



DEPARTAMENTO DE DIREITO
MESTRADO EM DIREITO
ESPECIALIDADE EM CIÊNCIAS JURÍDICAS
UNIVERSIDADE AUTÓNOMA DE LISBOA
“LUÍS DE CAMÕES”

**RESPONSABILIDADE CIVIL POR VIOLAÇÃO DE DADOS PESSOAIS:
DESAFIO DA SOCIEDADE INFORMACIONAL NO CIBERESPAÇO**

Dissertação para a obtenção do grau de Mestre em Direito

Autora: Lidia Maria Leal Ferreira da Cruz

Orientador: Prof. Dr. Ricardo Dinis Pedro

Número da candidata: 2015.0265

Junho de 2019

Lisboa

DEDICATÓRIA

Dedico esse trabalho a André Luiz Ildefonso Colares, (*in memoriam*), meu cunhado, que sem o seu incentivo e insistência não teria concluído. Suas palavras cheias de entusiasmo, de certeza e de confiabilidade, me levaram a trilhar esse caminho e ter chegado ao destino. Mesmo não estando mais presente, só tenho a lhe dizer: Muito Obrigada! por ter acreditado, e ter sempre me incluído em sua vida.!

AGRADECIMENTOS

Aos meus pais (*in memoriam*), minha irmã, Maria Manuela Ferreira da Cruz, em especial aos meus sobrinhos Nicolas Ferreira Colares e Oscar Vicente Ferreira Colares que estão sempre presentes nessa jornada diária de grandes batalhas e dificuldades, mas sempre com foco na conquista e na vitória.

Ao eterno amigo, Alexandre Callmann, amigo de todas as horas, sempre com uma palavra amiga e incentivadora, até nos momentos difíceis nessa viagem da vida.

Ao meu orientador, Professor Doutor Ricardo Dinis Pedro que muito ajudou e enriqueceu com suas observações sempre relevantes.

RESUMO

O presente trabalho visa analisar o cenário da globalização com toda a carga de evolução tecnológica no domínio da comunicação interpessoal, que de certa forma, vem possibilitando a desedificação ou até mesmo o extermínio da privacidade das pessoas através da violação de seus dados pessoais sem precedentes e em larga escala. O que necessariamente num futuro causará danos graves e irreversíveis nas pessoas. A privacidade está em grande perigo se não forem tomadas as medidas legais necessárias para que as pessoas tenham os seus dados pessoais preservados, podendo exercer de forma livre o exercício à autodeterminação informativa. O consentimento é assim considerado o baluarte da proteção de dados pessoais e a sua livre circulação como forma de empoderar o titular dos dados pessoais. A legislação sobre dados pessoais engrandeceu quando adjetivou o consentimento, devendo ser ele livre, informado, inequívoco, explícito e/ou específico. O consentimento não deve ultrapassar os limites relativos à sua finalidade. As informações postas na internet são vertiginosamente propagadas alcançando de forma imediata, em tempo real, milhões de pessoas no mundo inteiro. A internet não esquece, pelo contrário traz à memória fatos do passado que muitas vezes queremos esquecer. Nessa rota, o surgimento do exercício do direito ao esquecimento é uma forma de resguardar e respeitar a liberdade e o direito à privacidade e intimidade conforme a sua autodeterminação. Na seara do ciberespaço, não se pode obliterar o princípio da Responsabilidade Civil, positivado no Regulamento Geral de Proteção de Dados em vigor na União Europeia e na Lei 13.709/2018 no Brasil que, se vê frente aos novos anseios de uma população digital no surgimento de uma nova sociedade de risco com vista à preservação e manutenção dos Direitos à Proteção dos dados pessoais.

PALAVRAS-CHAVE: Privacidade; violação de dados pessoais; autodeterminação informativa; direito ao esquecimento.

ABSTRACT

What is so interesting about this subject is that it is not only a great challenge for the people who work with the Law, but also for every citizen that uses the internet on a computer, a tablet or a smartphone. We are living in a globalized world, in a society bombarded by information because of the huge technological advancements in the communication domain. Due to these advancements, there have been several violations or even complete eradication of people's private lives through unprecedented web breaches which will most certainly create generate gravely big and irreversible damages to these persons. Privacy is being vandalized as a result of the wildness in which information is spread in nowadays virtual world and reaches millions of people on the web. Because of the increasingly large number of people seeking to communicate with one another, farther apart and at a faster pace, sharing information, fueling the search engines with their personal data. Therefore, data protection is a fundamental right of everyone and is being taken into consideration in all the five continents of the globe. The world is uneasy, on edge, looking for ways to minimize this large-scale data violation. The search engines redirect everything that is published on the internet with no restriction whatsoever, making it impossible to escape this virtual index. Living in a cyberworld era does not mean civil responsibility regarding personal data violation shall be annihilated. On the contrary, it is a path we can ensure legal security to the owners of that data so that it can be handled by the status of the general regulation on data protection. Against the renewed desires of a digital population in an in-risk society, aiming to preserve and keep the rights to protect personal data.

KEYWORDS: privacy; personal data violation; informative self-determination; civil responsibility.

SUMÁRIO

INTRODUÇÃO	7
CAPÍTULO I	18
1 PRIVACIDADE NO CIBERESPAÇO – UM DOS MAIORES DESAFIOS NA ERA DIGITAL	18
1.1 Cenário da privacidade	24
1.2 Privacidade um dos maiores problemas na era digital: internet ameaça o direito à privacidade da civilização humana?	33
CAPÍTULO II	38
2 DIREITO À PROTEÇÃO DE DADOS PESSOAIS	38
2.1 Antecedentes e evolução da legislação de proteção de dados pessoais	39
2.2 Os pilares das normas de proteção de dados pessoais	53
2.2.1 Dados pessoais	54
2.2.2 Anonimização e pseudonimização de dados	57
2.2.3 Consentimento - o baluarte da proteção de dados pessoais como forma de empoderar o titular dos dados pessoais	59
2.3 A proteção de dados pessoais no Brasil e na América Latina	62
2.3.1 A influência do marco civil da internet nos países da Itália e França	70
2.3.2 Lei 13.709/2018 – Lei de proteção de dados pessoais no Brasil	72
CAPÍTULO III	76
3 DATA BREACH - VIOLAÇÃO DE DADOS PESSOAIS	76
3.1 Um panorama na Europa e na América do Sul	76
3.2 Direito ao esquecimento	85
3.2.1 Limitações ao exercício do direito ao esquecimento digital	99
3.2.1.1 <i>Liberdade de expressão e liberdade de informação</i>	101
3.2.1.2 <i>Interesse Público</i>	104
3.2.1.3 <i>Memória histórica</i>	105
3.2.1.4 <i>Atuação do próprio titular</i>	106
CAPÍTULO IV	109
4 RESPONSABILIDADE CIVIL POR VIOLAÇÃO DE DADOS PESSOAIS A LUZ DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS	109
4.1 A responsabilidade pelos operadores dos motores de busca na qualidade de responsáveis pelo tratamento de dados	123
CONCLUSÃO	129
REFERÊNCIAS	136

INTRODUÇÃO

“A multidão não é mais solitária e anônima: está nua”

Stefano Rodotá

Violação de dados!!!! O que são dados? O que isso tem a ver com as pessoas que surfam nas ondas da internet? Como meus dados foram violados se estou de posse dos meus documentos pessoais e só eu detenho o poder das informações a meu respeito? Precisamos nos preocupar? As pessoas têm a real noção do perigo da utilização dos dados pessoais sem o consentimento do titular? A quem devo recorrer se meus dados forem violados? O ciberespaço, vem propiciando um cenário onde o direito à privacidade vem sendo aniquilado? Onde o controle dos dados pessoais vem sendo subtraídos das mãos dos cidadãos sem que os mesmos percebam. A privacidade vem sendo vulgarizada em virtude da fugacidade em que as informações circulam e atingem a bilhões de pessoas na rede em todo o mundo virtual, em virtude de que cada vez mais cresce a possibilidade dos homens comunicarem-se uns com os outros, em tempo mais rápido e lugares distantes? O exercício do direito ao esquecimento é sólido e eficaz no caso de violação dos dados pessoais?

Essas indagações são pertinentes na sociedade informacional que estamos vivendo. É incontestável que não podemos fugir ao avanço tecnológico galopante, mas também não podemos ignorar o forte impacto na vida das pessoas, que passaram a ser vigiadas, observadas, onde a privacidade, direito fundamental da personalidade, que diz respeito a uma pessoa, vem tendo publicidade em larga escala e sem precedentes, o mais perturbador é frente a improbabilidade de controlarmos os efeitos da tecnologia. E ao utilizarmos as redes sociais, ou até mesmo diversos aplicativos nos desnudamos, exibimos aos quatro cantos do mundo nossos interesses, nossas opiniões, fazendo com que nosso perfil seja construído e facilmente arremessado na rede em questões de milésimos de segundo. Estamos trilhando um caminho que não existe a possibilidade de retorno, ao revés, a mão é única e a tecnologia evolui a passos largos.

Existem hoje no mundo entre 2005 e 2018 3,9 bilhões de internautas, utilizadores da Internet, que correspondem a 47% da população mundial, estimada em 7,6 bilhões¹. A taxa de penetração global on-line é de 57 por cento, com a América do Norte e norte da Europa, ficando

¹ TRACTO - **Number of internet users worldwide from 2005 to 2018 (in millions)**. [Em Linha]. [Consult. 23 maio 2019]. Disponível em WWW: <URL:<https://www.tracto.com.br/quantas-pessoas-tem-acesso-a-internet-no-mundo/>>.

em primeiro lugar com uma taxa de penetração da Internet de 95 por cento entre a população², isto quer dizer que o acesso à internet é um direito do cidadão, positivado na legislação, onde a suspensão do acesso é considerada uma violação do direito do usuário.

Nessa senda a violação de dados pessoais é um fato real, é um desafio da sociedade informacional atual para preservar a vida privada e a liberdade das pessoas envolvidas. Em contrapartida, pode-se lançar mão do exercício do direito ao esquecimento, incluído nos direitos da personalidade como uma forma de resguardar a privacidade e intimidade dos usuários da famosa rede de internet.

Como conter o avanço dessas questões que estão no cotidiano da maior parte das pessoas que ouvem diariamente através das diferentes mídias no universo, notícias³ tais como:

Facebook deu acesso a mensagens privadas de usuários a Netflix e Spotify; Banco Inter vai pagar R\$ 1,5 milhão por vazamento de dados de clientes (19 dez 2018-07h31); Falha no Facebook permitiu vazamento de fotos de 6,8 milhões usuários – (14 dez 2018 - 17h25); Zuckerberg apoiou compartilhamento de dados de usuários do Facebook – (6 dez 2018- 14h37); Facebook forneceu dados de usuários a fabricantes de celulares – (14 nov 2018 -16h11); Ministério Público abre investigação sobre vazamento de dados da Stone (7 nov 2018-17h58) [dentre outras]

Devemos nos preocupar sim! A proteção de dados pessoais está na pauta do dia! “A proteção de dados pessoais tem implicações que vão além da possibilidade de um estrito controle individual”, como muito bem acentua Danilo Doneda⁴.

Os nossos dados pessoais integram a nossa personalidade e afetam diretamente a nossa privacidade, a nossa intimidade e liberdade pessoal, e por essa razão devem ser protegidos através de direitos positivados em normas jurídicas. Temos a liberdade de expressão, garantida constitucionalmente em diversos países ao redor do mundo, mas, no entanto, essa liberdade deverá ser exercida nos estritos limites da responsabilidade. A pessoa tem o direito de exercer a autodeterminação informativa dispondo do seu conteúdo privado da forma como lhe aprouver, exceto nos casos em haja interesse público, onde a supremacia do direito público se sobrepõe a do direito privado. Não se pode tirar da pessoa o controle de seus dados pessoais. Na grande maioria dos casos os dados e as imagens das pessoas são utilizados na rede sem que as mesmas

² TRACTO - **Number of internet users worldwide from 2005 to 2018 (in millions)**. [Em Linha]. [Consult. 23 maio 2019]. Disponível em WWW: <URL:<https://www.tracto.com.br/quantas-pessoas-tem-acesso-a-internet-no-mundo/>>.

³ VEJA. **Vazamento de dados** [Em linha]. [Consult. 10 abr. 2019]. Disponível em WWW: <URL:<https://veja.abril.com.br/noticias-sobre/vazamento-de-dados/>>.

⁴ DONEDA, Danilo Cesar Maganhoto - **Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade**. [Em linha]. [Consult. 15 fev. 2018]. Disponível em WWW: <URL:<http://www.egov.ufsc.br/portal/sites/default/files/anexos/8196-8195-1-PB.htm>>.

tenham conhecimento. Só são sabedoras quando o dano já está feito, quando direitos fundamentais são lesionados.

Nesse contexto, dissertaremos, à luz da doutrina clássica, numa breve revisão bibliográfica, sobre os temas privacidade, dados pessoais, violação de dados e responsabilidade civil, dentro de um contexto inicialmente teórico, relacionando aspectos fundamentais para o entendimento da importância da proteção de dados pessoais dos cidadãos, com vistas a propiciar segurança jurídica através de ferramentas diversas evitando possíveis danos irreparáveis a direitos personalíssimos das pessoas. O processo de globalização é inevitável, com toda a carga de evolução tecnológica no domínio da comunicação interpessoal, que de certa forma, vem possibilitando a vulgarização ou até mesmo o extermínio da privacidade das pessoas através da violação de dados pessoais e transferindo-os a terceiros sem o consentimento dos titulares dos dados. O que necessariamente num futuro causará danos graves e irreversíveis as pessoas. A privacidade está em grande perigo se não forem tomadas as medidas legais necessárias para que as pessoas tenham seus dados pessoais preservados, podendo dispor da forma como lhe aprouver.

A sociedade moderna vem sofrendo alterações significativas em diferentes aspectos, não podendo mais desprezar que estamos diante do mundo globalizado, onde a informação chega quase que instantânea sem qualquer barreira territorial, nos mais distantes lugares do mundo. Entretanto, é bem verdade, que todo o desenvolvimento acarreta consequências positivas e negativas para a população.

No caso em tela, o surgimento da INTERNET, onde o seu principal traço presumia-se o anonimato, revolucionou o mundo, e a reboque trouxe no seu bojo problemas que estão colocando em xeque direitos fundamentais, até então tidos como impenetráveis e indestrutíveis. Estamos vivenciando momentos de impasse, onde frequentemente nos deparamos com colisão de princípios onde sempre temos de um lado, o direito à informação, a liberdade e até interesses públicos e de outro a violação de direitos da personalidade. A busca da informação precisa e rápida é fundamental para o desenvolvimento de um país e para a garantia do Estado democrático de direito. Um país democrático mede-se pelo volume de informação, pelo seu valor e principalmente pelo número de pessoas atingidas.

Globalização também não é um fenômeno novo. Ele já estava presente, por exemplo, nos antigos impérios, provocando sucessivos surtos de modernização econômica, cultural e

jurídica. “A globalização está longe de ser um conceito original ou inédito na história, na sociologia política, na teoria econômica ou mesmo na ciência do direito”⁵.

É nesse contexto que desponta o direito a proteção de dados pessoais, uma faceta do direito dos direitos fundamentais, em especial o direito da personalidade, uma vez que o ciberespaço, assim é considerado um admirável mundo novo, onde reina a liberdade, mas em contrapartida mister se faz harmonizar o direito à privacidade e à intimidade que vem, neste ambiente, sendo violado em grande escala. A internet, sem dúvida traz em seu bojo o poder de transformar a sociedade criando novos paradigmas em relação ao processamento das informações e comunicação entre as pessoas e a superexposição. A internet pode ser acessada não só pelo computador, mas também pelos smartphones, que possibilita as pessoas criarem seus grupos por afinidades ou simplesmente pelo simples prazer de criar comunidades de amigos, família etc.

O cenário que se desponta é de uma sociedade informacional, onde o acesso à informação ficou facilitado, pois basta um simples click e a informação referente a pessoas, coisas e, lugares surge. Até mesmo fatos passados ressurgem passando a existir no mundo virtual, onde é quase impossível deter o anonimato.

Em função do crescimento acelerado da tecnologia, tem-se visto uma redução de custos para possibilitar o acesso de todos à internet, e a reboque, como consequência da socialização sem precedentes, de forma incontrolável se tem o espargimento dos dados das pessoas nas redes, nos motores de busca, dados esses manipulados por terceiros desconhecidos, podendo vir a atingir direitos da personalidade como a privacidade e a intimidade.

Ainda, não se pode mensurar com exatidão a extensão dos danos à privacidade e intimidade de uma pessoa por não dispormos de meios de controlar o abarcamento de determinada informação contida no ciberespaço.

Nessa conjuntura não pode ficar relegado a segundo plano a Responsabilidade Civil na internet, por violação de dados pessoais, por ser inevitável uma vez que o número de atos ilícitos cometidos na rede é elevado. Os dados pessoais dos cidadãos circulam nos motores de busca do gigante Google e outros, sem o consentimento dos titulares. A Responsabilidade Civil vem alcançando grandes voos na perspectiva de sempre indenizar a vítima recompondo-a ao seu estado anterior à prática do ato ilícito, *restitutio in integrum*.

A personalidade é inerente ao ser humano e é em decorrência dessa concepção que germina o Direito. “Não há Direito sem pessoas, sem pessoas humanas, de corpo material, com

⁵ FARIA, José Eduardo *apud* MINHOTO, Antonio Celso Baeta – **Globalização e Direito: o Impacto da Ordem Mundial Global sobre o Direito**. São Paulo: Juarez de Oliveira, 2004. ISBN 85-7453-460-9, p. 15.

amor e ódio, alegria e tristeza, prazer e dor, bondade e maldade, solidez e fragilidade, concepção e morte. São elas o fundamento ontológico do Direito. Seria impossível que o Direito não se ocupasse delas”⁶.

