.

Na conjuntura da economia digital com base em tratamento de dados, faz-se mister proteger não só a privacidade dos titulares de dados pessoais sensíveis coletados, preservando sua autonomia, mas também garantir um equilíbrio na relação que se formou em torno da crescente importância financeira dada ao dado pessoal.

Consolida-se então um direito à autotutela dos dados pessoais, correlato aos direitos da personalidade, haja vista que do dado pessoal é uma verdadeira extensão de seu titular, devendo sua identidade digital externar fidedignamente a singularidade de seu detentor, tendo este o direito de controlá-lo e retificá-lo em hipótese de erro. O indivíduo titular de dados pessoais não se porta mais como mero fornecedor destes, mas tem também atuação ativa no controle de seus dados

É incontroversa a necessidade de proteção de dados pessoais sensíveis no bojo da sociedade da informação, levando-se em consideração que a coleta destes mediante o aceite de termos de uso mitigaram de forma latente o poder de autodeterminação por parte de seus titulares, incorrendo em diversas situações em prejuízos sociais e econômicos para estes, haja vista a manifesta possibilidade de utilização destes dados pessoais sensíveis para fins discriminatórios, situação esta que os novos diplomas específicos sobre o tema se propõem a evitar.

Neste contexto, quando na configuração dos incidentes de vazamento de dados, não só a privacidade é colocada em voga, mas também o bem-estar dos cidadãos, haja vista a existência de coleta de dados pessoais sensíveis, que em seu conhecimento público e processamento podem ter destinação discriminatória e lesiva aos seus titulares.

É necessário prevenir que estas informações sejam utilizadas e manipuladas contra seus donos, incorrendo na restrição de acesso a serviços públicos e privados

e até mesmo o exercício de direitos por parte destes, haja vista que garantir a proteção a estes dados é proteger os fundamentos do Estado Democrático de Direito, tendo em conta que a discriminação enseja a violação de direitos humanos fundamentais.

É importante considerar que, mesmo que a novel legislação protetiva classifique o que são dados pessoais sensíveis, é necessário encarar tal conceito por uma visão dinâmica, haja vista que dados que *a priori* não são sensíveis, podem se tornar quando combinados com outras informações que levem a dados sensíveis de seus titulares.

As novas legislações no panorama nacional e internacional visam garantir a partir de suas disposições normativas a tutela dos direitos do usuário contra os riscos que ameaçam sua personalidade em face do processamento de seus dados pessoais e também a garantia de controle do fluxo desses dados na sociedade, principalmente no que tange aos dados pessoais sensíveis, haja vista o seu demarcado poder de utilização para finalidades discriminatórias ou lesivas

Estes novos marcos legislativos não visam frear o desenvolvimento tecnológico, mas sim compatibilizar este com os direitos e expectativas dos titulares de dados pessoais, viabilizando o tratamento legítimo destes.

REFERÊNCIAS

BAUMAN, Zygmunt. **Vigilância Líquida**. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2014.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: A função e os limites do consentimento.** Rio de Janeiro. Forense, 2019.

BRASIL. **CÓDIGO CIVIL**. LEI Nº 10.406 DE 10 DE JANEIRO DE 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm>. Acesso em 17 de outubro de 2019.

BRASIL. LEI Nº 12.414 DE 09 DE JUNHO DE 2011. **Lei do Cadastro Positivo**. Brasília, DF, junho de 2011. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em 12 de outubro de 2019.

BRASIL. LEI Nº 12.965 DE 23 DE ABRIL DE 2014. **Marco Civil da Internet**. Brasília, DF, abril de 2014. Disponível em: < http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm>.
Acesso em 22 de setembro de 2019.

BRASIL. LEI Nº 13.709 DE 14 DE AGOSTO DE 2018. **Lei Geral de Proteção de Dados Pessoais**. Brasília, DF, agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 12 de outubro de 2019.

CASTELLS, Manuel. **A Galáxia Internet: reflexões sobre a Internet, negócios e a sociedade**. Zahar, 2003.

CASTRO, Luiz Fernando Martins. **Proteção de dados pessoais- panorama internacional e brasileiro.** Revista CEJ, v. 6, n. 19, p. 40-45, 2002.

