Centro Universitário de Brasília – UniCEUB
Faculdade de Ciências Jurídicas e Sociais – FAJS

PAULO VÍTOR FERREIRA GUIMARÃES

A Lei de Proteção de Dados e a Evolução da Preservação do Direito à Privacidade: Quanto ao Armazenamento de Dados

Brasília
2020

PAULO VÍTOR FERREIRA GUIMARÃES

A Lei de Proteção de Dados e a Evolução da Preservação do Direito à Privacidade: Quanto ao Armazenamento de Dados

Artigo científico apresentada como requisito parcial para a obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais- FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor André Gontijo

Brasília

2020

PAULO VÍTOR FERREIRA GUIMARÃES

A Lei de Proteção de Dados e a Evolução da Preservação do Direito à Privacidade: Quanto ao Armazenamento de Dados

Artigo científico apresentada como requisito parcial para a obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais- FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor André Gontijo

BRASÍLIA, 1 de outubro de 2020

BANCA AVALIADORA

_____

Professor(a) Orientador(a)

_____

Professor(a) Avaliador (a)

A Lei de Proteção de Dados e a Evolução da Preservação do Direito à Privacidade: Quanto o Armazenamento de Dados

Paulo Vitor Ferreira Guimarães

RESUMO

O presente artigo tem como objetivo de analisar o direito à privacidade e a disseminação de dados no ciberespaço, assim como seus efeitos no mundo jurídico. A partir de um estudo sob a égide da Constituição Federal de 1988, além da Lei Geral de Proteção de Dados (Lei n. 13.709/2018) e a General Data Protection Regulation (GDPR, Lei regulatória oriunda da União Europeia), firmou-se o entendimento de que o Legislador brasileiro não esgotou sobre o tema em sua totalidade, em especial, no que cerne às paredes de rastreamento (tracking walls), possibilitando que a sociedade tenha suas garantias fundamentais conduzidas e armazenadas sem regulação específica.

Palavras-chave: Direito à Privacidade. Ciberespaço. Internet. Constituição Federal. Lei Geral de Proteção de Dados. General Data Protection Regulation. Paredes de rastreamento.

1. INTRODUÇÃO

O presente artigo visa analisar o conceito de privacidade, bem como relacioná-lo com a nova Lei Geral de Proteção de Dados Pessoais. Antes de mais nada, é preciso compreender que a legislação se aplica à captação, armazenamento e disseminação de dados no meio físico ou eletrônico, mas que o assunto se tornou premente em face da maior facilidade de captação de dados no meio eletrônico. Dados sempre foram importantes para que os fornecedores pudessem orientar e programar suas práticas comerciais.

Tal notoriedade ganha escala no atual contexto em razão da entrada em vigência da Lei de Geral de Proteção de Dados (Lei 13.709/2018), que por causa da sobrevinda pandemia da Covid-19, a imersão da sociedade global em um mundo cada vez mais digital suplicava por uma imediata medida de garantia dos direitos fundamentais e à proteção de seus dados.

Durante a quarentena brasileira (medida de segurança restritiva para o trânsito de pessoas, que visa diminuir a velocidade de transmissão do Coronavírus), a utilização da rede digital teve um considerável aumento de aproximadamente 50%, segundo dados da Agência Nacional de Telecomunicações (ANATEL). A facilidade de conseguir realizar várias atividades comumente estabelecidas de forma presencial, contribuiu para o aumento de novos usuários, e a nova realidade trouxe diferentes contornos para a funcionalidade da sociedade.

Assim, a compreensão sobre como a COVID-19 gerou um aumento no número de pessoas on-line, fazendo com que o direito à privacidade corresse maiores riscos de ser violado, em virtude da existência de "tracking walls" e "cookies walls", ferramentas que permitem o armazenamento e a coleta de dados pessoais.

Adiante, a pesquisa desenvolverá o conceito de privacidade como direito fundamental, analisando a evolução do reconhecimento desse direito na perspectiva internacional e do direito constitucional nacional, bem como o primeiro influenciou o segundo. Ainda, será tratada da Lei Geral de Proteção de Dados como legislação brasileira garantidora dos direitos fundamentais na perspectiva da globalização e da proteção de dados, enquanto marco teórico, com o objetivo de analisar o porquê da violação do direito à privacidade causada por paredes de rastreamento.

Pretende-se destacar a violação ao direito à privacidade no Brasil antes da nova legislação, abordando a evolução jurisprudencial, e demonstrando como o direito à privacidade foi condicionado e violado por diversos servidores para que dados dos usuários fossem rastreados.

2. FONTES JUSTIFICATIVAS PARA ESTUDO DO TEMA

Com os impactos atuais e as incertezas futuras causadas pela pandemia da COVID-19, subsiste um aumento exacerbado do número de pessoas conectadas ao meio virtual. Portanto, pretende-se estudar e analisar, por meio de estudos comparados, a legislação vigente e sua efetividade na proteção de dados pessoais contra a violação da privacidade da população.

Vale destacar também que o rastreamento on-line e a segmentação comportamental levantam sérias questões sobre a privacidade. Em diversos países, o rastreamento on-line para publicidade direcionada requer o consentimento dos usuários da internet para ser considerado legal. Nesse campo, as empresas utilizam de diferentes estratégias para coletar o consentimento das pessoas para o rastreamento on-line. Uma das estratégias é oferecer às pessoas a opção de "pegar ou largar", sendo que alguns sites operam por uso dos chamados “tracking walls”, também conhecidas como barreiras que os visitantes só podem ultrapassar se permitirem que o site ou seus parceiros os rastreiem.

De acordo com o art. 5º, inciso II, da Lei 13.709/18, dado pessoal sensível é aquele vinculado à pessoa natural e que versa sobre origem racial ou étnica, convicção religiosa, opinião, política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, saúde, vida sexual, genética ou biometria. Mostra-se importante alertar sobre tais informações, visto que se encontram vinculadas à personalidade e dignidade humana, ou seja, direitos fundamentais. Por serem informações de inquestionável importância, não podem ser submetidas a atividades arbitrárias por parte dos agentes controladores.