De igual forma, temos a consciência de que no mundo virtual essa garantia plena da privacidade e de que o uso dos dados pessoais sem consentimento dos titulares ocasionando a violação de dados incomensurável é um grande desafio, na medida em que, vivemos numa sociedade informacional, ao acessarmos nossos computadores, smartphones através de diversos aplicativos que nos são exigidos nos dias de hoje, deixamos rastros em todos os lugares. O caminho da informação não é retilíneo, ela passa por diversos caminhos tortuosos, e, em cada percurso nossos vestígios, nossas marcas, ficam agarradas, como se fosse uma tatuagem difícil, ou quase impossível de ser removida. Por esse motivo, ao apagar uma informação num determinado site não significa dizer que estará apagada, já que a informação perpassa por diversos canais, fazendo-se necessário a desindexação de informações, de dados e de imagens, o que pode se dizer que é quase impossível apagar a informação relevante ou não, na origem.

Paulo Silva Fernandes⁷ citando Milan Kundera nos revela que “no reverso da medalha encontramos o facto – para muitos aterrador – de estarmos privados, hoje como nunca, da nossa privacidade, já que parece já ninguém poder “esconder-se em parte nenhuma e que cada um está à mercê dos outros”, principalmente após os acontecimentos de 11 de setembro, uma nova realidade despontou no horizonte, onde e a população de alguns países, em especial a Grã Bretanha, que é (considerado o país mais bem monitorado do mundo), os movimentos das pessoas, hábitos, os locais públicos, as ruas e etc. estão constantemente vigiados. Falamos assim, de uma sociedade de vigilância onde atualmente ninguém mais está escondido ou poderá agir no anonimato.

A Internet encurtou distâncias, podemos estar em diversos lugares ao mesmo tempo interagindo com diversos segmentos da sociedade, empresas públicas e privadas, o acesso à todo tipo de informação não encontra barreiras, desencadeando também uma série de indagações relacionadas com um dos direito fundamental que é a privacidade, que dá a pessoa o direito de expor fatos, de contar o que quiser.

Não podemos falar da responsabilidade civil pela violação de dados pessoais sem primeiro entendermos o conceito de dados pessoais, os pilares de sustentação das normas de

⁶ VASCONCELOS, Pedro Pais – **Direitos da Personalidade**. Coimbra: Almedina, 2006, ISBN: 9789724029948, p. 47.

⁷ KUNDERA, Milan *apud* FERNANDES, Paulo Silva - **Globalização, “Sociedade de Risco” e o Futuro do Direito Penal**. São Paulo: Almedina, 2001. ISBN 978-9724015408, p. 38.

proteção aos dados pessoais em especial o consentimento, o pilar fundamental da proteção de dados pessoais e em seguida mergulhar no instituto da privacidade, onde podemos dizer que este nasceu a partir do “direito de ser deixado só”, moldado pelo Juiz Thomas Cooley, e que até os dias de hoje é memorável, um marco no instituto da privacidade, seguido da publicação em 1890 do artigo intitulado *The Right to Privacy*, de Samuel Warren e Louis Brandeis.

Nessa linha abordaremos no primeiro capítulo, privacidade no ciberespaço, dois tipos de direitos da personalidade: o direito à privacidade e à intimidade, direitos esses que, reconhecidamente vem sendo banalizados na nova sociedade virtual, no ciberespaço, em função da ampla e irrestrita liberdade, por parte de seus usuários, ao disponibilizar, fotos, conversas, vídeos, o que fazem no seu dia a dia, para um mundo de pessoas que estão conectadas 24 horas por dia em qualquer lugar do mundo, podendo colocar em riscos direitos tutelados pela ordem jurídica.

Explorando o cenário da privacidade a partir do conceito de privacidade e intimidade por parte de grandes e renomados doutrinadores, fluindo na positivação dos direitos da personalidade e intimidade nas diferentes legislações pátrias na Europa e no Brasil. Trataremos da teoria dos Círculos Concêntricos da esfera da vida privada, na Alemanha de 1957, que visa diferenciar intimidade e vida privada. Em seguida, o direito à privacidade sobre a ótica digital, uma das questões que tem sido pauta nas mídias sociais, já que no mundo virtual não existe mais limites, tempo, onde a rede de computadores mudou significativamente a vida de todos os cidadãos.

O capítulo dois, intitulado direito à proteção de dados pessoais é de vital importância para a garantia do direito fundamental a privacidade. Hoje, todos, sem exceção podem ter acesso a qualquer informação contida nos bancos de dados no ciberespaço. Estamos diante de um novo cenário, o cibernético: Milhares de pessoas, nos mais diversos lugares do planeta, conectadas à internet, através da rede mundial de computadores, aparelhos celulares de ponta, os smartphones, possibilitando essa conexão em tempo real, através de diferentes formas tais como sites, facebook, blogs, Instagram, snapchat, Twiter, e-mails e etc.

Evidenciaremos os antecedentes e a evolução da legislação de proteção de dados de forma a construirmos o entendimento do significado de proteção de dados pessoais bem como a sua vital importância para a edificação do princípio basilar das sociedades democráticas, a dignidade da pessoa humana.

A expressão ciberespaço foi primeiro utilizada por William Gibson no seu romance seminal, *Neuromancer*, de 1986⁸. O autor criou-a a partir de uma combinação da raiz grega *Cyber*, que significa “controlo” e da palavra inglesa *space*, significado “espaço”. Com este termo pretendeu o autor designar um mundo virtual, uma dimensão fechada e controlada, por oposição ao nosso mundo aberto e infinito. O ciberespaço assenta, pois, numa complexa e luxuriante natureza artificial que o permite e possibilita enquanto verdadeiro ecossistema virtual.

Nessa aldeia global, verificamos que estamos operando num cosmo sem restrições, onde seus usuários são livres para navegar e postar o que bem entender, já que é um mundo sem regras, sem controlo, onde o futuro da humanidade corre riscos sem direitos tutelados no ciberespaço.

Como muito bem salientou Farinho⁹ em sua respeitável obra, “o potencial de lesão do ciberespaço é o mais elevado possível de entre todos os cenários, quer pelo número de destinatários a que pode chegar quer pela dificuldade em localizar a fonte do dano”. Deste modo a divulgação de informações relativas à vida privada dos indivíduos, na internet, ganha particular relevo, pois não só a exposição da vida íntima se encontra potenciada quanto aos destinatários, mas também se encontra disperso o meio através do qual a informação é difundida.

E nessa quadra, temos as redes sociais, tais como Facebook, Instagram, snapchat, e-mails, sites, blogs, Youtube etc., inclusive com acesso nos smartphones. São veículos de grande eficácia para a propagação sem limites de intimidades de seus usuários, que diariamente ou a cada minuto divulgam nas redes, a sua rotina do dia a dia, de seus familiares e amigos, suas fotos, vídeos, passeios, enfim, toda a sua vida é, a cada minuto, desnudada para o ciberespaço, é uma superexposição sem limites.

Cabe aqui aduzir, segundo Paesani¹⁰, a internet não pertence a ninguém, não é financiada por instituições, governos ou organizações internacionais, e também não é um serviço comercial, tendo sido programada para funcionar e distribuir informações de forma ilimitada. Aduz ainda que a explosão da internet determinou uma transformação qualitativa e quantitativa

⁸ FARINHO, Domingos Soares – **Intimidade da Vida Privada e Media no Ciberespaço**. Coimbra: Almedina, 2006, ISBN: 9789724027401, p. 13-4.

⁹ *Idem* – **Op. Cit.** p. 70-71.

¹⁰ PAESANI, Liliana Minardi – **Direito e Internet: Liberdade de Informação, privacidade e Responsabilidade Civil**. São Paulo: Atlas, 2013. ISBN 978-85-224-7891-0, p. 20.

das informações e a possibilidade de comunicação imediata criou um novo domínio social do indivíduo: o poder informático¹¹.

Nessa linha é importante sublinhar que o acesso à internet não está mais limitado aos faustos, mas até mesmo às pessoas de classe menos favorecidas, Hoje qualquer pessoa, independente de classe social ou idade, tem acesso à internet, não só através de computadores, mas por meio da telefonia celular e das redes de wi-fi, que democratizaram o livre acesso à internet, a qualquer hora e em qualquer lugar bem como a quantidade de informação que circula no mundo virtual.

Daremos destaques aos pilares das normas de proteção de dados: dados pessoais, anonimização e pseudonimização de dados pessoais e o consentimento tido como fundamental para garantir ao titular dos dados pessoais o completo domínio de suas informações.

Desenvolveremos a legislação de proteção de dados no Brasil e na América do Sul de forma concisa, dando destaque ao Marco da Civil da Internet e sua influência na Legislação da França e Itália e a Lei 13.709/18, sancionada em 14 de agosto de 2018 alterada pela medida provisória 869 de 27 de dezembro de 2018 que finalmente positivará e consagrará o direito a proteção de dados pessoais no Brasil. Em relação ao velho mundo, o Brasil retardou a implementação de uma legislação específica diferente de alguns países da América do Sul como Chile e Argentina. Mesmo assim, desaguarão no Judiciário vários e polêmicos casos envolvendo o direito a proteção de dados se contrapondo a outros preceitos amparados constitucionalmente, onde os Tribunais Superiores lançaram mão das técnicas de ponderação de valores com vistas a conciliar interesses e direitos fundamentais.

O capítulo três versa sobre *Data Breach* - violação de dados pessoais propriamente dita, num passeio pela Europa e América do Sul, relatando algumas notícias nas grandes mídias sobre a violação de dados de milhares de pessoas ao redor do mundo. Partindo daí entraremos na seara do Direito ao Esquecimento como um meio de possibilitar ao titular dos dados pessoais de ver eliminada as informações que lhe causem dor, tristeza, angústia e sofrimento em alguma fase de sua vida. É uma questão de valorizar e respeitar a dignidade da pessoa humana, não se podendo eternizar informações sobre os indivíduos, ainda que verdadeiras, mas que possam vir a trazer lembranças dolorosas e sofrimentos. A pessoa tem o direito de esquecer fato ocorridos no passado. Ninguém pode ser obrigado a conviver com fatos que a época fora desabonadores e até de interesse público, caso contrário estaríamos condenando-o para todo o sempre.

¹¹ PAESANI, Liliana Minardi – **Direito e Internet: Liberdade de Informação, privacidade e Responsabilidade Civil**. São Paulo: Atlas, 2013. ISBN 978-85-224-7891-0, p. 20.

Como já foi dito anteriormente, os danos causados em função da violação de dados pessoais no ciberespaço são imensuráveis devido a sua incalculável extensão, mas de todo o modo, a vítima tem o direito ao esquecimento. Ou seja, é uma prerrogativa do usuário, um direito inalienável e primordial àquele que se sentiu lesado, independentemente de qualquer ação dos provedores de internet.

A aplicação do direito ao esquecimento não é absoluta, requerendo pelo aplicador da lei, que seja feito um juízo de ponderação de valores em cada caso concreto, pois nem sempre prevalecerá o direito ao esquecimento. Limites ao direito do esquecimento são firmados em virtude da existência de outros direitos da personalidade que merecem de igual forma a tutela jurídica. Nesse contexto mister se faz analisar caso a caso a fim de delimitar o direito que se evidencia. Assim não é qualquer informação que seria eliminada do mundo virtual ou de veículos de informação e motores de busca. Há que se ponderar primeiro se não há naquele fato de que se busca o esquecimento pelo particular interessado, o direito à memória de todo um povo¹².

Evidenciaremos um *leading case* famoso que eclodiu o debate sobre o direito ao esquecimento envolvendo a Google Spain Sl, Agência Espanhola de Proteção de Dados e o cidadão espanhol Mario Costeja González. No Brasil, o famoso caso da Chacina da Candelária e a Rede Globo no programa Linha Direta se contrapondo ao caso Aída Curi.

Os cidadãos digitais, sem qualquer preocupação, de forma voluntária, oferecem seus dados pessoais aos gigantes da internet, quando, publicam suas intimidades abrindo mão de sua privacidade, sem qualquer embaraço, esquecendo-se de que tudo que é visualizado no famoso “Face”, que nada tem de privado, e sim torna-se público instantaneamente, já que aquele que postou não exerce mais nenhum controle sobre a propagação e multiplicação dos dados ali inseridos. Mesmo que a pessoa tenha o direito a que a informação seja retirada, o dano já está consumado, uma vez que é inexequível mensurar quantos computadores e quantas pessoas já armazenaram as informações ora editadas no Facebook e outras plataformas digitais bem como que destino terão tais informações.

Francisco Rui Cádima¹³, em seu artigo sobre o tema Facebook, leciona que “desde início, o Facebook sempre defendeu, nomeadamente através do próprio Mark Zuckerberg,

¹² CONSALTER, Zilda Mara – **Direito ao Esquecimento**. Curitiba: Juruá, 2017. ISBN 978-85-362-6485-11, p. 312.

¹³ CÁDIMA, Francisco Ruy – **O Facebook, as redes sociais e o direito ao esquecimento**. [Em linha]. [Consult. 03 out. 2015]. Disponível em WWW: <URL:http://www.researchgate.net/publication/277556597_O_Facebook_as_redes_sociais_e_o_direito_ao_esquecimento>.

criador do Facebook, uma quase “não-política” de privacidade, deixando que os dados fossem colocados praticamente sem restrições, não respeitando ciclicamente o domínio dos direitos de reserva, onde os argumentos invocados eram absolutamente simplistas, isto é, se um membro se inscrevia na rede e colocava determinada informação *online* não era certamente para se esconder”.

Observando e analisando o que Richard Allan, responsável Europeu para questões relacionadas à privacidade, disse que “os membros da rede estariam mais preocupados na permanência dos seus dados no Facebook do que na sua eliminação”¹⁴, nos remete a aquiescer com a sua fala na medida em que, constatamos que o ciberespaço é um admirável mundo novo, onde os internautas estão simplesmente deslumbrados com a possibilidade de navegar por caminhos nunca antes navegados, visitar lugares que nunca pensaram em estar, sem qualquer preocupação, e sem qualquer repressão. E, em contrapartida, essa sedução que a internet propicia acaba promovendo a banalização do direito à privacidade e à intimidade, já que os usuários das redes sociais estão perdendo o foco de salvaguardar seus direitos e garantias.

Meditando sobre o tema, a internet tem como prumo a liberdade total logo, o anonimato só poderá ser desvendado através de uma ordem judicial caso a pessoa se sinta lesada, caso contrário, estaria na contramão dos princípios do mundo virtual, qual seja a garantia da liberdade e anonimato.

Por último, enfrentaremos a responsabilidade civil por violação de dados a luz do Regulamento geral de Proteção de Dados da União Europeia. Trilhando esse caminho, a obediência ao princípio da Responsabilidade Civil, deve estar sempre presente, ainda que no mundo virtual. Não é porque a internet é uma “terra ainda sem lei”, onde reina a liberdade e o anonimato, que seus usuários, internautas não estejam sujeitos a obedecer ao princípio basilar de não lesar ninguém, *neminem laedere*. A Responsabilidade Civil não é aniquilada pelo simples fato de estarmos na era do mundo virtual. Ao revés, ela acompanha na mesma proporção, a evolução científica e tecnológica. Exploraremos a visão dualista da responsabilidade civil e os pressupostos mais problemáticos em matéria de violação de dados pessoais para gerar o dever de indenizar, com base no artigo 82 do Regulamento Europeu.

¹⁴ CÁDIMA, Francisco Ruy – **O Facebook, as redes sociais e o direito ao esquecimento**. [Em linha]. [Consult. 03 out. 2015]. Disponível em WWW: <URL:http://www.researchgate.net/publication/277556597_O_Facebook_as_redes_sociais_e_o_direito_ao_esquecimento>.

Verificamos que em que pese o ciberespaço ser uma realidade fática, ainda engatinhamos em relação às legislações específicas que estabeleçam as normas para quem faz uso no seu dia a dia da era digital.

O Código Civil Português, no nº 1 do artigo 483 trata dos pressupostos da Responsabilidade Civil: “Aquele que, com dolo ou mera culpa, violar ilicitamente o direito de outrem ou qualquer disposição legal destinada a proteger interesses alheios fica obrigado a indemnizar o lesado pelos danos resultantes da violação”.

Corroborando nesse sentido, Gonzalez¹⁵, simplifica expondo:

Numa sociedade caracterizada por alto grau de divisão de tarefas, por uma acentuada celeridade da própria forma de viver e por um domínio avassalador de tecnologia, há incontáveis riscos que lhe são inerentes e pelos quais não faz sentido imputar responsabilidade a alguém, por se considerar que se devem aceitar e, portanto, se deve assumir a possibilidade da respectiva concretização. Pelo que, ao contrário, só se pode imputar a alguém a responsabilidade por um dano causado a outrem quando este desenvolva uma conduta que envolva riscos que ultrapassem a fasquia do socialmente aceitável (ou seja, que vão para além dos riscos normais da vida).

Em que pese o ciberespaço ser considerado um mundo sem censura, não se pode desconsiderar o perigo que ronda os usuários da internet, pois que sua utilização pode suscitar a prática de atos ilegais e danosos impondo-se buscar a responsabilidade civil dos agentes causadores por violação de dados pessoais.

O surgimento da responsabilidade civil como corolário da violação de dados encontra-se positivado no artigo 82.º Regulamento Geral de Proteção de Dados onde sanciona o direito à vítima de receber uma indenização por parte do responsável pelo tratamento ou do subcontratante em casos de ter sofridos danos materiais e morais, da mesma forma, no Brasil temos positivado na Lei de Proteção de dados pessoais (LGPD) - Lei 13.709/2018 na seção III do artigo 42 da responsabilidade e do ressarcimento de danos.

Para concluir, não se perde tempo, mas ao contrário se enriquece com as palavras sábias de Antônio Celso Baeta Minhoto¹⁶ quando acertadamente diz que “a globalização é inevitável e que lutar contra isso é querer lutar contra o curso da história o que, em última análise, significaria perda de tempo, energia e exercício involuntário de obtusidade intelectual”.

¹⁵ GONZÁLES, José Alberto – **Responsabilidade Civil**. p. 84.

¹⁶ MINHOTO, Antonio Celso Baeta – **Globalização e Direito**: o Impacto da Ordem Mundial Global sobre o Direito. 2004. p. 23.