D´AQUINO, Fernando. **A história das redes sociais: como tudo começou**. Disponível em www.tecmundo.com.br. Acesso em 29 de setembro de 2019.

DA COSTA, Mariana Monteiro. **A Era da Vigilância no Ciberespaço e os Impactos da Nova Lei Geral de Proteção de Dados Pessoais no Brasil: Reflexos no Direito à Privacidade.** Rio de Janeiro, 2018.

DA SILVEIRA, Sergio Amadeu. **Tudo sobre tod@s: Redes digitais, privacidade e venda de dados pessoais**. Edições Sesc, 2017.

DE ANDRADE, Gustavo Piva. **O GDPR e a proteção dos dados sensíveis.** Disponível em: <https://www.migalhas.com.br/dePeso/16,MI280651,71043-O+GDPR+e+a+protecao+dos+dados+sensiveis>. Acesso em 20 de outubro de 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, 2011.

DONEDA, Danilo. **Pessoa e privacidade na sociedade da informação, Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **Reflexões sobre proteção de dados pessoais em redes sociais. Revista Internacional de Protección de Datos Personales**, n. 1, 2012.

ESTEVE, Asunción. **The business of personal data: Google, Facebook, and privacy issues in the EU and the USA**. International Data Privacy Law, v. 7, n. 1, p. 36-47, 2017.

EUROPEAN DATA PROTECTION SUPERVISOR, **Opinion 3/2018. EDPS Opinion on online manipulation and personal data**. Março de 2018. Disponível em: <https://edps.europa.eu/shttps://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdfites/edp/files/publication/18-03-19_online_manipulation_en.pdf>. Acesso em 20 de outubro de 2019.

FRAZÃO, Ana. **Nova LGPD: o tratamento dos dados pessoais sensíveis**. Disponível em: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018>. Acesso em: 11 de outubro de 2019.

FRAZÃO, Ana. **Nova LGPD: principais repercussões para a atividade empresarial.** Disponível em: <https://www.ab2l.org.br/nova-lgpd-principais-repercussoes-para-a-atividade-empresarial/>. Acesso em: 26 de outubro de 2019.

Here's Why Data Is Not The New Oil. Bernard Marr, Forbes, 2018. Disponível em: <https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/#292b93b23aa9> Acesso em 05 de outubro de 2019.

LEONARDI, Marcel. **Tutela e privacidade na internet**. Editora Saraiva, 2012.

MAGRANI, Eduardo. **Direito e Tecnologia**. Rio de Janeiro: FGV, 2016.

MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. 2ª Edição. Porto Alegre: Arquipélago Editorial, 2019.

MANGETH, Ana Lara; NUNES, Beatriz; MAGRANI, Eduardo. **Seis pontos para entender o Regulamento Geral de Proteção de Dados da EU**. ITS Rio, 2018. Disponível em: <https://feed.itsrio.org/seis-pontos-para-entender-a-lei-europeia-de-prote%C3%A7%C3%A3o-de-dados-pessoais-gdpr-d377f6b691dc>. Acesso em 26 de outubro de 2019.

MARTINS, Ana Paula Pereira. **Vazamento e Mercantilização de Dados Pessoais e a Fragilidade da Segurança Digital do Consumidor: um estudo dos casos Netshoes e Uber.** Disponível em: < https://www.researchgate.net/profile/Ana_Martins195/publication/327416131_VAZAMENTO_E_MERCANTILIZACAO_DE_DADOS_PESSOAIS_E_A_FRAGILIDADE_DA_SEGURANCA_DIGITAL_DO_CONSUMIDOR_um_estudo_dos_casos_Netshoes_e_Uber/links/5b8e042e299bf114b7f05bbb/VAZAMENTO-E-MERCANTILIZACAO-DE-DADOS-PESSOAIS-E-A-FRAGILIDADE-DA-SEGURANCA-DIGITAL-DO-CONSUMIDOR-um-estudo-dos-casos-Netshoes-e-Uber.pdf> Acesso em: 19 de outubro de 2019.