Nesse sentido, os dados produzidos pela segunda edição do Painel TIC COVID-19, promovido pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), ligado ao Comitê Gestor da Internet no Brasil (CGI.br), informa que as principais preocupações apontadas pelos usuários em relação ao uso de seus dados pessoais foram: prejuízo financeiro por fraudes bancárias (32%), roubo de identidade (23%), invasão de privacidade (21%), e venda de dados para terceiros (13%). O estudo abrange um universo de cerca de 97 milhões de pessoas, que corresponde a 80% dos usuários de Internet com 16 anos ou mais.

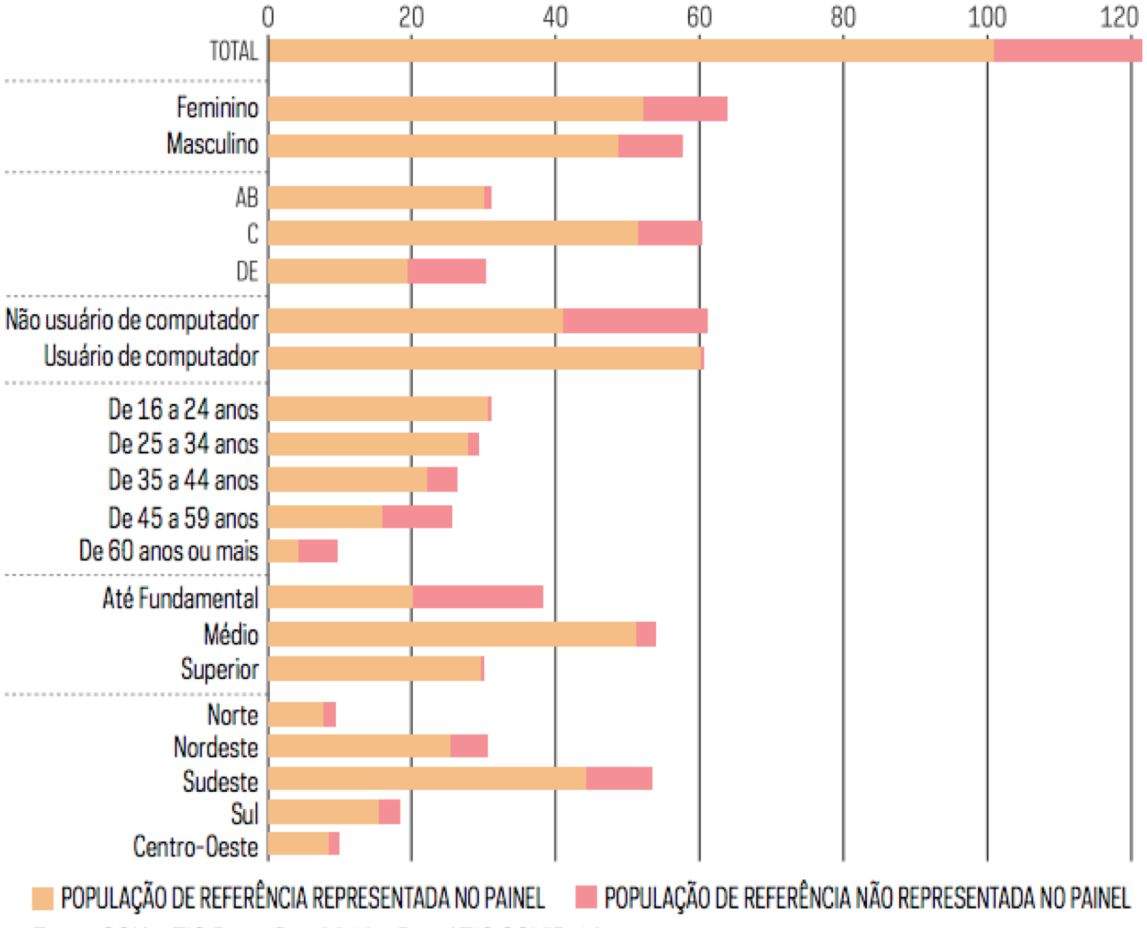
Nota-se, a partir dos dados supracitados, que há uma preocupação por parte da população com o uso de seus dados pessoais e qual seu destino. Compreendendo que a internet foi instituída como uma ferramenta para conectar pessoas e intercambiar informações, esta acabou se transformando numa gigantesca máquina armazenadora de dados, capaz de monitorar

informações de todo mundo, além de gravar buscas e interesses íntimos. Ainda, subsiste um fator agravador, qual seja, a pandemia teria aumentado o número de acessos no ambiente virtual, em razão das medidas de segurança aconselhadas pela Organização Mundial da Saúde (quarentena, trabalho remoto, aulas on-line).

Conforme os dados obtidos no Painel TIC COVID-19, que representava um contingente de cerca de 101 milhões de usuários de Internet, o que corresponde a 83% dos usuários na faixa etária considerada (16 anos e superiores), identificou-se um aumento expressivo na realização de serviços públicos e financeiros pela internet, durante o período em pandemia. Esse avanço foi ainda maior nas classes C, D e E, entre os usuários de internet com menor escolaridade, e também entre os não usuários de computador, conforme se depreende do gráfico:

GRÁFICO 1 - COMPARATIVO DA POPULAÇÃO DE USUÁRIOS DE INTERNET COM 16 ANOS OU MAIS NA POPULAÇÃO DE REFERÊNCIA E NO PAINEL TIC COVID-19

População em milhões



Fonte: CGI.br, TIC Domicílios 2019 e Painel TIC COVID-19.

Assim, pode-se notar o aumento dos acessos a serviços de forma virtual a partir das taxas apresentadas pelo Comitê Gestor da Internet no Brasil, e, junto dele, o possível aumento dos dados armazenados.

Nada obstante, O Cisco Visual Networking Index consolidou as informações sobre o tráfego global de dados na internet, que em 2014 atingiu 42,4 exabytes por mês, acima dos 32,8 exabytes mensais, em 2013. Isso significa 1,4 exabytes por dia, acima dos 1,1 exabytes diários obtidos em 2013. Segundo o Cisco, o tráfego global da internet, em 2014, foi equivalente a 127 bilhões de DVDs, 11 bilhões de DVDs por mês ou 15 milhões de DVDs por hora. Em 2014, o tráfego da internet foi equivalente a 21 vezes o volume de toda a internet em 2005. Ou seja, quantidade de dados pessoais captados e armazenados para o uso pelo capital aumenta quanto mais cresce o uso das redes de serviços, informações e entretenimento.