CAPÍTULO I

1 PRIVACIDADE NO CIBERESPAÇO – UM DOS MAIORES DESAFIOS NA ERA DIGITAL

A abordagem do tema privacidade, no século XXI, é hoje um assunto que deve ser amplamente debatido e discutido para que não se chegue ao ponto de falar que privacidade “é coisa do passado”, “privacidade não existe”. É de fácil constatação que o direito à privacidade, garantido nas principais constituições dos diversos países vem sendo ameaçado, principalmente com a chegada da internet, e das diversas tecnologias que encurtam distâncias e divulgam informações em questão de segundos nos mais distantes lugares desse mundo virtual, onde não temos como nos esconder.

Aliado a impetuosa evolução tecnológica, temos também, um movimento mundial, face aos acontecimentos do 11 de setembro, que quer queiramos ou não foram considerados um marco na história, no qual levantou-se a bandeira da vigilância permanente e sem precedentes a fim de possibilitar a segurança total dos cidadãos mediante a possibilidade de ataques terroristas. A vida privada das pessoas ao redor do mundo vem sendo monitorada, invadida, deixando a população sem qualquer conhecimento de que suas informações pessoais estão sendo coletadas, guardadas e até divulgadas ou vendidas, caracterizando-se a violação de dados pessoais, incluindo a instalação de câmeras de segurança que fazem reconhecimento facial em diversos locais.

Nesse contexto ao abordamos o tema violação de dados necessariamente temos que adentrar na seara da privacidade. Partiremos da definição de privacidade segundo José Afonso da Silva¹⁷, que elucida de forma clara e absoluta como “o conjunto de informação acerca do indivíduo, que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito”. Ou seja, a pessoa é a titular exclusiva de seus dados pessoais dispondo-os da forma que melhor lhe aprouver, anuindo de forma clara e transparente o tratamento de seus dados pessoais junto as organizações públicas ou privadas, exceto no tocante aos casos de ameaça à segurança nacional.

Não há como abordar o direito à privacidade sem se examinar o direito a intimidade face a conexão dos dois institutos, que agregam os direitos da personalidade. Decotado para o mundo digital, mister se faz um breve estudo, em que pese na doutrina levantarem alguns questionamentos sobre a integração deles, como se fossem um só. É costumeiro constatar

¹⁷ SILVA, Jose Afonso - **Curso de Direito Constitucional Positivo**. 26 ed. São Paulo: Malheiros, 2005, p. 206.

o emprego dos termos privacidade e intimidade como se sinônimos fossem. O conceito dos dois institutos é complexo devido à natureza subjetiva, sendo fortemente influenciada pela sociedade, que está sempre em transformação em virtude do avanço tecnológico.

Tem-se a intimidade diretamente ligada à pessoa. Sem intimidade não haveria pessoa, sujeito de direito. Portanto, o sujeito de direito tem seu mundo íntimo e o Direito protege-o, de maneira parecida como defende o nascituro, antes de nascer¹⁸.

O surgimento da rede Internet, por exemplo, decididamente alargou as possibilidades de comunicação e fez emergir um grande número de questões ligadas à privacidade. Danilo Doneda sustenta que “o impacto que esta rede representa, porém, estava em grande parte já incubado em outras tecnologias anteriores, que provocaram fenômenos em certa medida comparáveis e que, se hoje parecem pálidos, devem ser considerados em relação ao que representaram à sua época”¹⁹.

A complexidade em diferenciar intimidade e vida privada, restringe-se ao fato de cada pessoa de per si ter autonomia para conceber o que entende por intimidade e vida privada, estando diretamente ligada a sua conduta, vinculados a valores intrínsecos de cada indivíduo que está inserido na sociedade, sociedade essa com valores em constante mutação em função de novas exigências, em face do desenvolvimento tecnológico que passou a exigir novos padrões de comportamento, onde a distância e o relacionamento entre as pessoas ficou deveras facilitado. Nesse sentido, o conceito de privacidade e/ou intimidade pode variar de pessoa para pessoa. O que para uma pessoa pode ser resguardo, íntimo, segredo, para outra é irrelevante dar a saber a terceiros sobre sua vida privada, não tendo qualquer embaraço em fazê-lo. Daí a dificuldade de se definir com precisão privacidade, já que muitas vezes, o limiar do público e privado se confunde podendo ocasionar a violação da intimidade.

Ao contrário da intimidade *stricto sensu*, que se manifesta para o interior do indivíduo, a vida privada manifesta-se para o exterior, estando, pois, mais exposta e condicionada a regras (e costumes) de convivência social. Não obstante isso, o indivíduo segue com o poder de determinação do alcance de seu âmbito privado, o qual, frente a certas circunstâncias pode ver-se diminuído²⁰. A privacidade *stricto sensu*, está diretamente relacionada com fatos e atitudes que a pessoa não deseja que venha a público, devendo permanecer reservadas ao seu titular.

¹⁸ ALONSO, Felix Ruiz – Pessoa, intimidade e o direito à privacidade. *in*: MARTINS FILHO, Ives Gandra; MONTEIRO JUNIOR, Antônio Jorge (Coord.). **Direito à privacidade**. São Paulo: Centro de Extensão Universitário, 2005. ISBN 85-98239-36-4, p. 17.

¹⁹ DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006. ISBN 85-7147-562-8, p. 56.

²⁰ PEREIRA, Marcelo Cardoso - **Direito à Intimidade na Internet**. Curitiba: Juruá, 2011. ISBN 85-362-0516-4, p. 116.

A intimidade é o âmbito interior da pessoa mais profundo, mais recôndito, secreto ou escondido dentro dela, é algo inacessível, invisível, que só ela conhece, onde ela só elabora ou constrói livremente seu próprio agir e onde se processa sua vida interior. Na intimidade, a pessoa constrói-se e descobre-se a si própria²¹.

Marcelo Cardoso Pereira²² citando Bajon Fernández, entende a intimidade como uma esfera pessoal em que o indivíduo pode desenvolver-se como ser humano, livre de ataques e ingerências exteriores. Em outras palavras, vincula a intimidade a um âmbito pessoal no qual há a possibilidade de que o indivíduo desenvolva e fomenta sua personalidade.

E, ainda, aclarando os embates, Sônia Aguiar Vieira²³ explanou que “numa conceituação mais técnica, vida privada é o gênero do qual a intimidade é a espécie. A vida privada é a esfera que concentra outros valores, quais sejam: a intimidade e a esfera do segredo”. Continuando ainda, citando Pierre Jacomet, “a intimidade e a vida privada são valores em constante perigo. Vivem à borda de serem conspurcados de maneira iniludível e permanente”.²⁴

Ou seja, tem-se a privacidade numa amplitude maior, mais larga, onde a intimidade situa-se dentro dessa esfera mais ampla, sendo que numa dimensão bem menor, face as suas peculiaridades, que dizem respeito a esfera mais intrínseca da pessoa. Privacidade e intimidade estão intimamente conectadas, daí a grande dificuldade por parte dos doutrinadores, de distinguir e separá-las.

O direito à privacidade ou à intimidade nada mais é do que projeção da dignidade humana. Para ser digno, é necessário que o ser humano possa dispor, no âmbito da sua esfera individual, de um largo espaço em que prefira permanecer sozinho, sem a intromissão de terceiros. Esse reduto diz respeito à própria liberdade individual²⁵.

Enquanto existem divergências e dificuldade de conceituar o direito a intimidade e o direito à privacidade, o Brasil avançou e passou a conceber na Carta Magna e na legislação infraconstitucional a intimidade e a privacidade como direitos distintos, positivados e albergados na qualidade de direitos fundamentais elevados a garantias constitucionais.

A Constituição Federal do Brasil em seu artigo 5º inciso X²⁶, deferiu a mesma tutela à intimidade e à vida privada de sorte a atribuir integral proteção, considerando invioláveis a

²¹ ALONSO, Felix Ruiz – Pessoa, intimidade e o direito à privacidade *in*: MARTINS FILHO, Ives Gandra; MONTEIRO JUNIOR, Antônio Jorge (Coord.). **Direito à privacidade**. 2005. p. 17.

²² BAJO *apud* PEREIRA, Marcelo Cardoso - **Direito à Intimidade na Internet**. 2011. p. 112.

²³ VIEIRA, Sonia Aguiar do Amaral - **Inviolabilidade da Vida Privada e da Intimidade pelos Meios Eletrônicos**. São Paulo: Juarez de Oliveira, 2002. ISBN 85-7453-349-1, XV.

²⁴ *Idem- Op. Cit.* p. XVI.

²⁵ SANTOS, Antonio Jeová – **Dano Moral na Internet**. São Paulo: Metodo, 2001. ISBN 858645625X, p. 166.

²⁶ BRASIL. **Constituição da República Federativa do Brasil**, de 05 de outubro de 1988. [Em linha]. [Consult. 27 de abr. de 2019]. Disponível em WWW: <URL:http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.html>.

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.

De toda sorte, verifica-se que a Constituição Brasileira, tutelou os dois institutos de forma igualitária, valorizando-os como integrantes da personalidade da pessoa humana. Em que pese a intimidade estar num círculo menor, e abriga o direito ao segredo e a privacidade num círculo maior que engloba a intimidade, ambas receberam integral proteção constitucional.²⁷ Antonio Jeová Santos definiu intimidade como “ Nada mais íntimo que meu próprio pensamento, enquanto não é dado ao conhecimento de outra pessoa Intimidade são meus desejos, meus apetites e, em parte, podem ser minhas necessidades e até a maneira de satisfazê-las ²⁸.

A Constituição do Brasil ao abrigar a privacidade e intimidade de forma distintas, assim o fez no sentido de expandir a definição dos dois conceitos, já que considerou que a existência da vida humana compreende duas dimensões, uma externa e outra interna ²⁹.

A vida exterior, que envolve a pessoa nas relações sociais e nas atividades públicas, pode ser objeto das pesquisas e das divulgações de terceiros, porque é pública. A vida interior, que se debruça sobre a mesma pessoa, sobre os membros de sua família, sobre seus amigos, é a que integra o conceito de vida privada, inviolável nos termos da Constituição ³⁰.

Felix Ruiz Alonso³¹, trata a problemática da distinção entre privacidade e intimidade que está intimamente relacionada com as ações da pessoa humana, tendo sempre na essência a dignidade da pessoa humana. Assim define os atos humanos como “aqueles que se realizam de maneira consciente, quer dizer: sabendo o que fazemos e fazendo-os porque queremos.”

Os atos humanos, quando internos, pertencem à intimidade, enquanto que só atos humanos externos, alguns dentre eles, situam-se no mundo da privacidade. A chamada privacidade, por outro lado, é própria dos atos humanos externos e jurídicos que o Direito preserva, não se imiscuindo neles nem normatizando-os. Sabe, pois, de sua existência e de sua alteridade, mas respeita sua privacidade, em virtude de sua função, natureza, significado ou excelência humana ³².

Por difícil que seja cristalizar a problemática da privacidade em um único conceito, é, no entanto, razoavelmente natural constatar que ela sempre foi diretamente condicionada pelo estado da tecnologia em cada época e sociedade. Podemos inclusive aventar a hipótese de que

²⁷ JABUR, Gilberto Haddad – A dignidade e o rompimento de privacidade. in: MARTINS FILHO, Ives Gandra; MONTEIRO JUNIOR, Antônio Jorge (Coord.). **Direito à privacidade**. 2005. p. 90.

²⁸ SANTOS, Antonio Jeová – **Dano Moral na Internet**. São Paulo: Metodo, 2001. ISBN 858645625X, p. 172

²⁹ *Idem* - **Op. Cit.** p. 177.

³⁰ *Idem* – **Ibidem**.

³¹ ALONSO, Felix Ruiz – Pessoa, intimidade e o direito à privacidade in: MARTINS FILHO, Ives Gandra; MONTEIRO JUNIOR, Antônio Jorge (Coord.). **Direito à privacidade**. 2005. p. 17.

³² *Idem* – **Op. Cit.** p. 23.

o advento de estruturas jurídicas e sociais que tratem do problema da privacidade são respostas diretas a uma nova condição da informação, determinada pela tecnologia³³.

Mergulhando no instituto da intimidade e da privacidade, tem-se como uma peculiaridade do direito da personalidade comum a cada indivíduo. A privacidade é um aspecto fundamental da realização da pessoa e do desenvolvimento da sua personalidade³⁴.

Há de se consignar, segundo Sônia Aguiar³⁵, a distinção entre direito da personalidade e personalidade. Em sentido jurídico, personalidade é a aptidão para ser sujeito de direitos e obrigações no mundo jurídico, bastando para tanto a concepção para que tal aptidão lhe seja conferida. É um dom inato, que deriva da própria condição humana e não decorrem da vontade do homem. Onde o direito, através do ordenamento jurídico, compete sujeitar-se a estes direitos, (e não ditar-lhes a existência), tutelando-os de forma eficaz³⁶.

Maria Helena Diniz³⁷ situa “personalidade como o primeiro bem da pessoa, que lhe pertence como primeira utilidade, para que ela possa ser o que é, para sobreviver e se adaptar às condições do ambiente em que se encontra, servindo-lhe de critério para aferir, adquirir e ordenar outros bens”. Os direitos da personalidade derivam da própria existência humana, sendo irrenunciáveis e intransmissíveis, tais como: vida, integridade física, honra, imagem, nome, liberdade, intimidade e vida privada. São direitos que se apoiam na personalidade, servindo à sua proteção e tutela³⁸.

A pessoa, é o valor-fonte de todos os valores, sendo o principal fundamento do ordenamento jurídico; os direitos da personalidade correspondem às pessoas humanas em cada sistema básico de sua situação e atividades sociais. Cada direito da personalidade se vincula a um valor fundamental que se revela através do processo histórico, o qual não se desenvolve de maneira linear, mas de modo diversificado e plural, compondo as várias civilizações, nas quais há valores fundantes e valores acessórios, constituindo aqueles as que denomino invariantes axiológicas. Estas parecem inatas, mas assinalam os momentos temporais de maior duração, cujo conjunto compõe o horizonte de cada ciclo essencial da vida humana³⁹.

Como já mencionado os dois direitos intimidade e privacidade, têm garantias constitucionais, e que uma vez violados deverão ser reparados, em que pese as diferenças muito

³³ DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006. ISBN 85-7147-562-8, p. 60.

³⁴ *Idem* – **Op. Cit.** p. 9.

³⁵ VIEIRA, Sônia Aguiar do Amaral - **Inviolabilidade da Vida Privada e da Intimidade pelos Meios Eletrônicos**. 2002. p. 7.

³⁶ *Idem* – **Op. Cit.** p. 11.

³⁷ DINIZ, Maria Helena - **Curso de Direito Civil Brasileiro: Teoria Geral do Direito Civil**. 14ª ed. São Paulo: Saraiva, 1998. ISBN 9788502143326, p. 99.

³⁸ VIEIRA, Sônia Aguiar do Amaral - **Inviolabilidade da Vida Privada e da Intimidade pelos Meios Eletrônicos**. 2002. p. 8.

³⁹ JUNIOR REALE, Miguel – **Os Direitos da Personalidade**. [Em linha]. [Consult. 26 jan. 2018]. Disponível em WWW: <URL:<http://www.miguelreale.com.br/artigos/dirpers.htm>>.

tênuas entre os dois institutos, há de se sopesar o alcance dos valores alvejados uma vez que a tutela jurisdicional pode não ser idêntica para ambos os direitos maculados. A violação da intimidade carece de uma sanção mais severa pois atinge a parte mais íntima do ser humano, são segredos que só ele possui e que não quer sejam assoalhados, enquanto a violação da vida privada, atinge particularidades de sua vida, mas numa órbita menos íntima.

Devido à complexidade de uma definição de privacidade e intimidade, diversas expressões são utilizadas para expressar esse significado: “direito de estar só”, “direito a ser deixado em paz”, “direito à proteção da intimidade da vida privada ou direito à zona de intimidade da esfera privada.

O direito à intimidade é considerado por doutrinadores, tribunais e tratados internacionais, segundo Antonio Jeová dos Santos⁴⁰, como sendo de suprema importância para a felicidade humana. É considerado como direito fundamental da humanidade. Protege o indivíduo das autoridades, do público em geral e dos demais indivíduos. O direito à intimidade é o direito de viver de forma independente sua própria vida, com um mínimo de ingerência alheia.

Para assegurar o direito à intimidade não se faz necessário que o indivíduo esteja recluso, “só”, a violação desse direito pode suceder a distância através da tecnologia avançada com uso da internet. E, o real infrator pode estar a léguas de distância.

⁴⁰ SANTOS, Antonio Jeová – **Dano Moral na Internet**. 2001. p. 175-6.

1.1 Cenário da privacidade

Como já retratado, a relação simbiótica entre privacidade e intimidade, nos leva a comungar com a assertiva de Marcelo Cardoso Pereira⁴¹ onde a intimidade abrange, por assim dizer, um âmbito mais limitado, ligado, ao menos em sua acepção mais estrita, ao interior, à zona espiritual da pessoa. Partindo dessa premissa, podemos afirmar que a vida privada seria, em uma primeira aproximação, tudo o que não pertença a esse âmbito íntimo, mas que, por sua vez, não transpassasse à esfera pública. A vida privada está condicionada a uma série de fatores que, se não a podem configurar totalmente, influem de forma decisiva na determinação de seu âmbito e alcance. Assim por exemplo, fatores culturais, sociais e até mesmo econômicos podem influenciar no âmbito da vida privada de uma pessoa⁴².

Danilo Doneda⁴³ discorre no sentido de que a privacidade não era expressiva, em função de sociedades mais rígidas onde o ordenamento jurídico tinha um cunho patrimonial e corporativista e até mesmo pelo seu cunho eminentemente subjetivo. O despertar do Direito para a privacidade ocorreu justamente num período em que mudou a percepção da pessoa humana pelo ordenamento, do qual ela passou a ocupar papel central e ao qual se seguiu a juridificação de vários aspectos do seu cotidiano⁴⁴.

A definição de privacidade é mutável no tempo e no espaço. A concepção de privacidade data dos primórdios, no final do século XIX, nos Estados Unidos, alastrando-se para os países que adotavam o Common Law. O caso emblemático de *right of privacy* (assim denominado nos Estados Unidos) só ganhou realce e destaque na comunidade jurídica, com publicação do artigo intitulado “O direito de estar só”, de Samuel D. Warren e Louis D. Brandeis, em 15 de dezembro de 1890, na *Harvard Law Review*, assim considerado o mola propulsora que incitou o direito à privacidade, em que pese já ter existido uma embrionária preocupação, no ano de 1834, com manifestação da vontade da pessoa de ser deixada só, *O right to be let alone*, de cunho individualista, num caso decidido pela Suprema Corte (*Wheaton v. Peters*) do Magistrado norte americano Cooley, que no entanto, não foi assentida pelo mundo jurídico.