MASILI, Clarissa Menezes Vaz. **Regulação do uso de dados pessoais no Brasil: papel do usuário na defesa de um direito à tutela de dados pessoais autônomo**. 2018.

MENDES, Laura Schertel. **Privacidade e dados pessoais. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação**. Panorama Setorial da Internet. Número 2. Junho, 2019. Ano 11.

MULHOLLAND, Caitlin Sampaio. **Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18).** Revista de Direitos e Garantias Fundamentais, v. 19, n. 3,2018.

NETO, Eugênio Facchini; DEMOLINER, Karine Silva. **Direito à Privacidade e Novas Tecnologias: Breves Considerações Acerca da Proteção de Dados Pessoais no Brasil e na Europa**. REVISTA INTERNACIONAL CONSINTER DE DIREITO Ano IV–Número VII, v. 7, 2019.

NETO, Pery Saraiva; FENILI, Maiara Bonetti**. NOVOS MARCOS LEGAIS SOBRE PROTEÇÃO DE DADOS PESSOAIS E SEUS IMPACTOS NA UTILIZAÇÃO E TRATAMENTO DE DADOS PARA FINS COMERCIAIS.** Revista de Estudos Jurídicos e Sociais-REJUS ON LINE-ISSN 2594-7702, v. 1, n. 1, 2018.

O que são dados pessoais? Comissão Européia. Disponível em: < https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt#resposta > Acesso em 05 de outubro de 2019.

OCDE. **Addressing the Tax Challenges of the Digital Economy, Action 1 - 2015 Final Report, OECD/G20 Base Erosion and Profit Shifting Project**. OECD Publishing, Paris, 2015. Disponível em: [http://dx.doi.org/10.1787/9789264241046-en]. Acesso em 29 de setembro de 2019.

PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. Editora Atlas SA, 2000.

PINHEIRO, Patrícia Peck. **Direito digital.** Saraiva Educação SA, 2016.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. Saraiva Educação SA, 2018.

PNAD Contínua TIC 2017: Internet chega a três em cada quatro domicílios do país. **IBGE, 2019**. Disponível em: < https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/23445-pnad-continua-tic-2017-internet-chega-a-tres-em-cada-quatro-domicilios-do-pais>**.** Acesso em: 29 de setembro de 2019.

SCHERKERKEWITZ, Iso Chaitz. **Direito e internet**. Ed. Revista dos Tribunais, 2014.

SILVEIRA, Sergio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce. **A privacidade e o mercado de dados pessoais| Privacy and the market of personal data**. Liinc em Revista, v. 12, n. 2z, 2016.

SOLOVE, Daniel J. **Conceptualizing Privacy**. California Law Review, California, v. 90, jul. 2002.

The world's most valuable resource is no longer oil, but data. The Economist, 2017. Disponível em <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data >. Acesso em 05 de outubro de 2019.

TOMAÉL, Maria Inês et alii. **Das redes sociais à inovação**. Disponível em: scholar.google.com.br – scielo.br. Acesso em 29 de setembro de 2019.

UNIÃO EUROPÉIA. Regulation 2016/679 of The European Parliament and of The Council of 27 april 2016. **General Data Protection Regulation**. Disponível em: <

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.
Acesso em: 12 de outubro de 2019.
VALENTE, Jonas**. Privacidade em Perspectivas**. Organizadores: Sérgio Branco, Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

PARECER

A monografia-final de curso de **Clarissa Maria Lima Moura** apresentada à defesa de título ***DADOS PESSOAIS COMO ATIVO NA ECONOMIA DIGITAL: A tutela jurídica na legislação nacional e europeia acerca da manipulação de dados sensíveis para fins econômicos*** atende aos requisitos formais.

O tema é atual e relevante, que parte dos efeitos da chamada revolução digital, especificamente na utilização de dados pessoais sem autorização, trazendo sérias implicações que passam a ser ponto da Lei Geral de Proteção de Dados.

Os argumentos postos reforçam o esforço na pesquisa que resulta na monografia, trabalho de conclusão de curso, recomendado à defesa pública.

É o parecer.

Recife, 27 de outubro de 2019.

Prof.ª Eugênia Cristina Nilsen Ribeiro Barza