Nessa senda, será cotejada a aplicabilidade da Lei Geral de Proteção de Dados – LGPD (Lei 13.709/2018), que entrou em vigor no ano de 2020, para tentar a chave da proteção de dados em vista de assegurar o direito fundamental à privacidade, com base na análise comparada à General Data Protection Regulation (GPDR) da União Europeia.

3. O DIREITO FUNDAMENTAL À PRIVACIDADE

Preliminarmente, é necessário compreender as distinções teóricas e conceituais sobre o direito fundamental à privacidade. O artigo abordará o conceito de direito fundamental; a privacidade como direito fundamental da pessoa humana e sua evolução no Direito Internacional e na perspectiva do Direito Constitucional; por fim, como a privacidade é violada quando os dados inseridos no meio virtual são rastreados e armazenados sem o consentimento expresso dos usuários.

O direito à privacidade no Brasil, assim como em outros diversos países, é assegurado constitucionalmente como direito humano fundamental. A Constituição Federal brasileira não se restringe apenas ao direito à privacidade, apresentando abrangência em relação à preservação da vida privada e da intimidade da pessoa, a inviolabilidade da correspondência, do domicílio e das comunicações, em consonância com o previsto no artigo 5º, inciso 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" e no inciso 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". (BRASIL, 1988)

Em sede do entendimento da privacidade como um direito fundamental, faz-se necessário observar o conceito de direitos fundamentais como normas jurídicas de George Marmelstein:

> "[...] ligadas à ideia de dignidade da pessoa humana e de limitação do poder, positivadas no plano constitucional de determinado Estado Democrático de Direito, que, por sua importância axiológica, fundamentam e legitimam todo o ordenamento jurídico" (2008, p. 20).

Apesar do conceito fomentado por Marmelstein, a noção de o direito fundamental estar ligado diretamente à ideia de dignidade, ocasiona a necessidade de voltar-se para um dos problemas centrais ao se tratar do direito fundamental, como explicitado por Bobbio (2004): "o problema fundamental em relação aos direitos do homem, hoje, não é tanto o de justificá-los, mas o de protegê-los. Trata-se de um problema não filosófico, mas político".

A proteção de um direito fortifica a ideia de estabilidade dentro de uma sociedade e, sob o prisma do desenvolvimento, a noção de que um direito fundamental fomenta segurança para sociedade. Nesse sentido, é possível tender a existência e a evolução do direito à privacidade para o lado do poder de polícia do Estado, em querer preservar sua privacidade, e não tender a um crescimento moral e filosófico de preservar a ideia do indivíduo.

Vislumbrando o do conceito de Direito Fundamental, José Afonso da Silva (2005) assevera:

> "Direitos fundamentais do homem [..], além de referir-se a princípios que resumem a concepção do mundo e informam a ideologia política de cada ordenamento jurídico, é reservada para designar, no nível do direito positivo, aquelas prerrogativas e instituições que ele concretiza em garantias de uma convivência digna, livre e igual de todas as pessoas".

Perpetuando o conhecimento, o professor Gilmar Mendes, na revista Diálogo Jurídico (2002), adiciona:

> "Os direitos fundamentais são, a um só tempo, direitos subjetivos e elementos fundamentais da ordem constitucional objetiva. Enquanto direitos subjetivos, os direitos fundamentais outorgam aos titulares a possibilidade de impor os seus interesses em face dos órgãos obrigado. Na sua dimensão como elemento fundamental da ordem constitucional objetiva, os direitos fundamentais - tanto aqueles que não asseguram, primariamente, um direito subjetivo, quanto aqueloutros, concebidos como garantias individuais - formam a base do ordenamento jurídico de um Estado de Direito democrático. " (MENDES, P.2)

Ademais, apesar da "concreção positiva" (LUÑO, 1995), não há incompatibilidade entre as normas de direitos humanos e de direitos fundamentais, o que se comprova pela incorporação de normas internacionais ao direito interno.

4. A IMPORTÂNCIA DO DIREITO À PRIVACIDADE NA ESFERA INTERNACIONAL

De início, faz-se importante distinguir o conceito de direito fundamental e de direitos humanos, pois, apesar de o constituinte de 1988, prever no artigo 4°, inciso II, que os direitos humanos são aqueles que se referem às relações internacionais, há uma verdadeira "balbúrdia terminológica" que assola a doutrina (CAVALCANTE FILHO, p.5). Para tentar amenizar tal problemática, Peces-Barba , portanto, conclui:

> "são faculdades que o direito atribui a pessoa e aos grupos sociais, expressão de suas necessidades relativas à vida, liberdade, igualdade, participação política ou social, ou a qualquer outro aspecto fundamental que afete o desenvolvimento integral das pessoas em uma comunidade de homens livres, exigindo o respeito ou a atuação dos demais homens, dos grupos sociais e do Estado, e com garantia dos poderes públicos para restabelecer seu exercício em caso de violação ou para realizar sua prestação" Peces-Barba (1982, p. 7)

No que tange à privacidade, seu objeto principal baseia-se na moral e a integridade do sujeito. O artigo 12, da Declaração Universal dos Direitos Humanos, de 1948, promulgada no Brasil, pelo Decreto no 19.841/1945, prevê que:

> "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda pessoa tem direito à proteção da lei.".

A criação de um panorama internacional de privacidade e proteção de dados pessoais foi percebido a partir do ano de 1990, estando diretamente relacionado ao inerente desenvolvimento econômico, que passou a ter uma subordinação muito maior dos fluxos internacionais de bases de dados, especialmente relacionados aos indivíduos e disponibilizados pelo avanço da tecnologia globalizada.

Destarte, houve a necessidade de uma repactuação dos governantes com a sociedade, para que, com o advento do meio virtual, direitos e garantias não fossem abandonados, tais como: a privacidade e segurança. Direitos esses que já eram inegáveis, desde a Declaração Universal dos Direitos Humanos (DUDH) de 1948.