A mais antiga definição acerca do direito à privacidade foi trazida pelo Juiz Cooley, em 1873, para quem o direito à privacidade é identificado como o direito de ser deixado

⁴¹ PEREIRA, Marcelo Cardoso - **Direito à Intimidade na Internet**. 2011. p. 115.

⁴² *Idem* – **Op. Cit.** p. 116.

⁴³ DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006. ISBN 85-7147-562-8, p. 8.

⁴⁴ *Idem* – **Ibidem**.

só: *The right to be alone*⁴⁵. “O artigo de Brandeis e Warren enfocava justamente a tecnologia como provedora dos meios que possibilitavam a intromissão indevida em assuntos privados: a fotografia, a imprensa, as gravações, todas em contínuo desenvolvimento”, como sinaliza Danilo Doneda, em seu artigo⁴⁶.

Os grandes teóricos concebem o referido artigo como o início do direito à privacidade. O texto faz uma abordagem da intensidade e a complexidade da vida, o avanço da sociedade e da tecnologia que tornou os indivíduos mais sensíveis a certa publicidade, onde a privacidade e a solidão passaram a ser crucial na individualidade de cada pessoa, devendo as mesmas serem salvaguardadas.⁴⁷ É bem verdade que os tribunais norte-americanos, de início, não reconheciam a existência do direito à privacidade, mas com o passar do tempo passou a ser defendido e acolhido a tese de violação ao direito à privacidade a partir do conteúdo do referido artigo.

O artigo é original ao propor uma força inédita ao novo *right to privacy*, e também é mais que mero reflexo de uma época, fazendo estender sua influência por algumas de suas características: i) partia-se de um novo fato social, que eram as mudanças trazidas para a sociedade pelas tecnologias de informação (jornais, fotografias) e a comunicação de massa, fenômeno que se renova e continua moldando a sociedade futura; ii) o novo “direito à privacidade; iii) no que interessa somente aos EUA, o artigo abriu caminho para o reconhecimento (que porém ainda tardaria décadas) do direito à privacidade como um direito constitucionalmente garantido⁴⁸.

Algumas críticas foram feitas a cerca desse artigo, e nessa linha José Ribas Vieira, citando Solove⁴⁹, propôs uma análise pragmática das diversas percepções sobre a privacidade desde o artigo – *The Right to Privacy* formulado por Samuel Warren e Louis Brandeis (1890), onde muitos doutrinadores ainda hoje reconhecem como o marco do início do reconhecimento do direito à privacidade, movendo-se para o acesso limitado à esfera do indivíduo, e seguida para o sigilo, varando para o controle sobre as informações pessoais, a proteção da personalidade até a intimidade, não significando dizer com isso que exista uma gradação valorativa entre eles, e sim a construção de teorias que perpassaram de um cenário acanhado para uma visão mais ampla como assevera Solove⁵⁰.

⁴⁵ VIEIRA, Sonia Aguiar do Amaral - **Inviolabilidade da Vida Privada e da Intimidade pelos Meios Eletrônicos**. 2002. p. 19.

⁴⁶ DONEDA, Danilo Cesar Maganhoto - **Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade**. [Em linha]. [Consult. 15 fev. 2018]. Disponível em WWW: <URL: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/8196-8195-1-PB.htm>>.

⁴⁷ WARREN S D.; BRANDEIS, Louis D. *The Right to Privacy*. Harvard Law Review. Cambridge. ISSN: .4:5 (1890) p. 196. [Em linha]. [Consult. 17 fev. 2018]. Disponível em WWW: <URL: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>>.

⁴⁸ DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. 2006. p. 138-9.

⁴⁹ SOLOVE *apud* VIEIRA, Jose Ribas – *Trajetórias Teóricas do Direito à Intimidade e à Vida Privada in: VIEIRA, Jose Ribas (Coord). Direitos à Intimidade e à Vida Privada*. Curitiba: Juruá, 2011. ISBN 978-85-362-1999-8, p. 95.

⁵⁰ *Idem* – **Op. Cit.** p. 95.

Uma crítica relacionada ao tema o direito de estar só, salienta Solove⁵¹, “uma vez que este reside na vagueza da expressão direito de estar só, posto que não se define com clareza o que deve ser reputado como inquestionavelmente pertencente ao privado”. A privacidade no artigo de Warren e Brandeis, retratava os anseios de uma sociedade altamente patrimonialista, valorando o direito do indivíduo de dispor das suas informações, e, nesse sentido, não apresentava uma descrição clara, abrindo um leque aos intérpretes acerca da definição da matéria, verifica-se, inicialmente uma visão mais restrita sobre privacidade, onde ao longo do tempo foi expandida com vistas a responder a necessidade da coletividade. “Subsiste a forte constatação de que a *privacy*, hoje, compreende algo muito mais complexo do que o isolamento ou a tranquilidade”⁵², alcançando um número bem maior de pessoas de forma indiscriminada.

A tentativa de conceituar privacidade como sigilo, é considerada estreita por muitos teóricos; com efeito, a privacidade envolve não somente a prevenção da exposição pública indevida, mas também a habilidade de o indivíduo controlar a transmissão das informações desejadas apenas nos limites por ele traçados⁵³. Já o acesso ilimitado à esfera do indivíduo, segundo Solove⁵⁴, representa uma extensão da concepção do direito de estar só, realçando o direito dos indivíduos de buscarem um espaço privado, fora do alcance dos olhares dos não convidados a participar desse âmbito reservado.

A tese da autodeterminação informativa, empodera a pessoa de controlar a informação que diz respeito a sua pessoa, estabelecendo o que pode ou não ser divulgado, ou até mesmo retificar as informações. O artigo 35.º da Constituição Portuguesa contempla a pedra angular da privacidade, o direito à autodeterminação informativa. Entretanto, Solove, citado por José Ribas⁵⁵, faz ponderação a cerca dessa teoria uma vez que não se define os tipos de informação que devam ser controladas. Prossegue proclamando que o tema privacidade não se restringe exclusivamente à esfera individual, como se fosse uma faculdade pessoal a ser exercida por cada indivíduo de acordo com suas ideias; ao revés, cuida-se de matéria de interesse da sociedade que estabelece quais valores agregados ao conceito de privacidade serão protegidos.

Enquanto a intimidade, na qualidade de última concepção teórica concernente à privacidade, e como elemento caracterizador mais importante, reforça a ideia de restrição ao

⁵¹ VIEIRA, Jose Ribas – Trajetórias Teóricas do Direito à Intimidade e à Vida Privada *in*: VIEIRA, Jose Ribas (Coord). **Direitos à Intimidade e à Vida Privada**. 2011. p. 95.

⁵² DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. 2006. p. 10-3.

⁵³ VIEIRA, Jose Ribas – Trajetórias Teóricas do Direito à Intimidade e à Vida Privada *in*: VIEIRA, Jose Ribas (Coord). **Direitos à Intimidade e à Vida Privada**. 2011. p. 96.

⁵⁴ SOLOVE, Daniel J. - **The Digital Person Technology and Privacy in the Information Age**. United States of America: General Editors, 2004. ISBN 0-8147-9846-2, p. 95.

⁵⁵ SOLOVE, Daniel J *apud* RIBAS - Trajetórias Teóricas do Direito à Intimidade e à Vida Privada *in*: VIEIRA, Jose Ribas (Coord). **Direitos à Intimidade e à Vida Privada**. 2011. p. 97.

acesso privado e de controle de informações que os indivíduos pretendem guardar da curiosidade alheia⁵⁶.

Novoa Monreal, citado por Antonio Jeová Santos⁵⁷, descreve três elementos típicos que caracterizem a privacidade: Em primeiro lugar, devem tratar-se de manifestações que normalmente se subtraíam do conhecimento de pessoas alheias ao círculo da intimidade; em segundo lugar, que o conhecimento de tais manifestações da parte de terceiros, provoque na pessoa um estado de turbção mora, ao ver afetado seu sentido de pudor ou de recato; finalmente, que o sujeito não queira que os demais tomem conhecimento daqueles fatos.

Caracteriza a vida privada todos aqueles dados, fatos ou situações desconhecidas para a comunidade que são verídicas e que estão reservadas ao conhecimento, seja do sujeito mesmo, seja de um grupo reduzido de pessoas, cuja divulgação ou conhecimento por outros traz aparelhado algum dano – patrimonial ou moral.⁵⁸

Olhando o padrão europeu, destacam-se dois pilares sobre as quais se assentam a intimidade e a vida privada. A intimidade é um âmbito delimitado e especialmente protegido, ao qual se acrescenta um elemento de vontade, de exclusão pretendida. Também é um espaço de plena disposição por parte do indivíduo, de onde exerce liberalidades de forma constante⁵⁹. Lucrecio Rebollo Delgado assim define intimidade como “um conjunto íntegro espiritual, um espaço físico e anímico regido pela vontade do indivíduo”⁶⁰.

Na França, com a Constituição de 1791⁶¹, o primeiro documento revolucionário importante para uma nova espécie de sociedade liberal europeia, incluía proteções extensivas a liberdade de imprensa. Mas ao mesmo tempo, adicionou proteções contra calúnias e insultos relativos à vida privada.

O Direito francês avançou em relação ao direito à intimidade quando de um julgamento famoso em 1867 que envolveu Alexandre Dumas, pai, autor de Os Três Mosqueteiros, que versava sobre a discussão da privacidade das relações amorosas envolvendo sexo, o Tribunal

⁵⁶ RIBAS *apud* SOLOVE, Daniel J. - **The Digital Person Technology and Privacy in the Information Age**. 2004. p. 98.

⁵⁷ MONTREAL, Novoa *apud* SANTOS, Antonio Jeová – **Dano Moral na Internet**. São Paulo: Metodo, 2001. ISBN 858645625X, p. 173.

⁵⁸ DELIA FERREIRA *apud* SANTOS, Antonio Jeová – **Dano Moral na Internet**. São Paulo: Metodo, 2001. ISBN 858645625X, p. 178.

⁵⁹ VIEIRA, Jose Ribas – Trajetórias Teóricas do Direito à Intimidade e à Vida Privada *in*: VIEIRA, Jose Ribas (Coord). **Direitos à Intimidade e à Vida Privada**. 2011. p. 82.

⁶⁰ DELGADO, Lucrecio Rebollo – **El Derecho fundamental a la intimidad**. 2ª ed. Madrid: Dickinson, 2005. p.69.

⁶¹ VIEIRA, Jose Ribas – Trajetórias Teóricas do Direito à Intimidade e à Vida Privada *in*: VIEIRA, Jose Ribas (Coord). **Direitos à Intimidade e à Vida Privada**. 2011. p. 89.

ênfatiou o princípio da dignidade que se sobrepõe a propriedade⁶². A partir desse caso emblemático ficou patente a existência do direito a imagem das pessoas, sendo utilizado em diversas outras demandas.

A Alemanha teve um retardo na construção de um sistema jurídico uniforme em função de ter sido uma sociedade de unificação política tardia. Por esse motivo a experiência alemã sobre direitos fundamentais apresentou dois momentos distintos de desenvolvimento: dos estágios iniciais de sua unificação até a ascensão do regime nacional-socialista, período que compreende cerca de sete décadas, e após o armistício de 1945, momento em que foi derrubado um regime totalitário, adquiriu grande vulto a defesa das liberdades⁶³.

Após 1880, a Alemanha percebeu que o elemento de maior relevância para a tutela da privacidade residia no reconhecimento da honra, a ser tratada através do direito ao insulto, em coordenação com o direito de propriedade artística. Afigurando assim como fundamento do direito de personalidade alemão o direito de insulto e o direito de criação artística.⁶⁴

Na Alemanha, Heinrich Henkel, no ano de 1957, defendeu a Teoria dos Círculos Concêntricos da esfera da vida privada, que consistia em três círculos: o círculo maior e mais extenso, tem-se a esfera da vida privada, onde abarca as relações interpessoais, admitindo-se a possibilidade de interesse público se forem de grande importância para uma coletividade⁶⁵. O círculo intermediário encontra-se a esfera da intimidade já com uma certa restrição, limitando o número de pessoas com relações mais próximas e mais confiabilidade, com acesso a informações pessoais, e, por último, no menor círculo, de uma dimensão bem menor e restrita a esfera do segredo, lugar de reserva, onde estão contidas informações que o indivíduo não quer que seja de domínio público e que só participam delas os amigos bem mais próximos.

A referência a essa teoria, que de certa forma procurou diferenciar os limites das esferas privacidade, intimidade e segredo, também enfrentou críticas por não estabelecer de forma clara o limiar dos institutos, deixando dúvidas. No Direito Alemão, houve superação desta tese na medida em que, para a devida proteção jurídica, não se pode levar em consideração somente

⁶² “ (...) pelo menos quando imagens lascivas estiverem envolvidas: a privacidade de alguém, como outros aspectos da honra pessoal, não era uma commodity de mercado que podia simplesmente ser vendida de forma definitiva. Qualquer venda por uma pessoa que tivesse momentaneamente ‘esquecido sua dignidade’ tinha que ser efetivamente anulada”. WHITMAN *apud* VIEIRA, Jose Ribas – Trajetórias Teóricas do Direito à Intimidade e à Vida Privada *in*: VIEIRA, Jose Ribas (Coord). **Direitos à Intimidade e à Vida Privada**. 2011. p. 90.

⁶³ VIEIRA, Jose Ribas – Trajetórias Teóricas do Direito à Intimidade e à Vida Privada *in*: VIEIRA, Jose Ribas (Coord). **Direitos à Intimidade e à Vida Privada**. 2011. p. 91.

⁶⁴ WHITMAN *apud* VIEIRA, Jose Ribas – Trajetórias Teóricas do Direito à Intimidade e à Vida Privada *in*: VIEIRA, Jose Ribas (Coord). **Direitos à Intimidade e à Vida Privada**. 2011. p. 92.

⁶⁵ COSTA JUNIOR, Paulo José da - **O direito de estar só: tutela penal da intimidade**. 2ª ed. São Paulo: RT, 1995. ISBN: 9780786162635, p. 36.

a natureza das informações, mas também a necessidade e finalidade da utilização destes dados⁶⁶.

A divulgação do artigo Right to Privacy, desencadeou no mundo jurídico um reconhecimento maior no que diz respeito ao direito à intimidade e a privacidade, podendo-se testemunhar através de várias decisões não só da Corte Suprema Americana, mas em diversas declarações e convenções de âmbito internacional⁶⁷. Exemplificando tem-se a Declaração Universal dos Direitos Humanos⁶⁸, em 1948, legitimou em seu artigo XII o direito à vida privada e a intimidade: “Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques”.

A Convenção Europeia de Direitos do Homem⁶⁹, em 1950, lastreada na Declaração Universal dos Direitos do Homem aclamada pela Assembleia Geral das Nações Unidas em 10 de dezembro de 1948, reconheceu de forma expressa em seu artigo 8º o direito ao respeito pela vida privada:

Artigo 8º : Direito ao respeito pela vida privada e familiar 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.

E, posteriormente em 2004 com o Tratado da Constituição Europeia⁷⁰, que abarcou a Convenção Europeia de Direitos do Homem de 1950, ressaltou o respeito a vida privada num sentido mais amplo em seu artigo II-67 e já se vislumbra a necessidade de dar arrimo a proteção de dados, como consta no artigo II-68.

⁶⁶ FILHO JOSE, Wagson Lindolfo - **Teoria dos círculos concêntricos da esfera da vida privada**. [Em linha]. [Consult em 30 Jan. 2018]. Disponível em WWW: <URL:<http://www.magistradotrabalhista.com.br/2016/03/teoria-dos-circulos-concentricos-da.html>>.

⁶⁷ CARVALHO, Luis Gustavo Grandinetti Castanho – **Direito à Privacidade**. [Em linha] [Consult. 31 maio 2018] Disponível em WWW: <URL:http://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista02/revista02_51.pdf>.

⁶⁸ DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS. [Em linha]. [Consult. 01 fev. 2018]. Disponível em WWW <https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf>.

⁶⁹ EUROPEAN COURT OF HUMAN RIGHTS. Convenção Europeia de Direitos do Homem. [Em linha]. [Consult. 01 fev. 2018]. Disponível em WWW: <URL:http://www.echr.coe.int/Documents/Convention_por.pdf>.

⁷⁰ UNIÃO EUROPEIA - **Tratado da Constituição Europeia** [Em linha]. Luxemburgo: Europa, 2005. [Consult. 01 fev. 2018]. Disponível em WWW: <URL: https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_establishing_a_constitution_for_europe_pt.pdf>.

A Carta dos direitos fundamentais da União Europeia de 2016⁷¹ reconheceu e adaptou a Carta proclamada em 07 de dezembro de 2000 e manteve em seus artigos 7 e 8 o respeito a vida privada e a proteção de dados de caráter pessoal.

A Resolução do Parlamento Europeu de 13 de dezembro de 2016, sobre a situação dos direitos fundamentais da União Europeia em 2015⁷², dentre outros pontos que foram relatados, defendeu e reiterou que a dignidade da pessoa humana é a base inviolável de todos os direitos fundamentais e não deve ser sujeita a nenhum tipo de instrumentalização e que deve respeitar –se e proteger-se em todas as iniciativas da União. Requisitando a conscientização dos cidadãos da União sobre a dignidade no âmago do ser humano de forma mais justa.

E, no que tange aos direitos digitais, rememora que toda a pessoa tem direito a sua esfera privada e a proteção dos dados pessoais que lhe afeta e que inclui o direito de acesso aos dados coletados relativos a eles e o direito de corrigir esses dados. Destacando ainda o direito de cada pessoa decidir por si mesma sobre seus dados pessoais, em especial o direito de decidir sobre o uso e a divulgação de seus dados pessoais.

A dignidade da pessoa humana não é um direito, mas um atributo que todo ser humano possui, independentemente de sua origem, sexo, idade, condição social ou qualquer outro requisito⁷³. É imperioso ressaltar que as legislações vigentes não outorgam dignidade aos seus indivíduos, mas incontestavelmente tem o dever de tutelá-la contra o menor indício de mácula, independentemente dos direitos que estão sendo atingidos. E, é consolidado na doutrina e na jurisprudência que o direito a intimidade e a privacidade são direitos fundamentais, que tem como sustentáculo o princípio basilar da dignidade da pessoa humana contido em diversas constituições de países da Europa e do Brasil.

A Constituição Federal da República Federativa do Brasil de 1988, destacou dos direitos da personalidade, a intimidade e a privacidade de forma salvaguardar a dignidade da pessoa humana, como fundamento do Estado Democrático de Direito, e qualquer violação deverá ser reparada. A dignidade da pessoa humana está intrinsecamente relacionada com o atuar do homem. O homem ganha sua própria dignidade enquanto determina autonomamente o seu próprio comportamento e, assim, constrói para si uma identidade⁷⁴. A privacidade e a

⁷¹ UNIÃO EUROPEIA - **Carta dos Direitos Fundamentais da União Europeia**. [Em linha]. [Consult. 01 fev. 2018]. Disponível em WWW: <URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN>.

⁷² UNIÃO EUROPEIA (PARLAMENTO) - **Resolución del Parlamento Europeo de 13 de diciembre de 2016, sobre la situación de los derechos fundamentales en la Unión Europea en 2015**. [Em linha]. [Consult. 01 fev. 2018]. Disponível em WWW: <URL:http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2016-0485&language=ES&ring=A8-2016-0345>.

⁷³ NOVELINO, Marcelo. **Direito constitucional**. 2ª edição. São Paulo: Método, 2008, p. 210.

⁷⁴ HASSO, Hofmann *apud* DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. 2006. p. 72.

intimidade alcançam o princípio constitucional da dignidade da pessoa humana. A pessoa é o próprio ser humano.

O artigo 5º inciso X da Constituição Federal⁷⁵, dispõe “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”. O código Civil⁷⁶ brasileiro em seu artigo 21, também ratifica o mesmo pensamento: “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”. Os dois direitos não se misturam, devendo ser interpretados em função de suas peculiaridades, e tutelados de per si.

Yves Gandra da Silva Martins e Celso Ribeiro Bastos citados por Sônia Aguiar⁷⁷ afirmam que a tutela à vida privada e à intimidade consiste:

Na faculdade que tem cada indivíduo de obstar a intromissão de estranhos na sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano.

O direito à vida privada e à intimidade deve ser tutelado pelo Estado, mas não podemos achar que estes institutos sejam absolutos, sem sofrer qualquer restrição, já que a vida em sociedade nos impõe várias limitações diariamente. Nenhum direito fundamental é absoluto. Esses direitos estão atrelados à sociedade e as pessoas que nela convivem. Logo, em determinadas ocasiões em que nos deparamos com valores em conflito, temos que analisar e ponderar os valores em jogo, onde muitas vezes o interesse público se justapõe em detrimento do interesse privado, ainda que para isso muitas vezes, tenhamos que renunciar o direito a intimidade. Importante sinalizar que as limitações a vida privada e a intimidade existem sendo que estas jamais poderão ser desprezadas. Porque, o interesse público haverá que se deter diante da esfera mais íntima da vida privada, que é inviolável. A intromissão ali, do interesse público, seria injustificável, configurando-se mera curiosidade⁷⁸.

Há casos, ainda, nos quais o conflito existe entre dois interesses privados, cabendo estabelecer qual deles deve prevalecer. Justifica-se a revelação de aspectos da vida privada e da intimidade da parte contrária que servirão de fundamento para o pedido de ações como anulação

⁷⁵ BRASIL. **Constituição da República Federativa do Brasil**, de 05 de outubro de 1988.

⁷⁶ BRASIL. Lei n.º 10.406, de 10 de janeiro de 2001. **Institui o Código Civil**. [Em linha]. [Consult. 01 de jan. 2018]. Disponível em WWW: <URL: http://www.planalto.gov.br/ccivil_03/leis/2002/110406.html>.

⁷⁷ VIEIRA, Sonia Aguiar do Amaral - **Inviolabilidade da Vida Privada e da Intimidade pelos Meios Eletrônicos**. 2002. p. 23.

⁷⁸ MORSILLO *apud* VIEIRA, Sonia Aguiar do Amaral - **Inviolabilidade da Vida Privada e da Intimidade pelos Meios Eletrônicos**. 2002. p. 28.

de casamento, reconhecimento de filiação, separação judicial e divórcio; igualmente se concebe sejam os rendimentos de alguém revelados judicialmente por aquele que pleiteia alimentos⁷⁹.

O surgimento da internet, onde o seu principal traço é o anonimato, revolucionou o mundo, e a reboque trouxe no seu bojo problemas que estão colocando em xeque direitos fundamentais, até então tidos como impenetráveis e indestrutíveis. Estamos vivenciando momentos de impasse, onde frequentemente nos deparamos com colisão de princípios onde sempre temos de um lado, o direito à informação e de outro a violação de direitos de dados pessoais. A busca da informação precisa e rápida é fundamental para o desenvolvimento de um País e para a garantia do Estado democrático de direito. Um país democrático, há de ser mensurado pela dimensão da informação, pela sua valia e em especial pelo alcance da quantidade de pessoas atingidas.

Paulo Silva Fernandes⁸⁰ citando Milan Kundera nos revela que “no reverso da medalha encontramos o facto – para muitos aterrador – de estarmos privados, hoje como nunca, da nossa privacidade, já que parece já ninguém poder “esconder-se em parte nenhuma e que cada um está à mercê dos outros”.

Como apontamos no início, o incidente ocorrido em 11 de setembro de 2001, foi um marco para a história mundial, onde foram promulgadas leis que produziram grandes limitações a direitos e garantias individuais, com vistas a enfrentar a guerra contra o terrorismo. Uma nova realidade despontou no horizonte, onde a população de alguns países, em especial a Grã-Bretanha, que é (considerado o país mais bem monitorado do mundo), os movimentos das pessoas, hábitos, os locais públicos, as ruas etc. estão constantemente vigiados. Falamos assim, de uma sociedade de vigilância onde atualmente ninguém mais está escondido ou poderá agir no anonimato. A bandeira do terrorismo desencadeou um poder irrestrito as autoridades norte americanas, para agir em qualquer instância, para empreender programa de vigilância em massa, não só restrito aos Estados Unidos, mas em qualquer país do mundo onde porventura viesse a existir uma pequena possibilidade de ameaça terrorista.

Vigilância eletrônica em massa e a privacidade no mundo digital passou a ser uma tormenta mundial, em qualquer lugar do planeta você pode estar sendo vigiado. Segundo Glenn Greenwald⁸¹, o temor relacionado ao terrorismo – intensificado pelos constantes exageros quanto ao risco real – vem sendo explorado por líderes norte-americanos para justificar uma

⁷⁹ MORSILLO *apud* VIEIRA, Sonia Aguiar do Amaral - **Inviolabilidade da Vida Privada e da Intimidade pelos Meios Eletrônicos**. 2002. p. 28.

⁸⁰ KUNDERA *apud* FERNANDES, Paulo Silva - **Globalização, “Sociedade de Risco” e o Futuro do Direito Penal**. 2001. p. 38.

⁸¹ GREENWALD, Gleen – **Sem Lugar pra se Esconder**. Rio de Janeiro: 2014. ISBN 978-85-431-0096-8, p. 15.

ampla gama de políticas extremistas. Continuando, a internet não é apenas nosso correio e nosso telefone. Ela é a totalidade do nosso mundo, o lugar onde tudo acontece. É lá que se faz amigos, se escolhe livros e filmes, se organiza o ativismo político, e é lá que são criados e armazenados os dados mais particulares de cada um. É na internet que desenvolvemos e expressamos nossa personalidade e individualidade. Transformar a internet em um sistema de vigilância em massa é estar a um passo do aniquilamento da privacidade uma das garantias fundamentais do cidadão⁸².

A Internet reduziu drasticamente as barreiras de tamanho, tempo e distância entre pesquisadores, empresas e governos, facilitando o crescimento baseado no conhecimento, na pesquisa de ponta e no acesso à informação⁸³.

David R. Koepsell⁸⁴ leciona que o ciberespaço, foi forjado pelo romancista de ficção científica William Gibson. Como foi usado em sua ficção “ciberpunk”, o termo refere-se ao que ele chama de “alucinação consensual” que os usuários de rede de computador futuristas vivenciam ao abandonar uma rede de computador mundial.

É nesse contexto que surge a questão da proteção de dados, uma vez que o ciberespaço, assim é considerado um admirável mundo novo, onde reina a liberdade, mas em contrapartida mister se faz harmonizar o direito à privacidade que vem, neste ambiente, sendo violados dados pessoais em grande escala, com danos que podem ser irreversíveis aos internautas.

1.2 Privacidade um dos maiores problemas na era digital: internet ameaça o direito à privacidade da civilização humana?

A análise de um direito fundamental da pessoa humana, a privacidade, esmiuçada para a era digital, é imprescindível a compreensão, ainda que ligeira e não aprofundada do conceito de internet e da forma como se opera a rede atingindo milhares de pessoas ao redor do mundo, compartilhando dados, que muitas vezes acabam sendo violados sem que o titular dos dados possa dispor do seu direito à privacidade.

A revolução tecnológica, segundo Antonio Jeová Santos⁸⁵, sempre cria uma ambivalência difícil de ser equacionada. De um lado os benefícios que ela sempre traz; por

⁸² GREENWALD, Gleen – **Sem Lugar pra se Esconder**. Rio de Janeiro: 2014. ISBN 978-85-431-0096-8, p. 15.

⁸³ PAESANI, Liliana Minardi – **Direito e Internet: Liberdade de Informação, privacidade e Responsabilidade Civil**. 2013. p. 1.

⁸⁴ KOEPESELL, David R. – **A Ontologia do Ciberespaço**. Madras, 2004. ISBN 8573748907, p. 24.

⁸⁵ SANTOS, Antonio Jeová – **Dano Moral na Internet**. 2001. p. 180.

outro, as amplas possibilidades de interferir na vida de um ser humano ferindo a sua dignidade⁸⁶.

A abordagem desse admirável mundo novo que se chama internet, o ciberespaço, não é uma questão nova e vem numa marcha desenfreada de grandes transformações. Em decorrência dos avanços impostos pela informática surge a internet, um meio de comunicação eletrônica, ou ainda uma rede de comunicação virtual e mundial que coloca em contato, de forma irrestrita e a custos reduzidos, todas as pessoas do planeta, com a simples utilização de um computador adaptado aos equipamentos e programas adequados⁸⁷.

O surgimento da Web em 1989 impulsionou a internet e alastrou em todo globo terrestre, sem qualquer obstáculo. Criou-se os navegadores, acessados através das conexões de rede, onde milhares de pessoas acessam em busca de informações dos mais variados temas, o que vem crescendo a cada dia. É inconteste que o acesso à internet é uma fonte interminável de conhecimento.

Entretanto, analisando as diversas definições de internet na doutrina, Marcelo Cardoso Pereira⁸⁸ considera equivocada a ideia de que a Internet não é uma simples rede mundial de redes de computadores que possibilita o acesso a intercâmbio de informações, bem como a utilização de serviços em nível mundial, incluindo a possibilidade de comunicação entre máquinas (leia-se computadores). A realidade mostra-nos que a Rede das redes é extremamente surável de sistemas e plataformas.

Evoluindo nessa linha, a internet é um fato, um acontecimento extraordinário e seguramente um dos mais importantes e impactantes fenômenos tecnológicos surgidos até o presente momento. Ainda que o surgimento da Rede não seja um fato novo, seus efeitos e consequências estão, todavia, por vir⁸⁹. É muito comum constataremos a utilização do termo WEB como sinônimo de internet já que é por esse meio que a pessoa acessa a internet. Entretanto há diferenças significativas entre os termos.

Tem-se internet, como já pontuado anteriormente como uma rede de rede que conecta milhares de computadores entre si num mundo sem fronteiras. A web nada mais é que um meio pelo qual oportuniza o acesso à internet.

A internet tornou-se mais uma forma de extensão do homem. Extensão que é coroado pelo fato de estar em determinados lugares ao mesmo

⁸⁶ SANTOS, Antonio Jeová – **Dano Moral na Internet**. 2001. p. 180.

⁸⁷ PODESTÁ *apud* VIEIRA, Sonia Aguiar do Amaral - **Inviolabilidade da Vida Privada e da Intimidade pelos Meios Eletrônicos**. 2002. p. 74.

⁸⁸ PEREIRA, Marcelo Cardoso - **Direito à Intimidade na Internet**. 2011. p. 35.

⁸⁹ *Idem* – **Op. Cit.** p. 36.

tempo, quedando imóvel. Pode-se conversar com alguém que esteja além-mar, com o Oriente, com a América e, até, com um vizinho⁹⁰.

Antonio Jeová Santos⁹¹, assevera que hoje, todos são escravos da Internet, seja pelo fascínio que ela exerce, seja porque o mundo que se antepõe aos olhos do usuário é algo que hipnotiza e que pode embotar outros sentimentos, tornando mais fácil a possibilidade de a pessoa tornar-se misantropo. Os usuários da internet não se apercebem que a internet é um meio muito eficaz de aniquilar o direito à intimidade, e em sua grande maioria de difícil reparação.

Por esse motivo, não há como retroceder, a internet é fato e vem florescendo a passos largos. O Estado tem o dever de acompanhar esse caminho e principalmente desenvolver políticas públicas de forma a garantir ao cidadão internauta que os direitos fundamentais tais como privacidade e intimidade, e os dados pessoais de seus usuários sejam preservados no ciberespaço. A internet é um mundo sem fronteiras. Não existem questões nacionais, nem internacionais, que lhe oponha óbices. A ausência de fronteiras revela que a Internet é um espaço sem território, sem localização geográfica, onde o universo em sua grandeza cabe na Internet. O que está na Rede está no mundo sem qualquer limitação, é transfronteiriço.

A todo momento o internauta, de forma consciente alimenta a rede fornecendo seus dados pessoais, sem qualquer constrangimento, sem imaginar que esses dados são utilizados por várias empresas para diversas finalidades. A privacidade deixa de ser aquele sagrado direito consistente “em estar só” para ser um problema que está ligado diretamente à informação⁹².

A internet acaba sendo o local mais propício para causar danos as pessoas por violação do direito à intimidade, a privacidade e a honra, já que impera a falsa sensação de anonimato, possibilitando os ofensores agirem à vontade para perquirir seu intuito, o de lesar pessoas, violando direitos e garantias estatuídos na Constituição Federal, no inciso X, artigo 5º da Carta Magna.

A captura de dados sem que o usuário tenha conhecimento e sem que tenha consentido com essa prática é efetiva intromissão na vida do cidadão, fere direito individual e rompe com a constituição⁹³.

Nessa seara, relativa ao direito à privacidade, não podemos deixar de dizer que o Estado está presente na vida diária do cidadão⁹⁴.

⁹⁰ SANTOS, Antonio Jeová – **Dano Moral na Internet**. 2001. p. 22.

⁹¹ *Idem* – **Op.Cit.** p. 23-31.

⁹² *Idem* – **Op.Cit.** p. 184-5.

⁹³ *Idem* – **Op.Cit.** p. 186.

⁹⁴ *Idem* – **Op.Cit.** p. 183.

O estado é o grande detentor e invasor da vida privada das pessoas, sob o manto protetor do argumento que necessita de informações cadastrais de seus clientes, bancos e comércio por meio da SERASA e de SPC's, recebem gama de informações que desbordam do simples informe cadastral, porque todos os dados da pessoa são ali deixados. Não se apercebe o cliente que ao preencher simples ficha, tida como cadastral, está abrindo mão de vários aspectos da sua vida privada ⁹⁵.

Nas menores atividades, aquelas que podem parecer insignificantes, ele está presente colacionando informações acerca das pessoas, sendo armazenadas em computadores. É inegável que o surgimento do Computador, foi um facilitador para se proceder ao armazenamento de informações de todos os indivíduos em uma larga escala.

Discorrendo sobre o tema privacidade, onde se está diretamente ligado a captura de dados pessoais, não podemos deixar de mencionar os cookies, que consiste no meio que as empresas operam para aquisição de informações pessoais dos usuários da internet. Antonio Jeová⁹⁶ leciona que esse instrumento é utilizado para obter dados sobre os hábitos dos consumidores, frequências de visita a uma determinada seção, tipo de notícias que o consumidor prefere e assim por diante. Na posse desses dados, eles são incluídos em uma lista que é vendida a comerciantes que as utiliza efetuando estatísticas de critérios de consumo, para enviar produtos não desejados. Uma vez transferidos certos dados, eles são capturados na Rede, podendo-se conhecer os gostos, as preferências pessoais, as ideias de uma pessoa, pelos sites que ela visita com mais assiduidade⁹⁷.

Os cookies são arquivos de dados gerados toda vez que a empresa que cuida da manipulação de dados, recebe instruções que os servidores da web enviam programas navegadores e que são guardadas em diretório específico do computador do usuário. Uma vez captada, a informação pode ser utilizada pelos administradores do sistema com o intuito de elaborar o perfil pessoal dos visitantes de sites. Sendo que o que caracteriza o uso dos cookies não é a finalidade estatística, mas a obtenção de informações com intuito exclusivamente comercial, o arquivo cookie contém o endereço IP do usuário, o que permite que o provedor o identifique imediatamente, como comenta Antonio Jeová Santos ⁹⁸.

Ou seja, o usuário da internet que idealiza que navegar na rede, no ciberespaço, é um território livre, sem qualquer vigilância, com sua privacidade garantida, não se dá conta de que os cookies, acoplados ao sistema dos provedores, na verdade estão espreitando sua navegação

⁹⁵ SANTOS, Antonio Jeová – **Dano Moral na Internet**. 2001. p.183.

⁹⁶ *Idem* – **Op. Cit.** p. 185.

⁹⁷ *Idem* – **Ibidem**.

⁹⁸ *Idem* – **Op.Cit.** p.196-7.

na internet sem qualquer notificação ao internauta, caracterizando dessa forma uma invasão da privacidade do usuário, violando o direito do cidadão a proteção de seus dados pessoais.