O alicerce da Declaração Universal dos Direitos Humanos está em prover a liberdade da sociedade, mas a sua sensatez é proveniente da transparência. Nesse sentido, as leis de proteção de dados possuem, em sua redação, uma particularidade própria, que por meio de seus arcabouços é possível medir e controlar se o compromisso está sendo executado.

5. EVOLUÇÃO HISTÓRICA DA PROTEÇÃO DE DADOS NO BRASIL

A princípio, faz-se a comparação da sociedade atual com a estrutura do panóptico, criada por Jeremy Benthan, visto que este retrata uma penitenciária, onde todos os presos estariam sempre sendo vigiados, ou com a sensação de estarem. Dessa forma, na sociedade digital, independente do consentimento, as pessoas permaneceriam vigiadas através da circulação ilimitada de dados no *cyberspace*.

No âmbito nacional, a questão da proteção de dados vem sendo debatida há quase uma década. No entanto, até 2014, o ordenamento jurídico brasileiro ainda não possuía um marco regulatório federal para disciplinar a proteção geral de dados pessoas de uma forma completa e unificada; a regulamentação era feita de forma esparsa, carecendo de uniformidade e segurança jurídica. (BIONI, Bruno Ricardo. De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados pessoais).

Nesse diapasão, a Constituição Federal servia como a principal resposta jurídica aos litígios que vinham surgindo, relacionados ao cenário do crescente hiperconectividade. Embora o constituinte originário não pudesse prever ao final da década de 80, os riscos que envolvem a proteção de dados atualmente, o art. 5º, inciso X, da CRFB/88, já previa a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, garantindo o direito de "indenização pelo dano material ou moral, decorrente de sua violação". (DONEDA, Danilo. A proteção de dados pessoais como direito fundamental. Revista Espaço Jurídico 12/103, Joacaba: Unose, 2011, p. 103)

Com o passar do tempo, também se tornaram aplicáveis outros diplomas, tais como o Código Civil, dispondo, por exemplo, sobre a proteção à personalidade, imagem e intimidade. A lei de acesso à informação (LAI), o Código de Defesa do Consumidor (CDC), o Marco Civil da Internet (MCI), a Lei do Cadastro positivo e a Lei de delitos informáticos (Lei 10.406, de 10 de janeiro de 2002, art. 21; Lei 12527, de 18 de novembro de 2011, §3º, II, art. 37); Lei 8.078/90, art. 43; art. 6º art. 8, art. 10, art. 12, art 14).

Nesse teor, também se destaca acerca do CDC, que define quais são os direitos básicos do consumidor e, dentre as práticas comerciais utilizadas para captação de dados, algumas já poderiam ser enquadradas como abusivas. Com efeito, o consumidor que tinha seus dados eventualmente coletados pelo fornecedor sem perceber o fato e, portanto, sem anuir com essa conduta, já estava em situação de vulnerabilidade técnica – que pode ensejar manifestação de vontade viciada – uma vez que não lhe foram corretamente informadas as características essenciais do serviço (BLUM, Rita Peixoto Ferreira. O direito à privacidade e à proteção dos dados do consumidor. São Paulo: Almedina, 2018, p 61).

Desta forma, assim como o diploma consumerista, o Marco Civil da Internet também demonstrou uma preocupação fundamental com a tutela da segurança e da privacidade dos dados pessoais, ao restringir o acesso ou uso de informações privadas na internet. Não à toa, o MCI, também prevê o respeito às regras de consumo; inviolabilidade da intimidade da vida privada, bem como, do sigilo no fluxo de comunicações pela internet; guarda e disponibilização dos registros de acesso a aplicações de internet, devendo atender à preservação da intimidade, honra e imagem das partes envolvidas.

No entanto, em que pese o avanço gradual na tutela da privacidade dos dados pessoais, essa evolução se mostrava lenta, frente aos desafios dos novos tempos. No contexto da sociedade da informação, nota-se que o desenvolvimento da tecnologia e das técnicas de marketing ensejam, ao mesmo tempo, benefícios e desafios à tutela de direitos fundamentais.

6. A GDPR - GENERAL DATA PROTECTION REGULATION: RELAÇÃO ENTRE DIREITOS E RESPONSABILIDADES

O debate acerca da proteção de dados teve sua origem na União Europeia (UE), a qual foi uma das fontes de inspiração para a elaboração da LGPD. No caso, os primeiros "Privacy Impact Assessment" (PIA) foram previstos na Diretiva nº 95/46/EC (Diretiva) e estavam relacionados à prevenção e mitigação de riscos, envolvendo possíveis violações aos direitos dos titulares.

A atualização da Diretiva teve início com um grande debate dentro da União Europeia, em especial com o partido "The Greens", e se consolidou na promulgação do Regulamento Geral de Proteção de Dados Pessoais Europeu n. 679, aprovada em 27 de abril de 2016 (GDPR), com o objetivo de abordar a proteção das pessoas físicas, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, conhecido pela frase "free data flow". Sendo

que a GDPR conseguiu o que a Diretiva não fez, que foi tornar os relatórios de impacto destaque no cenário regulatório de proteção de dados no mundo.

Por fim, em maio de 2018, com a vigência da GDPR, que substituiu uma antiga diretiva da União Europeia, antes facultativa, sobre tratamento de dados, mostrou-se ao Brasil a necessidade de uma legislação vinculativa sobre o assunto. Ademais, o regramento europeu dispõe que só pode haver fluxo internacional de dados se outro país tiver uma lei adequada de proteção da privacidade, semelhante à GDPR.

Com o objetivo de reduzir os riscos de abusos na coleta, tratamento, uso e transferência de dados na União Europeia (UE), em 2016, foi publicado o Regulamento Geral de Proteção de Dados ("general data protection regulation" – GDPR). Após uma *vacatio legis* de dois anos, essa norma entrou em vigor em maio de 2018, estabelecendo um novo regime regulatório para todos os estados membros da UE, e substituindo, assim, a antiga diretiva 95/46 CE, de 1995.

Em linhas gerais, segundo a GDPR, as empresas necessitam obter o consentimento expresso e inequívoco dos titulares de dados para autorizar a coleta e tratamento, devendo expor claramente como essas informações serão utilizadas, além de explicar o mecanismo pelo qual os indivíduos poderão revogar este consentimento.