No próximo capítulo nos ocuparemos com um dos mais novos aspectos do direito da personalidade: a proteção dos dados pessoais, assim considerados indicativos de aspectos da nossa personalidade⁹⁹, onde se impõe a tutela jurídica. Partiremos de uma abordagem histórica e evolutiva da proteção de dados pessoais, nos detendo nos pilares das normas jurídicas de proteção de dados pessoais, percorrendo pelos 3 eixos principais: dados pessoais, anonimização de dados pessoais e consentimento adjetivado, devendo ser livre, informado, explícito, específico, o que de certa forma empodera o seu titular, onde somente ele poderá controlar suas informações, elaborando sua esfera particular, caracterizando a autodeterminação informativa. E, finalizando com a legislação de proteção de dados pessoais no Brasil, inicialmente com o Marco Civil da Internet, sua influência na legislação da Itália e França, e finalmente, no Brasil, o surgimento de uma norma específica de Proteção de Dados a Lei 13.709 promulgada em 14 de agosto de 2018, onde sua vigência foi alterada, através de Medida Provisória 869/2018, para 24 meses após a sua publicação.

⁹⁹ DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. 2006. p. 1.

CAPÍTULO II

2 DIREITO À PROTEÇÃO DE DADOS PESSOAIS

O tratamento desse tema é de fundamental importância no nosso tempo. Os dias de hoje, tem-se uma situação factual e que atinge a toda uma humanidade nos cinco continentes, que é o mundo cibernético, onde as pessoas estão interligadas 24 horas por dia. A cada click que o cidadão dá no universo da internet, através de um computador ou um celular, está expondo sua vida privada, sem qualquer comedimento, seus dados pessoais estão circulando sem restrições nas redes sociais, abrindo uma lacuna para que terceiros, tido como invasores, se apoderem dos dados compartilhados em algum site e comercializarem o uso desses dados sem autorização do usuário. Os últimos anos são constantes as notícias nos grandes jornais de circulação, em especial no Reino Unido, onde o facebook foi multado por violação de dados pessoais de seus usuários, ou seja, dados de milhares de pessoas foram utilizados por desenvolvedores de aplicativos sem o consentimento informado dos utentes.

Nesse panorama de avanços tecnológicos galopantes, mister, ao longo dos tempos, passou-se a ter uma maior preocupação com as pessoas de forma a asseverar os seus dados pessoais. A questão da proteção de dados que começou a emergir, através de uma tutela jurisdicional, só aflora quando o seu exercício pode vir a ser lesivo aos direitos e garantias fundamentais da pessoa humana.

Desde os anos 60, em função do reconhecimento da magnitude do uso das telecomunicações, na Europa já se vislumbrava os primeiros passos para uma conscientização da necessidade de se resguardar os dados pessoais preservando assim a privacidade e a intimidade ainda que naquela época houvesse poucos recursos tecnológicos e de forma muito primitiva.

A abordagem desse tema dados pessoais nos remete, inquestionavelmente a ligação com o termo informação, consoante exemplifica Danilo Doneda¹⁰⁰, o conteúdo de ambos os vocábulos, dados e informação, se sobrepõe em várias circunstâncias, o que justifica promiscuidade na sua utilização, muito embora as palavras, necessariamente, representam um fato dentro de um contexto.

“Dado” apresenta uma conotação um pouco mais primitiva e fragmentada, estaria associado a uma espécie de “pré-informação”, anterior à interpretação e ao processo de elaboração, enquanto a informação, por sua vez, alude a algo além da representação contida no

¹⁰⁰ DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar. 2006. p. 152.

dado, chegando ao limiar da cognição, e mesmo nos efeitos que esta pode apresentar para o seu receptor. A doutrina não raro trata estes dois termos indistintamente. Um verdadeiro retrato da estrutura social pode ser tratado a partir da informação¹⁰¹.

Nessa rota Danilo Doneda alude Norbert Wiener¹⁰², onde amplia o conceito de informação, onde é concebida como o termo que designa o conteúdo daquilo que permutamos com o mundo exterior ao ajustar-nos a ele, e que faz com que o nosso ajustamento seja nele percebido. O processo de receber e utilizar informações é o processo de nosso ajuste às contingências do meio ambiente e do nosso efetivo viver neste ambiente.

Nesse contexto faremos um passeio, para melhor entender a longa caminhada evolutiva da necessidade cada vez maior de se proteger os dados pessoais de cada indivíduo garantindo e preservando o seu direito a intimidade e privacidade.

2.1 Antecedentes e evolução da legislação de proteção de dados pessoais

A primeira geração de normas relativas à proteção de dados surgiu como um meio de proteção de acordo com as necessidades existentes. O uso da base de dados era essencialmente pela Administração Pública devido ao alto custo dos computadores daquele período. Sequer se podia falar em uso indevido de dados por parte dos cidadãos, pois os computadores da época eram muito limitados, com poucos recursos. Os computadores tinham uma capacidade muito limitada, sem muita perfeição técnica, podendo se qualificar como rudimentar, precário sem muita engenharia. A informática estava na primeira infância, ainda engatinhando. A atenção com dados pessoais data de tempos atrás, sendo que com a evolução da tecnologia se fez necessário abrigá-los com mais veemência, onde começaram a emergir lesões a direitos consagrados pelo mau uso dos dados pessoais, o que mister se faz a necessidade de uma regulação jurídica, em busca de uma proteção jurídica eficiente. Em 1935 o Presidente norte-americano Roosevelt, aprovou a Social Security Act, criado com uma finalidade social que pretendia atualização de dados relativos a trabalhadores tal como assistência médica, pensões e outros benefícios¹⁰³.

Em função do grande número de dados coletados, e do público alvo, esses dados se multiplicaram por milhões de trabalhadores, o que supõem-se o primeiro grande desafio no

¹⁰¹ DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar. 2006. p. 152.

¹⁰² WIENER, Norbert *apud* DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar. 2006. p. 155.

¹⁰³ DELGADO, Lucrecio Rebollo – **Vida Privada Y Protección de Datos en la Unión Europea**. Madrid: Dykinson, 2008. p. 83.

tratamento de dados, mas, em função da escassez de meios e técnicas os objetivos eram alcançados de forma parcial.

O verdadeiro impulso técnico, veio da intenção de aprimorar as técnicas de guerra. Em 1943 um conjunto de especialistas a serviço do exército britânico construiu o chamado Colossus, que tinha como alvo durante a II grande Guerra Mundial decifrar em poucos segundos mensagens secretas dos nazistas¹⁰⁴.

Avançando, em 1968, através da IBM, se introduz o primeiro sistema de gestão de base de dados, onde com uma melhor aplicação dos computadores da época podiam gerenciar uma grande quantidade de dados distinguindo os técnicos de um lado e do outro estariam os dados relativos as pessoas¹⁰⁵. O uso lesivo da informática vai sendo incrementado na medida em que se produz o avanço tecnológico, e especialmente quando se começa a generalizar o uso do computador, não só pelas empresas institucionais, mas também por particulares¹⁰⁶. Dado isso conclui-se uma necessidade real de garantir a possibilidade de uma proteção jurídica face à iminência de ofensa a direitos fundamentais dos indivíduos.

Percebe-se que os Estados Unidos devido ao seu pioneirismo no desenvolvimento dos computadores, esperava-se, também que fosse desbravar no sentido da criação de leis que resguardassem os direitos fundamentais da pessoa em relação a proteção de seus dados pessoais. No entanto, a Europa saiu na vanguarda, despertou e fomentou o estudo do impacto da tecnologia da informação e os riscos para a invasão de direitos fundamentais do cidadão como a proteção à privacidade e intimidade dos dados pessoais, não só , limitando-se à esfera pública, pelo fato de desenvolver técnicas para exercer e controlar os dados pessoais da população, mas disseminando para a esfera privada onde se atestou, também, a probabilidade de lesionar direitos com a violação de dados pessoais, tanto quanto na esfera pública.

O pioneirismo da primeira experiência da lei que limita o uso da informática, sobre proteção de dados, sofreu forte influência da resolução 509/68, foi na Alemanha, em 07 de outubro de 1970, no Estado de Hesse, segundo Vittorio Frosini¹⁰⁷, o qual editou norma que limitava o controle sobre os acordos da administração pública uso da informática, continha dezessete artigos. Regulava a utilização dos centros de informática administrados pelas

¹⁰⁴ DELGADO, Lucrecio Rebollo – **Vida Privada Y Protección de Datos en la Unión Europea**. Madrid: Dykinson, 2008. p. 84.

¹⁰⁵ Idem – **Op. Cit.** p. 85.

¹⁰⁶ DELGADO, Lucrecio Rebollo – **Protección de Datos en Europea**. Madrid: Dykinson, [sd]. ISBN 978-84-9849-333-7, p. 63.

¹⁰⁷ FROSINI, Vittorio - Bancos de Datos Y Tutela de La Persona. [Em linha]. [sl]: **Revista de estudios políticos**. 30 (1982). p. 27. [Consult. 07 nov. .2018]. Disponível em WWW: <URL:https://dialnet.unirioja.es/servlet/articulo?codigo=26724>.

autoridades públicas de Hesse, e com uma preocupação quanto ao respeito a intimidade e o direito de controle sobre os dados. Em seguida a Suécia, promulgou Lei de proteção de dados - Data Lag, 1973, a França através da Lei 78-77 de 06 de janeiro de 1978 que foi recentemente modificada pela Lei n.º 2018-493, de 20 de junho de 2018, relativa à proteção dos dados pessoais visando adaptá-la ao novo Regulamento Geral sobre a Protecção de dados (RGPD) que entrou em vigor em maio de 2018¹⁰⁸.

A primeira lei orgânica e completa sobre a proteção da privacidade e sobre o controle dos bancos de dados, públicos e privados, foi emanada pelo Parlamento Sueco em 11 de maio de 1973; composta de vinte e cinco artigos e várias disposições transitórias; então, em 1979, o mesmo Parlamento confirmou algumas variações nesse texto¹⁰⁹. O entendimento passou a considerar que a pessoa de qualquer forma é sempre a titular legítima da informação. A informação integra um atributo da personalidade humana. É inconteste na doutrina e jurisprudência que os dados pessoais são direitos fundamentais de qualquer cidadão e têm sua proteção assegurada na Lei. Portugal foi o primeiro e um dos raros países a conferir dignidade constitucional à proteção de dados pessoais, na Constituição da República Portuguesa aprovada em 02 de abril de 1976.

Estreando, a Assembleia Geral das Nações Unidas em 10 de dezembro de 1948 proclamou a "Declaração Universal dos Direitos do Homem"¹¹⁰, primeiro instrumento jurídico de cunho internacional, onde já se exaltava, ainda que de forma acanhada, não tão explícita, uma vez que não se tinha ainda surgido alta tecnologia como os primeiros computadores, o direito do cidadão a proteção de dados pessoais através das leis, O artigo 12 garantia ao indivíduo à proteção da lei contra interferências e ataques na sua vida privada, da sua família, do seu lar, estendendo a proteção a sua correspondência.

A partir daí, seguindo essa rota tem-se a Europa na dianteira da atenção em relação a proteção de dados pessoais, já em função do avanço frenético das tecnologias de informação. Em 1967 o Conselho da Europa instituiu uma Comissão Consultiva que tinha o propósito do estudo das tecnologias da informação e o seu potencial de lesividade dos direitos das pessoas o que repercutiu diretamente na Resolução 509 de 1968 do Conselho da Europa, que versava sobre Direitos Humanos e novas conquistas científicas e técnicas.

¹⁰⁸ DELGADO, Lucrecio Rebollo – **Vida Privada Y Protección de Datos en la Unión Europea**. Madrid: Dykinson, 2008. p. 86.

¹⁰⁹ FROSINI, Vittorio - Bancos de Datos Y Tutela de La Persona. **Revista de estudios políticos**. 1982. p. 29.

¹¹⁰ DECLARAÇÃO UNIVERSAL DOS DIREITOS DO HOMEM – [Em linha]. [Consult. 22 out. 2018]. Disponível em <http://www.dhnet.org.br/direitos/deconu/textos/integra.htm>. Artigo 12. “Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques a sua honra e reputação. Todo o homem tem direito à proteção da lei contra tais interferências ou ataques”.

Maria Nieves de La Serna Bilbao¹¹¹, expressa que a citada resolução, embora não mencione a proteção de dados diretamente materializa a necessidade de adotar mecanismos de proteção que compreenda a vida privada e outros direitos fundamentais que podem ver-se afetados pelas TIC. A partir dela, se inicia muitos estudos que mostravam a preocupação pela relação existente entre a informática e a intimidade das pessoas e as implicações que aquelas teriam para os cidadãos, em especial no tratamento de dados pessoais. O final dos anos setenta e início dos anos oitenta, foi marcado pela ascensão galopante do uso da informática, que trouxe de forma implícita um reconhecimento do elevado grau de possibilidade de lesão a direitos da personalidade das pessoas envolvidas.

Em 1965, L Roberts y T. Meril, conectam-se pela primeira vez os computadores através de uma linha telefônica e constata a facilidade com que podem transmitir dados de um a outro, nascendo assim a ARPANET, através de usos militares, oferecendo correio eletrônico e transferência de arquivos dentro dos Estados Unidos, e em 1973 conseguem as primeiras conexões internacionais¹¹². Sendo a princípio computadores individuais, onde posteriormente o que está conectado são redes ou um conjunto de computadores. Prossegue Lucrecio Rebollo Delgado, que em 01 de janeiro de 1983 substitui-se o protocolo NCP por TCP/IP, que permanece até os dias de hoje, separando a parte militar surge a INTERNET que coexiste com a ARPANET até 1990, e um ano após aparece a World Wide Web como conhecemos, hoje¹¹³.

A partir da resolução 509/68, o Conselho da Europa manteve seus estudos e em 1973 o Comitê de Ministros do Conselho da Europa publica a resolução 73 de 26 de setembro de 1973 relativo a proteção da privacidade das pessoas físicas atinente a banco de dados eletrônicos do setor privado, garantindo a tutela dos indivíduos contra o processamento automatizado de seus dados. Em seguida, no ano subsequente entra em vigor a Resolução 74 de 20 de setembro de 1974 também referindo-se à precaução para evitar o uso indevido dos dados pessoais sendo que dentro da esfera pública do seu banco de dados.

A posição doutrinária assente que as legislações mencionadas configuram a origem real do movimento que nasceu na Europa, legitimando os princípios da proteção de dados pessoais que devem ser sempre avançados, indispensáveis e atinentes ao fim a que se destina.

Em 1974 entrou em vigor nos Estados Unidos a *Privacy Act*, que será o texto mais completo e melhor estruturado juridicamente até essa data, é o autêntico precursor das normas

¹¹¹ BILBAO, Maria Nieves de La Serna - **El Derecho a La Protección de Datos de Carácter Personal En Europa**. [Em linha]. [Consult. 30 out. 2018]. Disponível em WWW: <URL: http://ocw.uc3m.es/derecho-administrativo/derecho-de-las-tecnologias-de-la-informacion/material-de-clase-1/leccion_2.pdf>.

¹¹² DELGADO, Lucrecio Rebollo – **Vida Privada Y Protección de Datos en la Unión Europea**. 2008. p. 87

¹¹³ *Idem* - **Ibidem**.

posteriores sobre proteção de dados de caráter pessoal na Europa¹¹⁴. Essa Lei teve forte influência do escândalo Watergate, onde o Congresso Americano ao promulgá-la manifestou sua preocupação em restringir a vigilância e investigação ilegal de indivíduos por agências federais que haviam sido expostas durante o escândalo Watergate. E, de igual forma com o crescente uso de computadores que armazenava e recuperava dados pessoais dos indivíduos por meio de um identificador universal. Nessa ótica a referida lei anunciava quatro pilares relevantes, que podem ser resumidos em: limitar divulgação de registros identificáveis mantidos pelas agências; garantir aos indivíduos acesso ao registro mantido nas agências; assegurar o direito de solicitar a alteração dos registros abarcado nas agências e designar um código de prática de informações justas para que as agências cumpram os preceitos estatuídos de coleta, manutenção e disseminação¹¹⁵.

Posteriormente, em 1988 o *Privacy Act* de 1974, foi emendado pela Lei *Computer Matching and Privacy Act*¹¹⁶ que passou a salvaguardar direitos processuais dos indivíduos possibilitando-o refutar informações adversas, em relação a regular o uso de correspondência de computadores por órgãos federais envolvendo registros pessoalmente identificáveis mantidos em um sistema de registros sujeitos à Lei de Privacidade.

Portugal, aplaina de forma absoluta já na sua Constituição de 1977 o direito do cidadão de ter acesso aos dados informatizados que lhes digam respeito, admitindo a sua retificação e atualização, bem como o direito de conhecer a finalidade a que se destinam (artigo 35.º)¹¹⁷. Em 1991 Portugal publica a Lei de Proteção de Dados Pessoais a informática. A Espanha, em sua Constituição de 1978, não se apercebe uma alusão expressa ao direito fundamental de proteção de dados. O artigo 18.4. da Constituição Espanhola¹¹⁸ “diz respeito a uma limitação no uso da informática visando garantir a honra e a intimidade da pessoa e familiar dos seus cidadãos no exercício de seus direitos”. Entrementes foi promulgada a Lei Orgânica 5/1992¹¹⁹, de 29 de outubro, do Regulamento do Tratamento Automatizado de Dados Pessoais (LORTAD) que objetivava regular o tratamento automatizado dos dados de caráter pessoal que figurassem em

¹¹⁴ DELGADO, Lucrecio Rebollo – **Vida Privada Y Protección de Datos en la Unión Europea**. 2008. p. 87.

¹¹⁵ UNITED STATES OF AMERICA. **Privacy Act of 1974, 5 U.S.C. § 552**. [Em linha]. [Consult. 23 out. 2018]. Disponível em WWW: <URL:<https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1279>>.

¹¹⁶ UNITED STATES OF AMERICA. **Privacy Act of 1974, 5 U.S.C. § 552**. [s.d.].

¹¹⁷ PORTUGAL. Constituição Portuguesa. [Em linha]. [Consult. 28 out. 2018]. Disponível em WWW: <URL:<https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>>.

¹¹⁸ ESPANHA. Constituição Espanhola. [Em linha]. [Consult. 28 out. 2018]. Disponível em WWW: <URL:<https://www.tribunalconstitucional.es/es/tribunal/normativa/Normativa/CEportugu%C3%A9s.pdf>>.

¹¹⁹ ESPANHA. Lei Orgânica 5/1992, de 29 de outubro. De regulación del tratamiento automatizado de los datos de carácter personal [Em linha]. [Consult. 22 out. 2018]. Disponível em WWW: <URL:<https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189>>.

arquivos públicos ou privados, visando salvaguardar os direitos da personalidade contidos no artigo 18.4 da Constituição Espanhola. Verifica-se na referida Lei um caráter preventivo e não reparador, o que se propôs foi uma legislação que tencionava evitar que se produzisse prejuízos como resultado do uso indevido de dados e não visando a reparação a posteriori, que posteriormente foi derogada pela atual Lei Orgânica 15/1999, de 13 de dezembro, de Proteção de Dados Pessoais (LOPD). Tem-se também que Áustria, Dinamarca, Luxemburgo e Noruega, do mesmo modo, registraram leis sobre o tratamento de dados pessoais.

É pacífico na doutrina, consoante M^a Nieves de La Serna Bilbao¹²⁰, que a Resolução 509/68 fomentou o surgimento de diversas normas na Europa que tutelavam a proteção da vida privada das pessoas físicas, a proteção dos dados pessoais em diferentes esferas, médica, bancária, laboral, polícia, seguridade social entre outras recomendações foram desbravando. A Comissão elaborada no ano de 1973 intitulada “Uma política comunitária de informática” refletiu uma inquietude das instituições europeias com respeito ao emprego da informática e os direitos das pessoas sublinhando a necessidade de alcançar um consenso político que permitisse instaurar regras de base comum para evitar futuras divergências normativas que acarretasse uma atuação posterior de harmonização de legislação.

E a partir daí iniciou-se uma verdadeira caminhada marcada por diversas legislações de monta, de grande magnitude, sempre voltadas para garantir a proteção dos direitos das pessoas frente aos desafios dos avanços impetuoso da tecnologia canalizada para a informática, que crescia a passos largos, e que necessariamente fomentou a eclosão da Diretiva nos idos dos anos noventa, mais precisamente em 1995, Diretiva 95/46/CE, onde primeiramente foi desenvolvido um projeto da Diretiva em 27 de julho de 1990, alusivo à proteção das pessoas bem como o tratamento dos dados pessoais.

Em 1980 a Organização para Cooperação e desenvolvimento Econômicos, (OECD) ¹²¹, frente a chegada desenfreada da tecnologia da informação em diversos setores da sociedade, onde a informatização começou a dar seus primeiros passos, passando a valorizar o processamento de dados, estabeleceu as Diretrizes sobre a proteção da privacidade e fluxos transfronteiriços e dados pessoais a título de recomendações escorada em três princípios básicos: a democracia pluralista, respeito aos direitos humanos e economias de mercado abertas.

¹²⁰ BILBAO, Maria Nieves de La Serna - **El Derecho a La Protección de Datos de Carácter Personal En Europa**. [s.d.]. p. 5.

¹²¹ OECD. **Directrices de La OCDE Sobre Protección de La Privacidad Y Flujos Transfronterizos de Datos Personales** [Em linha]. p. 1. [Consult. 24 out. 2018]. Disponível em WWW: <URL:<https://www.oecd.org/sti/ieconomy/15590267.pdf>>.

Essas diretrizes emanadas objetivavam salvaguardar o respeito a privacidade, as liberdades individuais e a proteção de dados, alcançando tanto na esfera pública quanto na esfera privada.

Os princípios estabelecidos nas diretrizes da privacidade se caracterizam por sua clareza e flexibilidade de aplicação e por sua formulação, que é suficientemente geral para permitir sua adaptação às mudanças tecnológicas. Abrangem todos os meios de processamento de dados informatizados sobre indivíduos (de computadores locais a redes com complexas ramificações nacionais e internacionais). Todos os tipos de processamento de dados pessoais (desde a gestão de pessoas até a compilação de perfis de consumidores) e todas as categorias de dados (desde dados de tráfico até dados de conteúdo do mais trivial ao mais sensíveis). Tradução nossa.¹²²

Esmiçando os referidos princípios a serem seguidos pelos países membros da Europa, vê-se que abarcam um zelo com a proteção da privacidade e das liberdades individuais, a saber: princípio da limitação da recolha de dados, princípio da qualidade dos dados, princípio da especificação da finalidade, princípio da limitação do uso, princípio da salvaguarda da segurança, princípio da transparência, princípio da participação individual e o por último o princípio da responsabilidade¹²³.

O convênio 108 do Conselho da Europa de 28 de janeiro de 1981, que entrou em vigor em 01 de outubro de 1985, é considerado o primeiro dispositivo legal e internacional, que dispõe sobre a proteção de dados, visando fortalecer a proteção de dados e a proteção jurídica dos indivíduos em relação ao tratamento automatizado dos dados pessoais. Surge em decorrência de recomendação da Organização para a cooperação e desenvolvimento econômicos (OCDE) acerca da circulação internacional de dados pessoais garantindo a pessoa física o respeito aos seus direitos e liberdades fundamentais em relação ao tratamento automatizado dos dados de caráter pessoal, a proteção de dados. Princípios esses a serem seguidos por todos os estados signatários: princípio finalista, princípio da lealdade, princípio da exatidão, princípio da publicidade, princípio do acesso individual e princípio da seguridade¹²⁴. Pode se dizer que a vigência do convênio 108 do Conselho da Europa foi a estreia do uso universal do conceito de proteção de dados, onde a partir daí surgiram novas legislações.

Em seus considerando, assim dispõe, a inevitabilidade de harmonizar o princípio da livre circulação de informação e o respeito a vida privada (Preambulo da Convenção para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoa -

¹²² OCDE. **Directrices de La OCDE Sobre Protección de La Privacidad Y Flujos Transfronterizos de Datos Personales** [Em linha]. [Consult. 24 out. 2018]. Disponível em WWW: <URL:https://www.oecd.org/sti/ieconomy/15590267.pdf>.

¹²³ Idem – **Op. Cit.** p. 6-7.

¹²⁴ DELGADO, Lucrecio Rebollo – **Vida Privada Y Protección de Datos en la Unión Europea**. 2008. p.107.

OECD)¹²⁵. Abriga a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal, em ambas as esferas públicas ou privadas (artigo 1º). Já nessa época se previa a figura da autoridade controladora dos arquivos responsável por decidir a finalidade do arquivo automatizado, as categorias dos dados de carácter pessoal que deverão ser registradas e quais operações se aplicam (artigo 2, d)¹²⁶.

Lucrecio Rebollo Delgado¹²⁷ assenta que o texto do Convênio 108 do Conselho da Europa estabelece uma série de princípios básicos para a proteção de dados, aponta critérios que regulam seu fluxo e cria um Comitê Consultivo, a quem se confia a formulação de propostas para melhorar a aplicação da convenção. A introdução da Convenção reforça a proteção de dados, ou melhor, a proteção jurídica dos indivíduos com relação ao tratamento automatizado de dados de carácter pessoais que lhes dizem respeito.

Traz em seu bojo diversas características, tais como a exigência de veracidade e a correta utilização de dados, a proibição do tratamento automático de informações referentes a origem racial, opiniões públicas, crenças religiosas, saúde sexual, (tido como dados sensíveis) e condenação penitenciária, a segurança nos registros dos dados, o reconhecimento do direito por parte dos interessados em conhecer a existências de dados pessoais e a possibilidade de cancelar ou corrigi-los, a faculdade de recorrer uma vez detectada qualquer transgressão dos direitos antes mencionados¹²⁸.

O manual da legislação europeia sobre a proteção de dados, em relação ao convenio 108, assim consagra sua aplicabilidade:

que o Convênio 108 aplica-se a todos os tratamentos de dados pessoais realizados tanto pelo setor privado como pelo setor público, incluindo os tratamentos de dados efetuados pelas autoridades policiais e judiciárias. Protege as pessoas contra os abusos que podem acompanhar a recolha e o tratamento de dados pessoais e procura simultaneamente regular o fluxo transfronteiriço de dados pessoais. Quanto à recolha e tratamento de dados pessoais, os princípios estabelecidos na Convenção respeitam, em especial, à recolha e tratamento automatizado de dados de forma leal e lícita, armazenados para finalidades determinadas e legítimas, não podendo ser utilizados para fins incompatíveis com essas finalidades nem conservados por tempo superior ao necessário. Dizem também respeito à qualidade dos dados, estabelecendo, em especial, que têm de ser adequados, pertinentes e não excessivos (proporcionalidade), bem como exatos. Além de prever garantias relativas à recolha e tratamento de dados pessoais, a Convenção proíbe, na ausência de garantias jurídicas adequadas, o

¹²⁵ OCDE. **Directrices de La OCDE Sobre Protección de La Privacidad Y Flujos Transfronterizos de Datos Personales** [Em linha]. [Consult. 24 out. 2018]. Disponível em WWW: <URL:https://www.oecd.org/sti/ieconomy/15590267.pdf>.

¹²⁶ PORTUGAL. **Convenção 108. Para a Protecção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal**. [Em linha]. [Consult. 24 out. 2018]. Disponível em WWW: <URL:https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>.

¹²⁷ DELGADO, Lucrecio Rebollo – **Vida Privada Y Protección de Datos en la Unión Europea**. 2008. p. 106.

¹²⁸ PORTUGAL. **Convenção 108. Para a Protecção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal**. [s.d.].

tratamento de dados “sensíveis”, tais como dados sobre a raça, a opinião política, a saúde, as convicções religiosas, a vida sexual ou o registo criminal de uma pessoa¹²⁹.

O Convênio consagra o direito das pessoas a tomarem conhecimento da existência de informações a seu respeito, dando-lhe o direito de retificá-las caso seja de seu interesse¹³⁰. Reconhece-se a restrição de direitos imposta na lei quando estiver relacionado com interesses públicos de segurança nacional, que vão preponderar em detrimento do interesse privado, específico de cada pessoa.

A definição sobre proteção de dados, advém de um reconhecimento desde os idos da Carta dos Direitos Fundamentais da União Europeia, mais precisamente dos anos oitenta, face a expansão da tecnologia da informação através da informática, de uma faceta do direito da personalidade dos indivíduos, o direito à proteção dos dados pessoais. Tanto assim que eclode na sentença do Tribunal Federal Alemão em 1983, o direito à autodeterminação informativa, que consistia na capacidade do indivíduo de dispor de sua própria liberdade da forma que lhe convier, tendo o poder de decisão e controle.

Perseverando no caminhar pela história, em 25 de março de 1982, o governo alemão aprovou a Lei do Censo demográfico relativa à recolha de dados, onde os cidadãos deveriam responder a um questionário sobre a vida pessoal, condições de moradia, profissional, acadêmica. Ocorre que a real finalidade dos dados coletados não era meramente estatística, podendo ser utilizada por qualquer administração sempre que lhe fosse útil as suas funções. Não havia a garantia ao anonimato, já que qualquer pesquisa poderia disponibilizar quaisquer dados sobre pessoas ou associações de pessoas para finalidades diversas das que foram coletadas.

Todo esse movimento resultou com uma demanda judicial proposta, em Hamburgo pelas Advogadas Dr^a Gisela Wild e Dr^a Maja Stadler-Euler, em 1983 junto ao Tribunal Federal Alemão que declarou a inconstitucionalidade de alguns preceitos da Lei do Censo demográfico, relativos a transmissão de dados entre o Estado, regiões e câmaras pelo fato de lesarem direitos fundamentais do cidadão: direito ao livre desenvolvimento da personalidade em relação ao direito da dignidade da pessoa humana, direito à livre expressão de opinião e o direito a garantia processual¹³¹. A pedra de toque dessa sentença foi a introdução de um novo conceito

¹²⁹ EUROPA (AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA E CONSELHO DA EUROPA). **Manual da Legislação Europeia sobre Proteção de Dados**. [Em linha]. p.16. [Consult. 01 nov. 2018]. Disponível em <<https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-pt.pdf>>.

¹³⁰ *Idem* – ***Ibidem***.

¹³¹ HIGUERAS, Manuel Heredero - **La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del censo de población**. [Consult. 14 nov. 2018]. Disponível em WWW: <[URL:https://revistasonline.inap.es/index.php?journal=DA&page=article&op=view&path%5B%5D=4687](https://revistasonline.inap.es/index.php?journal=DA&page=article&op=view&path%5B%5D=4687)>.

denominado autodeterminação informativa, onde a pessoa atua com livre autodeterminação na qualidade de integrante de uma sociedade livre.

A sentença elucida o direito à autodeterminação informativa como sendo uma faculdade do indivíduo de decidir basicamente por si só e dentro de que parâmetros pode revelar situações de sua própria vida, onde pressupõe, também, as condições das modernas técnicas de tratamento da informação¹³². Avança, do mesmo modo, asseverando que a autodeterminação informativa não tem garantia de ser sem limite, ou seja, não existe soberania absoluta e ilimitada do indivíduo sobre seus dados. O Estado pode ter acesso aos dados relativos à pessoa igualmente podendo utilizá-lo reiteradamente sobretudo quando se depara com conflitos de interesses, devendo sopesar a vontade do indivíduo em se manter no anonimato em confronto com o interesse da coletividade em obter informações¹³³.

O acordo de Schengen de 14 de junho de 1985¹³⁴, tinha por finalidade suprimir gradualmente os controles das fronteiras comum em relação ao respeito à circulação das pessoas facilitando o transporte e a circulação das mercadorias.

O capítulo três inserido no título Sistema de Informação Schengen do referido acordo trata da protecção dos dados pessoais e segurança dos dados no âmbito do sistema de informação Schengen. Os artigos 102 a 118 norteiam aspectos da protecção de dados, impondo medidas de segurança, validando os princípios que devem permear todo o processo de tratamento de dados, exatidão, atualidade e licitude, certificando o direito ao acesso, retificação e eliminação de dados. Constata-se ainda, que o acordo de Schengen fortalece a preocupação com a protecção de dados pessoais quando dispôs um título específico para tratar sobre o tema. O título VI titulado Protecção de dados Pessoais sendo abordado nos artigos 126 a 130, onde visam garantir a protecção das pessoas face ao tratamento automatizado dos dados pessoais, assegurando um nível de protecção pelo menos igual ao decorrente dos princípios da Convenção do Conselho da Europa de janeiro de 1981¹³⁵.

¹³² HIGUERAS, Manuel Heredero - **La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del censo de población**. [s.d.]. p. 139-59. [Consult. 14 nov. 2018]. Disponível em WWW:

<URL:https://revistasonline.inap.es/index.php?journal=DA&page=article&op=view&path%5B%5D=4687>.

¹³³ SENTENCIA DE 15 DE DICIEMBRE DE 1983, DEL TRIBUNAL CONSTITUCIONAL FEDERAL ALEMÁN, LEY DEL CENSO. [Em linha]. [Consult. 14 nov. 2018]. Disponível em WWW: <URL:http://www.derecho-chile.cl/sentencia-de-15-de-diciembre-de-1983-del-tribunal-constitucional-federal-aleman-ley-del-censo/>.

¹³⁴ EUROPA. **Convenção de Aplicação do Acordo de SCHENGEN, de 14 de junho de 1985**. [Em linha]. [Consult. 16 nov. 2018]. Disponível em WWW: <URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:42000A0922(02)&from=ES>.

¹³⁵ EUROPA. **Convenção de Aplicação do Acordo de SCHENGEN, de 14 de junho de 1985**. [s.d.].

Prosperando e esmerando-se ao longo do tempo, a década de 90 foi sublinhada por grandes mudanças no sentido de se produzir uma concepção mais tangível sobre a proteção de dados. Tem-se efetivamente a primeira recomendação de sistematização de proteção de dados. Em 1992, em 07 de fevereiro, foi assinado o Tratado de Maastrich, que instituiu política e economicamente a União Europeia, que consistiria num mercado comum de uma União econômica, uma única moeda, e, onde os cidadãos dos estados membros que a compõe poderiam circular livremente, incluindo a circulação de dados pessoais entre os estados membros.

Dentro dessa evolução galopante, a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho de 24 de outubro de 1995, após cinco anos de negociação da primeira proposta de regulação apresentada pela Comissão, surgiu da constatação da necessidade de uma legislação a nível supranacional que unificasse a disparidade legislativa e estabelecesse meios de atualização jurídica com respeito as possibilidades técnicas já existentes¹³⁶. Cria um marco regulador destinado a estabelecer um equilíbrio entre um nível elevado de proteção da vida privada das pessoas e a livre circulação de dados pessoais dentro da Europa¹³⁷.

Pode ser considerada a quarta geração do direito a proteção de dados pessoais, no que diz respeito ao tratamento e a circulação desses dados, foi um dos mais significativos instrumentos jurídicos, sofrendo forte ascendência das Diretrizes da Organização para Cooperação e desenvolvimento econômico (OCDE), do ano de 1980 e do Convenio 108 do Conselho da Europa que asseverava a proteção das pessoas com respeito ao tratamento automatizado dos dados pessoais. Observa-se no considerando onze (11) da Diretiva 95/46/CE¹³⁸ que o princípio do direito à vida privada ampliou os princípios contidos na convenio 108 do Conselho da Europa de 28 de janeiro de 1981, concernente à proteção das pessoas no que dizia respeito ao tratamento automatizado de dados pessoais.

A Diretiva 95/46/CE, a quarta geração, dispõe em seu artigo 1º que os Estados-membros signatários deverão afiançar a proteção das liberdades e dos direitos individuais das pessoas singulares, em especial o direito à vida privada relativo ao tratamento de dados pessoais. Verifica-se que a Diretiva inovou visando a sua eficácia em relação a alguns aspectos presentes

¹³⁶ DELGADO, Lucrecio Rebollo – **Vida Privada Y Protección de Datos en la Unión Europea**. 2008. p. 94.

¹³⁷ “Crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea”. BILBAO, Maria Nieves de La Serna - **El Derecho a La Protección de Datos de Carácter Personal En Europa**. [s.d.]. p. 11.