Com base no exposto, as empresas restaram obrigadas a cumprir medidas de proteção de dados a partir da criação de qualquer nova tecnologia, garantindo também que os mecanismos de proteção adequada sejam incorporados aos produtos já existentes.

Além dessa importante restrição ao uso indiscriminado dos dados pessoais, segundo o princípio "accountability", os processadores de dados sujeitos às disposições da GDPR, precisaram manter registros detalhados de suas atividades, exigindo-se que as organizações implementem medidas técnicas e organizacionais apropriadas, e sejam capazes de prestar contas e demonstrar sua eficácia, quando solicitadas.

Na Europa, a política de privacidade do Facebook Inc. foi objeto de recentes questionamentos à rede social, a qual teria descumprido a lei francesa de proteção de dados pessoais, ao, supostamente, vender informações de navegação dos seus usuários para empresas interessadas em realizar anúncios de produtos e serviços, por meio de publicidade direcionada. (Direito privado e internet/ Guilherme Magalhães Martins – são Paulo: atlas, 2014, p. 62)

Considerando esse cenário, o regramento europeu também exigiu que as empresas responsáveis pelo processamento de um grande volume de dados deveriam ser demandadas a nomear um "data protection officer", para monitorar as atividades e garantir o cumprimento da

GDPR. Assim, qualquer violação à privacidade de dados pessoais deveria ser notificada ao órgão regulador, no prazo máximo de 72 horas, após identificação do fato.

Com efeito, as sanções previstas na GDPR, também são mais gravosas, chegando a multas de até 2% do volume anual de negócios mundiais da empresa infratora, com uma multa mínima de 10 milhões de euros.

Dessa forma, espera-se que essa regulação crie limites ao tratamento e processamento de dados pessoais pelas empresas envolvidas nesse contexto. Ainda, convém ressaltar que o direito europeu vai além do conceito básico de dados pessoais (nome, número de identidade, CPF) e, considera informações que, apesar de isoladamente não identificarem alguém, acabam levando a uma possível identificação. Assim, consideram-se dados de localização geográfica, endereço de IP, assim como o perfil comportamental sobre as notícias e anúncios clicados pelos consumidores. Com esse feito amplo, é difícil imaginar um cenário em que a referida lei não se aplique, no caso concreto.

Em seu art. 9º, a GDPR, destaca acerca da importância de uma categoria especial para os dados sensíveis, submetidos a um regime específico, que veda o processamento desse tipo de dado pessoal, exceto nas 10 hipóteses elencadas neste dispositivo. Simultaneamente, salvo raras exceções, o regramento europeu confere uma proteção especial àqueles dados capazes de revelar informações de cunho íntimo, por conter origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas.

Nesse sentido, já surge os primeiros litígios envolvendo a GDPR, na Europa. A iniciativa surgiu do portal “my pravicy is none of your business”, que ajuizou quatro ações perante autoridades administrativas na Áustria, Bélgica, Alemanha e França, respectivamente contra o facebook, instagram, whatsapp e google.

Por fim, convém ressaltar que, segundo o art. 46, da GDPR, uma vez obtido o consentimento expresso e inequívoco do titular de dados, os responsáveis pelo tratamento só poderão realizar a transferência desses dados para outros países ou organizações internacionais, se estes tiverem apresentados leis adequadas de proteção.

7. O TRATAMENTO LEGAL DADO PELA LEI GERAL DE PROTEÇÃO DE DADOS

Eis que, finalmente, em 10 de julho de 2018, o plenário do Senado Federal, aprovou o Projeto de lei da Câmara nº 53/2018, que altera o art. 7º, inciso X e o art. 16, inciso II, do Marco Civil da Internet, para disciplinar a proteção dos dados pessoais no Brasil e definir as situações em questões, que podem ser coletados e tratados, tanto por empresas, quanto pelo Poder Público.

Com isso, o Brasil saiu do rol minoritário de países para se juntar a diversos outros do mundo, que já possuem legislação específica sobre o tema. A Lei Federal nº 13.709, de 14 de agosto de 2018, entrou em vigor em agosto de 2020, tratando de diversos pontos que não possuíam previsão legal até então, ou eram abordados de maneira esparsa, por leis setoriais, que formavam uma "colcha de retalhos" sobre o tema.

Em vista da disponibilidade de dados pessoais na rede, faz com que se criem verdadeiros perfis de usuários, registrando desde os comportamentos pessoais, econômico e social. Informações que podem ser utilizadas para diversos fins, até comerciais. Além disso, tal exposição está diretamente ligada à invasão de privacidade.

Mostra-se produtiva a relação da análise do objeto estudado com os preceitos legais estabelecidos na Lei Geral de Proteção de Dados, aprofundada no decorrer deste, conforme segue:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I – o respeito à privacidade;
>
> II – a autodeterminação informativa;
>
> III – a liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV – a inviolabilidade da intimidade, da honra e da imagem;
>
> V – o desenvolvimento econômico e tecnológico e a inovação;
>
> VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Nessa senda, é possível observar que a tecnologia provoca um aumento desenfreado nas possibilidades e na velocidade do acesso à informação, levando consequentemente, a uma maior fragilidade da esfera privada, da intimidade das pessoas (COSTA JÚNIOR, 1970, p. 14). Neste cenário, a atuação da Lei de Proteção de Dados Pessoais (LGPD) e sua aplicação tornam-se ainda mais relevantes, já que a sociedade em um contexto totalmente dependente da tecnologia apresenta-se vulnerável aos riscos criados por esta, de maneira que se deve

estabelecer o poder julgador do Estado para responsabilizar as empresas coletoras de dados por interferência na privacidade dos usuários.

Dessa forma, a segurança dos dados no contexto da internet torna-se ponto de atenção, uma vez que as modernizações tecnológicas se tornaram tão avançadas, que os desenvolvedores muitas vezes não se atentam a garantir suficientemente segurança e privacidade das informações acessadas, com o mesmo empenho com que desenvolvem novas tecnologias.

O artigo 7º, da LGPD, abaixo transcrito, apresenta as hipóteses de tratamento de dados pessoais:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I.mediante o fornecimento de consentimento pelo titular;
> II.para o cumprimento de obrigação legal ou regulatória pelo controlador dos dados;
> III.pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos;
> IV.para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V.quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI.para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> VII.para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII.para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; IX.quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X.para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Finda, por ser importante citar o discurso feito pela Vice-Presidente da Comissão Europeia, Mackenzie Stuart Lecture, realizado em Cambrige no ano de 2019, sendo ele:

> "... data give us power. Power we can use to save resourcer, to find new solutions to our problems, to help us live happier and more fulfilling lives. So this is an exciting moment. But it's also a momente when we have choices to make, about who gets to use that power." Commissioner Vestager, Mackenzie Stuart Lecture, Cambridge 2019

Valendo-se do conhecimento citado, os dados se tornaram bens de maior valor na economia, substituindo o ouro e o petróleo das gerações anteriores. A discussão da privacidade

dos usuários e da proteção dos dados pessoais, se tornaram essenciais para que a sociedade possa estabelecer quais são os princípios fundamentais, para que precisamos seguir, defender, consolidando em legislações padrões normas de boas práticas em termos de uso de plataformas.

8. A PRIVACIDADE E SEUS CONFLITOS NORMATIVOS

Sob a jurisdição brasileira, o acesso e a utilização de dados pessoais dos consumidores, sem que tenham sido previamente consultados para a devida autorização, tem-se tornado algo bastante frequente, gerando um cenário estigmatizado pelo desrespeito à privacidade e intimidade. Ainda, observa-se que a maioria dos brasileiros não sabe se proteger no campo virtual, visto que, as informações que caracterizam certo indivíduo, para que possam ser conhecidas e manejadas, devem passar pelo crivo do aval deste, mas neste país, evidencia-se uma desatenção sobre os dados pessoais.

Compreende-se que a internet foi instituída como uma ferramenta para conectar pessoas e intercambiar informações, porém, esta acabou se transformando numa gigantesca máquina armazenadora de dados que monitora os dados de todo mundo, capaz de gravar buscas e interesses íntimos.

A coleta e utilização arbitrárias de dados pessoais dos consumidores, como registrado na parte introdutória deste artigo, são fatos que se alastram e não se restringem ao Brasil. Na matéria jornalística, da Revista Superinteressante, denominada "Como funciona a espionagem", consta a informação de que "Quase todos os sites estão interligados numa rede oculta – que monitora você", acessando qualquer sítio eletrônico, envia-se um arquivo, denominado cookie, que fica armazenado no celular do indivíduo, ou no seu computador, sendo que, atualmente, cerca de 80% (oitenta por cento) dessas estruturas informatizadas utilizam supercookies, como se observa no Google.

Existem várias técnicas para a obtenção de dados sobre os consumidores com o objetivo de concretização de publicidade comportamental, como: o monitoramento de navegação na internet; pode haver também, o monitoramento em variados sítios eletrônicos, pertencentes a organizações diversas, mas todas filiadas ao mesmo tipo de vigilância. A exemplo disso, tem-se a interceptação do fluxo de dados entre o usuário da internet e o site, técnica denominada de DPI (Deep Packet Inspection), é uma modalidade frequentemente utilizada. A mineração de dados (data mining) é outra sistemática que possibilita a identificação de informações relevantes para determinada atividade.

O consentimento nos sítios eletrônicos, implica a aceitação para a colocação de *cookies* (arquivos armazenados de forma temporária) em vários sites ou/e, para combinar dados que são coletados em sites de terceiros, de modo que, anunciantes e redes sociais, redes de mídia, podem colocar cookies de rastreamento para mostrar seus anúncios personalizados ou para seguir suas visitas ao site, caso navegue em sites fora da rede.

A tendência global de preocupação com a temática surge majorada frente ao escândalo de vazamento de dados do Facebook, a mais famosa rede social mundial da atualidade, que possui informações privadas de milhões de usuários, as quais foram compartilhadas indevidamente com a empresa britânica de *big data* e marketing político Cambridge Analytica, gerando um grande conflito sociopolítico e com grande reflexo nas eleições presidenciais norte-americanas em 2016.

Estima-se que 87 milhões de informações pessoais foram coletadas pela empresa britânica indevidamente, segundo a revista Exame, demonstrando a necessidade iminente de haver maior proteção das empresas em relação aos dados de seus usuários.

A compreensão das atuais normas que regem o tratamento de dados pessoais no Brasil pressupõe a prévia análise de conceitos essenciais que determinam o seu âmbito de aplicação. Sobre o conceito de dados pessoais, "compreendem qualquer informação alfabética, gráfica, fotográfica, acústica, independente do suporte (som e imagem)."(CASTRO,2005, P.78).

Tem-se como regra principal para o tratamento de dados pessoais o disposto pelo art. 7º, inciso I, da Lei 13.709/18. Estabelece o §5º, deste mesmo dispositivo, que o controlador, que obteve a permissão para lidar com as referidas informações, caso objetive comunicá-las ou realizar o seu compartilhamento com outros agentes, deverá providenciar confirmação específica. O uso em conjunto de dados pessoais poderá ocorrer entre entes ou órgãos públicos, no cumprimento de suas competências legais, assim como entre estes e entidades privadas, envolvendo a comunicação, difusão, transferência internacional.

Tratando-se de dados sensíveis, dispõe o art. 11, §3º, da Lei 13.709/18, que, na hipótese de a comunicação, ou o uso compartilhado, tiver o objetivo de obter vantagem econômica, poderá "ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências".

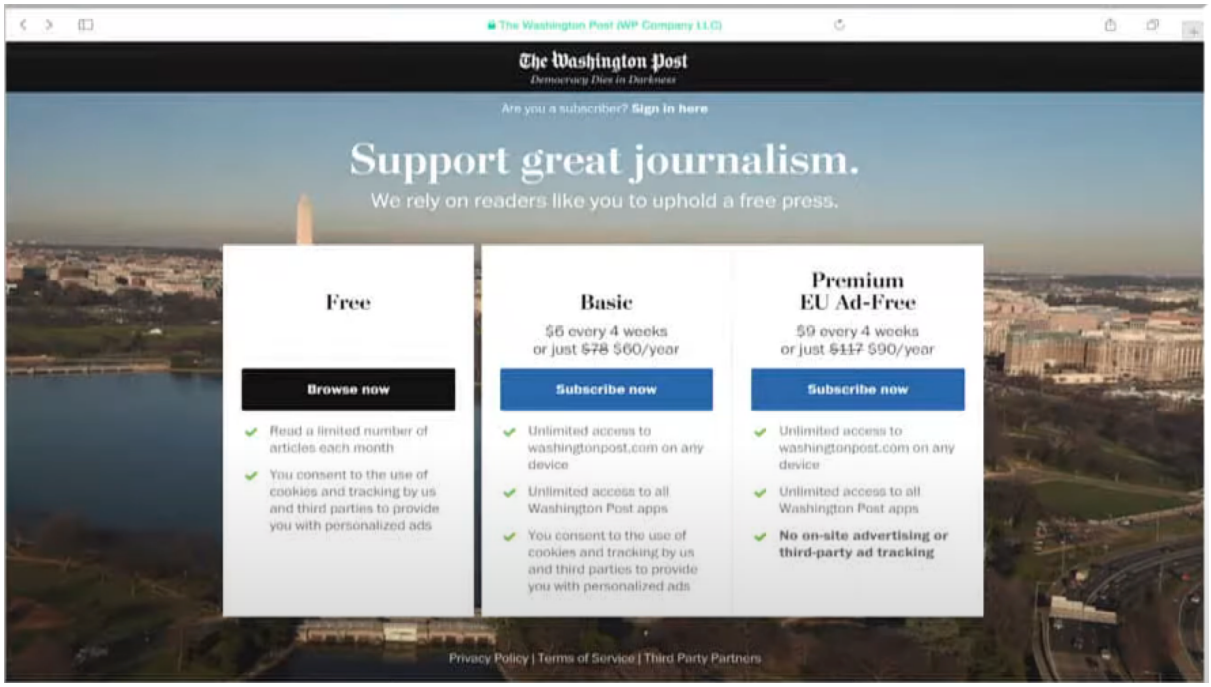
Além da classificação diferenciada, esse gênero de dado pessoal também possui forma de tratamento diversa. O seu tratamento se restringe aos casos nos quais o autor dos dados consente de forma específica e destacada, para finalidades específicas, exceto em algumas

hipóteses de exigências legais, judiciais e em usos por órgão de pesquisas, que deverão se comprometer com o anonimato dos titulares dos dados. O artigo 11, da LGPD, abaixo transcrito, apresenta as hipóteses de tratamento de dados pessoais:

> Art. 11 O tratamento de dados pessoais sensíveis:
> I.mediante o fornecimento de consentimento pelo titular;
> II. para o cumprimento de obrigação legal ou regulatória pelo controlador dos dados;
> III. pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos;
> IV.para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V.para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> VI.para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VII.para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

Mesmo que consentimento do titular dos dados pessoais seja primordial para o início do tratamento, verifica-se sua dispensa nas hipóteses dispostas no art. 7º, incisos II a X, da Lei 13.709/2018. Antes de qualquer ato vinculado à atividade, o controlador deverá observar se há manifestação livre, informada e inequívoca, pela qual o titular concorda com o procedimento que se refere às informações sobre a sua pessoa, para determinada finalidade explicitada. É o que dispõe o inciso XII, do art. 5º, do referido diploma legal. Quanto à forma, o art. 14, estabelece que deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular, dando-se ensejo à comprovação pelos meios eletrônicos avançados.

O modelo do sítio eletrônico do jornal americano Washington Post, atraiu muita atenção da União Europeia, no ano de 2019, pois normalmente o conteúdo digital de grandes jornais não é feito de forma gratuita, porém o jornal americano abre a possibilidade de se ter o conteúdo grátis, porém é necessário dar acesso a informações pessoais, ou é possível, pagar pelo conteúdo e ter menos processamento de dados.



(Notícia fornecida por Orla Linksey no 10º Seminário de Proteção à Privacidade e aos Dados Pessoas, em São Paulo em setembro de 2019)

Assim sendo, o debate provocou o entendimento de duas vertentes: i) que seria uma forma do mercado responder a legislação vigente; ii) que as pessoas estão pagando por seus direitos fundamentais.

E, se observarmos pelo prisma da segunda vertente, temos que diante de um Estado Democrático de Direito, sendo o Estado que visa à garantia do exercício de direitos individuais e sociais e os poderes constituídos (Legislativo, Executivo e Judiciário), são organizados de forma a que um não avance sobre a função precípua do outro. Considera-se que a liberdade de informação deve ser conceituada como um direito fundamental, oriundo da necessidade do homem de ter conhecimento dos fatos, para assim compreender o mundo em que habita. Dessa forma, de maneira livre, consegue formar sua opinião e reproduzir o conhecimento adquirido.

Para Cláudia Mara de Almeida Rabelo Viegas, o direito à liberdade de informação é corolário do direito à liberdade de manifestação, e estes podem ser utilizados tanto para o acesso, quanto para a divulgação de informações. Assim, depreende-se que a obtenção da informação decorre do relacionamento ou da troca de conhecimento entre particulares, sendo capaz de ser adquirida e multiplicada por intermédio dos meios de comunicação.

Nessa mesma perspectiva, Cláudio Luiz Bueno de Godoy se manifesta, *in verbis*:

> "antes concebido como um direito individual, decorrente da liberdade de manifestação e expressão do pensamento, modernamente vem sendo entendido como

> dotado de força componente e interesse coletivos, a que corresponde, na realidade de um direito à informação" (GODOY, 2001, p 49).

A própria Constituição, em seu art. 5º, incisos XIV e XXXIII, contempla o viés coletivo ao direito à informação:

> 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 prosperidade, nos termos seguintes:
> [...]
> XIV – é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;
> [...]
> XXXIII – todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado." (BRASIL, 1988).

No caso *supra*, verificou-se que este ainda não teve solução, mas tende a seguir pela não sobreposição dos direitos fundamentais às regras ou princípios internacionais, devendo haver uma harmonização ligada ao caso, para que prevaleça a liberdade de imprensa e o respeito à privacidade .

9. CONSIDERAÇÕES FINAIS

A partir das pesquisas e dos dados obtidos, realizou-se a sistematização das informações para alcance da seguinte etapa, a análise. Com base nos dados coletados por meio de sítios eletrônicos, bem como daqueles recebidos através dos requerimentos de informação, resta possível identificar se foram produzidas alterações normativas, no que toca a proteção do rastreamento de dados.

Desse modo, nesta última etapa estabeleceu-se um diálogo entre a sistematização dos resultados, relacionando o referencial teórico com as conclusões obtidas acerca do rastreamento de dados e a proteção do direito à privacidade.

Como foi demonstrado, em um comparativo com a LGPD, a GDPR tem objetivos que condizem com os da Lei nacional, visando também, assegurar direitos fundamentais de pessoas naturais, mediante proteção de dados, garantindo o direito à privacidade. A legislação brasileira, aos moldes da legislação europeia, introduz a regulação estatal sobre uma realidade que eclodiu com a chegada dos normativos de proteção de dados. A ética autorregulada dos operadores comunicacionais e econômicos da era digital passou a ter uma nova legislação, a

qual deve-se adequar. Na atual conjuntura de evolução digital, vive-se em um mundo onde a publicidade direcionada irrompe diariamente na tela dos aparelhos digitais dos cidadãos, e, consequentemente, a informação pessoal se torna cada dia mais valiosa. Nesse diapasão, medidas como a Criação da Lei n° 13.709/2018, resultam como necessárias ao desenvolvimento social saudável, tanto dentro do mundo virtual, quanto fora.

Nesse teor, a partir dos dados auferidos, pode-se afirmar que no Brasil, subsiste a problemática dos direitos fundamentais, tais como a privacidade e liberdade de informação, conflitando com os direitos inerentes à personalidade. Mesmo se comparados, esses fundamentos possuem embasamento constitucional, o que dificulta o deslinde da controvérsia.

REFERÊNCIAS

BENTHAM, Jeremy. O Panóptico. Belo Horizonte: Autêntica, 2000. (Organização e tradução de Tomaz Tadeu da Silva).

BIONI, Bruno Ricardo. De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados pessoais, 03 de julho de 2018. Disponível em: < https://www.anoregsp.org.br/noticias/32539/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados>. Acesso em : 24 de setembro de 2020

BLUM, Rita Peixoto Ferreira. O direito à privacidade e à proteção dos dados do consumidor. São Paulo: Almedina, 2018, p 61

BOBBIO, Norberto. **A Era dos Direitos**. 8 reimp. Rio de Janeiro: Elsevier, 2004.

BOYD, Danah. Big Data:Opportunities for computation a land social sciences.Disponível em: www.zephoria.org/thoughts/ archives/2010/04/17/big-data-opportunities-for-com- putational-and-social-sciences.html .Acesso em 16 de setembro de 2020

CGI.br/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), Pesquisa sobre o uso da Internet no Brasil durante a pandemia do novo coronavírus - Painel TIC COVID-19 - Edição 2. Disponível em: https://cgi.br/noticia/releases/painel-tic-covid-19-apresenta-dados-ineditos-sobre-acesso-a-servicos-publicos-on-line-e-desafios-a-privacidade-durante-a-pandemia/ . Acesso em 01 de agosto de 2020

CAVALCANTE FILHO, João Trindade. **Teoria Geral dos Direitos Fundamentais.** Repositório do Supremo Tribunal Federal, Brasília. Disponível

em <http://www.stf.jus.br/repositorio/cms/portalTvJustica/portalTvJusticaNoticia/anexo/Joao_Trindadade Teoria_Geral_dos_direitos_fundamentais.pdf>. Acesso em 15 de setembro de 2020

CASTRO, Catarina Sarmento e. Direito da informática, privacidade e dados pessoais. Coimbra: Edições Almedina, 2005. p. 70-88

COMO funciona a espionagem. Super Interessante. São Paulo, edição 389, página 28, junho de 2018.

COSTA JÚNIOR, Paulo José da. O direito de estar só: tutela penal da intimidade. São Paulo:Revista dos Tribunais, 1970.

DONEDA, Danilo. A proteção de dados pessoas como direito fundamental. Revista Espaço Jurídico 12/103, Joacaba: Unose, 2011, p. 103

INFORMAÇÕES sobre o tráfego global de dados. O Cisco Visual Networking Index,2014. Disponível em: http://www.cisco.com/c/en/us/solutions/service-provider/vni-service-adoption- . Acesso em: 23 de setembro de 2020

GODOY, Cláudio Luiz Bueno. A liberdade de imprensa e os direitos da personalidade. São Paulo: Atlas, 2001.

MARTINS, Guilherme Magalhães (Coord.). Direito privado e internet: atualizado pela Lei 12.965/2014 (Marco Civil da Internet no Brasil). São Paulo: Atlas, 2014

MARMELSTEIN, George. Curso de Direitos Fundamentais. São Paulo: Atlas, 2008.

MENDES, Gilmar. Os Direitos Fundamentais e seus múltiplos significados na ordem Constitucional. Revista Diálogo Jurídico. Salvador, Bahia, janeiro de 2002. Disponível em <http://staticsp.atualidadesdodireito.com.br/marcelonovelino/files/2012/04/Direitos-fundamentaisM%C3%BAltiplos-significados-GILMAR-MENDES.pdf>. Acesso em 20 de setembro de 2020

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direito Humanos. UNIC/RIO/005. Janeiro de 2009. Disponível em <https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf>. Acesso em 15 de setembro de 2020

PECES-BARBA, Gregório et alli. Derechos positivo de los derechos humanos. Madrid: Debate, 1998.

PERES LUÑO, António. Derechos Humanos, Estado de Derecho y Constitución. 5ª Ed., Madrid: Tecnos, 1995.

Revista Fórum de Direito na Economia Digital | Belo Horizonte, ano 3, n. 04, p. 79-98, jan./jun. 2019

SILVA, José Afonso. Curso de Direito Constitucional positivo. 25. ed. São Paulo: Malheiros Editores, 2005. p. 178.

USO da internet no Brasil cresce de 40% a 50% durante a pandemia. O Globo, 11 de julho de 2020. Disponível em: <https://gazetaweb.globo.com/portal/noticia/2020/06/_107633.php>. Acesso em: 15 de setembro de 2020.