¹³⁸ UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho - **relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. 24 de outubro de 1995. [Em linha]. [Consult. 01 nov. 2018]. Disponível em WWW: <URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>.

nas normas anteriores: criou-se a figura do encarregado do tratamento, o direito de oposição da pessoa em causa, o desenvolvimento de sistemas de auto regulação setorial, o regime de fluxo de transferência de dados pessoais para países terceiros, fora do âmbito da comunidade europeia.

O artigo 3º demarca o âmbito de aplicação da Diretiva que se destina ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados ¹³⁹.

Os princípios relativos à qualidade dos dados e a legitimidade do tratamento dos dados estão realçados no artigo 6º e 7º da Diretiva. Em relação a qualidade dos dados tem-se cinco princípios básicos: os dados devem ser tratados de forma leal e lícita; a recolha tem uma finalidade determinada, explícita e legítima; os dados devem ser adequados, pertinentes e não excessivos em relação a finalidade da recolha; exatos e se necessário, atualizados, sendo que os dados inexatos ou incompletos deverão ser retificados ou suprimidos; os dados deverão ser conservados de forma que se possa permitir a identificação das pessoas durante o período necessário para atingir a finalidade a que se propõe.

Nota-se que o artigo 7º da Diretiva é exaustivo quando estabelece que o tratamento de dados pessoais só pode ser efetuado se obedecer aos princípios elencados: o consentimento do interessado for de forma inequívoca; o tratamento for necessário para execução de um contrato onde o interessado é parte; igualmente pode efetuar o tratamento se necessário for para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; o tratamento seja vital para proteger interesses do interessado; se for necessário para a execução de interesse público ou o exercício da autoridade pública conferido ao responsável pelo tratamento ou a um terceiro a quem os dados sejam comunicados; e por fim se for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou terceiros a quem os dados sejam comunicados, no caso de não prevalecer os interesses ou os direitos e liberdades fundamentais da pessoa em causa ¹⁴⁰.

Verifica-se uma peculiaridade na Diretiva 95/46/CE com a previsão legal em seu artigo 29 da criação de um grupo de proteção das pessoas no tocante ao tratamento de dados pessoais. Esse grupo tem como característica ser consultivo e independente e é constituído por um representante da autoridade ou autoridades de controle designadas por cada Estado-membro. O

¹³⁹ UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho - **relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. 24 de outubro de 1995. [Em linha]. [Consult. 01 nov. 2018]. Disponível em WWW: <URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>.

¹⁴⁰ *Idem* – ***Ibidem***.

objetivo desse grupo é analisar demandas que dizem respeito à operacionalidade da Diretiva com o intuito de garantir uma maior homogeneidade, em sua aplicação, pelos estados membros que formam a Comunidade Europeia.

Dois anos mais tarde, em função de uma necessidade premente de salvaguardar o tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações por parte da União Europeia, surge a Diretiva 97/66/CE¹⁴¹, de carácter mais genérico, que obriga os Estados membros a criação de normas para garantir a confidencialidade das comunicações através das redes públicas¹⁴². Tendo como objetivo primordial o estabelecimento em toda a União Europeia de um nível equivalente de protecção das liberdades e direitos fundamentais e em particular, o direito a intimidade no que se refere ao tratamento de dados pessoais no setor das telecomunicações¹⁴³.

A Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de Julho de 2002¹⁴⁴ relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas revogou a Diretiva 97/66/CE, face a eclosão dos meios de comunicação eletrônicos através da internet desencadeando a possibilidade de novos riscos à privacidade no que tange aos dados pessoais dos indivíduos.

O artigo 3º dispõe o serviço abrangido pela Diretiva 2002/58/CE, sendo aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações electrónicas publicamente disponíveis nas redes públicas de comunicações da Comunidade.

Em 2001, foi aprovado o regulamento CE/45/2001 do Parlamento Europeu e do Conselho de 18 de dezembro de 2000¹⁴⁵ alusivo à protecção das pessoas físicas quanto ao tratamento de dados pessoais pelas instituições e organismos comunitários e a livre circulação de dados. Da mesma forma criou uma autoridade europeia independente de supervisão para assegurar a devida execução das disposições relativas a protecção de dados pelas instituições e os organismos da União Europeia, como impunha a Diretiva 95/46/CE. Emerge, de igual forma,

¹⁴¹ UNIÃO EUROPEIA. Directiva 97/66/CE do Parlamento Europeu e do Conselho - **relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações**. 15 de Dezembro de 1997. [Em linha]. [Consult. 15 nov. 2018]. Disponível em WWW:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31997L0066&from=PT>.

¹⁴² DELGADO, Lucrecio Rebollo – **Vida Privada Y Protección de Datos en la Unión Europea**. 2008. p. 94.

¹⁴³ DELGADO, Lucrecio Rebollo – **Protección de Datos en Europea**. [s.d.]. p. 71.

¹⁴⁴ UNIÃO EUROPEIA. Directiva 2002/58/CE do Parlamento Europeu e do Conselho. **Relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas** 12 de Julho de 2002. [Em linha]. [Consult. 18 mar. 2019]. Disponível em WWW:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=EN>.

¹⁴⁵ UNIÃO EUROPEIA. Regulamento CE/45/2001 do Parlamento Europeu e Conselho de 18 de dezembro de 2000. **Relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados**. [Em linha]. [Consult. 18 mar. 2019]. Disponível em WWW:URL:https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32001R0045>.

a figura do Supervisor Europeu de Proteção de Dados, como mais um meio ofertado ao cidadão em casos de ofensas por parte das empresas ou organismos em relação a proteção de dados.

O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016¹⁴⁶, que passou a vigor a partir de 25 de maio de 2018 em todos os Estados-Membros da União Europeia, revogou a Diretiva 95/46/CE. Ressaltando-se que as matérias de que trata o Regulamento não são novas, pois estavam inseridas na Diretiva 95/46. O Regulamento Geral sobre a Proteção de Dados estabelece regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e a livre circulação desses dados (artigo 1º), assegurando uma proteção uniforme no que fiz respeito ao tratamento dos dados das pessoas singulares no interior da União.

O Regulamento 2016/679, surge após 4 anos de estudos e discussões, onde alvejavam uma padronização das leis de privacidade de dados em toda a Europa, com regras mais rígidas propiciando a proteção da privacidade de dados dos cidadãos da União Europeia e visavam remodelar a forma como as organizações públicas ou privadas tratam os dados pessoais coletados, em função da globalização e do crescimento galopante de altas tecnologias.

O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016¹⁴⁷, conhecido como Regulamento Geral sobre a Proteção de Dados (RGPD), hoje em vigor em toda a Europa pelos seus Estados Membros emergiu de um cenário onde a frenética evolução de novas tecnologias que bem como a facilidade de acesso ao mundo cibernético aflorou nos internautas o desejo de minutos de celebridade, e, não só a superexposição, mas também, passaram a socializar seus dados pessoais na rede, fazendo com que o tráfego de conteúdos midiáticos desaguassem em empresas privadas que sem qualquer reserva disseminam os dados coletados, com fins meramente comerciais.

As pessoas, sem qualquer embaraço alimentam as redes sociais, os aplicativos etc. com suas informações, de cunho privado, mas que por força da internet adquirem uma publicidade facilmente ventilada aos quatro cantos do universo. Em função desse quadro, foi necessária uma intervenção mais proativa da União Europeia no sentido de dar maior segurança jurídica aos cidadãos, fazendo com que tenham mais controle sobre seus dados pessoais, fornecendo de forma expressa seu consentimento, não podendo ser considerado sua omissão como aquiescência. Da mesma forma, o titular dos dados tem direito de dispor de seus dados pessoais

¹⁴⁶ UNIÃO EUROPÉIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE**. [Em linha]. [Consult. 18 mar. 2019]. Disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679>>.

¹⁴⁷ *Idem* – **Op. Cit.**

e a qualquer momento, solicitar a retificação, com direito ao apagamento dos dados que entender, direito a exigir a limitação do tratamento, direito de se opor e até o direito de portabilidade dos seus dados.

Uma das principais inovações diz respeito ao alcance da Regulamento Geral de Proteção de Dados, aplicação territorial, uma vez que o item 1 do artigo 3º, é explícito no sentido de que todos os estabelecimentos que operam dados pessoais, independe de o tratamento ocorrer dentro ou fora da União estarão abrangidos pelo Regulamento, ou seja relativo ao fluxo de dados transfronteiriços.

Não resta mais nenhuma dúvida de que o direito à proteção de dados de caráter pessoal é um direito fundamental de todos os cidadãos e que a livre circulação desses dados de diversas formas é um fato incontestável, fruto da velocidade com que a tecnologia se desenvolve e os efeitos da globalização, onde inexiste barreiras fronteiriças. À vista disso, frisa o considerando quatro do RGPD¹⁴⁸, onde o direito à proteção de dados pessoais não é absoluto; devendo ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade.

O grau de “intimidade” da informação pessoal deve ser avaliado numa relação em que seja considerado o princípio da finalidade, ou seja a razão que justifica o tratamento dos dados. O princípio da finalidade desempenha várias funções dentro da proteção de dados. Por um lado, garante que a recolha de informação não é “cega” às suas consequências. Ou seja. Os tratamentos de dados pessoais só podem verificar-se quando uma situação ou um conjunto de situações fácticas o justificar¹⁴⁹.

2.2 Os pilares das normas de proteção de dados pessoais

Os três aspectos centrais de qualquer lei de proteção de dados pessoais, de acordo com Ricardo Bruno Bioni¹⁵⁰, é o que chama de tripé da proteção dos dados pessoais: conceito de dados pessoais, dados anônimos e consentimento do titular dos dados pessoais. Segundo o autor, os dados pessoais e os dados anônimos deverão ser sempre o alvo de qualquer legislação

¹⁴⁸ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE**. [Em linha]. [Consult. 18 mar. 2019]. Disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN>>.

¹⁴⁹ PINHEIRO, Patricia Peck – **Proteção de Dados Pessoais Comentários à Lei 13.709/2018 (LGPD)**. São Paulo: Saraiva Educação, 2018. ISBN 978-85-53605-28-6, p. 806.

¹⁵⁰ BIONI, Bruno RICARDO - **Xequemate o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPOPAI, 2015. p. 10-1.

relacionada a proteção de dados pessoais, enquanto o consentimento, é a pedra angular, é a base de todas as normas nos mais diferentes países.

2.2.1 Dados pessoais

Os dados pessoais são os que alimentam e movimentam tal economia e, mais do que isso, são a base de sustentação e ativo estratégico de uma série de modelos de negócios e para formulação de políticas públicas. Nesse contexto, normas de proteção de dados pessoais sempre tiveram dupla função de não só garantir a privacidade e outros direitos fundamentais, mas também fomentar o desenvolvimento econômico.¹⁵¹

A intelecção do conceito de dado pessoal e, por conseguinte, das estratégias regulatórias possíveis para a sua definição é algo fluido, que pode ser esclarecido a partir da dinâmica de conceitos básicos de sistemas de informação e de banco de dados.¹⁵² Um conceito de dado só se torna propriamente uma informação quando agrega ao seu conteúdo a identificação da pessoa a que se refere, e daí permite interpretações.¹⁵³ Essa informação, a princípio atomizada, organizada dentro de um contexto e com objetivos minimamente definidos transforma-se em conhecimento.¹⁵⁴

O “dado” apresenta conotação um pouco mais primitiva e fragmentada, como observamos por exemplo em um autor que o entende como uma informação em estado potencial, antes de ser transmitida¹⁵⁵; o dado estaria associado a uma espécie de “pré-informação”, anterior à interpretação e ao processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição, e mesmo nos efeitos que esta pode apresentar ao seu receptor.¹⁵⁶

Nesse contexto, o dado transformado em conhecimento transforma-se em Poder para que o detém e pode significar constrangimentos e até subjugação para aquele que se torna um pouco mais desvelado.¹⁵⁷

¹⁵¹ BIONI, Bruno RICARDO – **Proteção de Dados Pessoais a função e os limites do consentimento**. 2019. p. 108.

¹⁵² *Idem* – **Op. Cit.** p. 69.

¹⁵³ TRUTE apud SILVA, Carlos Bruno Ferreira da – **Proteção de Dados e Cooperação Transacional: Teoria e Prática na Alemanha, Espanha e Brasil**. Belo Horizonte: Arraes, 2014. ISBN 978-85-8238-056-7, p 825.

¹⁵⁴ HOFFMANN-RIEM apud SILVA, Carlos Bruno Ferreira da – **Proteção de Dados e Cooperação Transacional: Teoria e Prática na Alemanha, Espanha e Brasil**. 2014. p. 12.

¹⁵⁵ RAYMOND apud DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar. 2006. p. 155.

¹⁵⁶ DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar. 2006. p. 152.

¹⁵⁷ SILVA, Carlos Bruno Ferreira da – **Proteção de Dados e Cooperação Transacional: Teoria e Prática na Alemanha, Espanha e Brasil**. Belo Horizonte: Arraes, 2014. ISBN 978-85-8238-056-7, p. 24.

A orientação reducionista baseia-se em uma lógica restritiva pela qual dado pessoal é uma informação que deve estar associada a uma pessoa específica. Ele deve ser um signo que permita estabelecer de forma imediata ou direta um vínculo com o seu titular, individualizando-o de forma precisa¹⁵⁸. Enquanto a expansionista aposta em uma lógica mais flexível, que desconsidera a associação exata entre uma informação e uma pessoa. Dado pessoal pode ser qualquer tipo de informação que permita a sua identificação, ainda que o vínculo entre o dado e um indivíduo não seja estabelecido de prontidão, mas de forma mediata ou indireta.¹⁵⁹

Dados e informação não se equivalem.¹⁶⁰ Daí se afirmar que a informação é abrangente e se refere a todo conteúdo material ou imaterial a respeito de uma situação ou pessoa. Já a definição de “dados” é restrita, e está contida no conceito de informação; é a veiculação material da informação na sociedade globalizada. As informações são armazenadas em dados e circulam pela rede mundial de computadores, ou por meio de sistemas internos gerenciados por empresas de cadastros ou por verdadeiros bancos de dados, os quais detêm informações pessoais ou públicas dos indivíduos.¹⁶¹

Os dados pessoais passam a ser os intermediários entre a pessoa e a sociedade, prepostos nem sempre autorizados e capazes, e é justamente isto que produz como efeito a perda de controle da pessoa sobre o que se sabe em relação a si mesma – o que, em última análise, representa uma diminuição na sua própria liberdade¹⁶².

A análise elaborada por Bruno Ricardo Bioni partiu do exemplo de uma base de dados relacionais, onde a simples inclusão simples ou exclusão de colunas ou linhas nessa base de dados, estruturada em formato de uma tabela, são fatores determinantes para um dado ser adjetivado como pessoal¹⁶³. A definição do conceito de dados pessoais pode seguir uma orientação expansionista (pessoa identificável) ou reducionista (pessoa identificada), onde ambas demandam uma análise contextual de onde está inserido um dado, a fim de aferir o seu grau de identificabilidade para compreender se uma determinada informação está relacionada a uma pessoa identificada ou identificável¹⁶⁴.

¹⁵⁸ BIONI, Bruno RICARDO - **Xequemate o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. 2015. p. 17.

¹⁵⁹ *Idem - Ibidem*.

¹⁶⁰ *Idem – Op. Cit.* p. 36.

¹⁶¹ MORAES, Melina Ferracini - **Direito ao Esquecimento na Internet**. Curitiba: Juruá, 2018. p. 42.

¹⁶² DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar. 2006. p. 181.

¹⁶³ BIONI, Bruno RICARDO - **Xequemate o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. 2015. p. 4.

¹⁶⁴ *Idem - Ibidem*.

O Regulamento Geral da Proteção de Dados em seu artigo 4º¹⁶⁵ - define dados pessoais como informação relativa a uma pessoa singular identificada ou identificável (titular dos dados); sendo considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiologia, genética, mental, econômica, cultural ou social dessa pessoa singular.

A Europa, com a implantação do Regulamento desencadeou nos demais países do mundo, um “efeito dominó”, visto que passou a exigir que os demais países e as empresas que buscassem manter relações comerciais com a UE também deveriam ter uma legislação do mesmo nível que o GDPR, a fim de evitar sanções, tais como dificultando a possibilidade de fazer negócios com os países da União Europeia.

No Brasil, despontou a Lei 13.709 de 14 de agosto de 2018, recepcionada por ser uma legislação extremamente técnica e fortemente inspirada no Regulamento Europeu. Reuniu uma série de itens de controle para assegurar o cumprimento das garantias previstas, cujo lastro se funda na proteção dos direitos humanos.¹⁶⁶ A legislação brasileira aclara em seu artigo 5º a definição de dados pessoais como a informação relacionada a pessoa natural identificada ou identificável, aderindo ao mesmo conceito da legislação europeia.

A prática do direito à informação deu origem à criação de uma categoria específica de dados, a dos dados sensíveis. Alguns destes dados seriam as informações sobre raça, credo político ou religioso, opções sexuais, o histórico médico ou os dados genéticos.¹⁶⁷ A própria seleção de quais seriam estes dados considerados sensíveis provém da valoração de que a circulação de determinadas espécies de informação apresentaria um elevado potencial lesivo aos seus titulares, em uma determinada configuração social.¹⁶⁸

O dado a ser considerado nas legislações será eminentemente o dado pessoal, aquele já transformado em informação específica sobre um indivíduo, e assim devendo ser submetida ao

¹⁶⁵ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE**. [Em linha]. [Consult. 18 mar. 2019]. Disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN>>.

¹⁶⁶ PINHEIRO, Patricia Peck – **Proteção de Dados Pessoais Comentários à Lei 13.709/2018 (LGPD)**. 2018. p. 18.

¹⁶⁷ DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar. 2006. p. 160-1.

¹⁶⁸ ZENO-ZENCOVICH *apud* DONEDA, Danilo Cesar Maganhoto - **Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade**. [Em linha]. [Consult. 15 fev. 2018]. Disponível em WWW:<URL:<http://www.egov.ufsc.br/portal/sites/default/files/anexos/8196-8195-1-PB.htm>>.

interesse e à regulação jurídica. Pelo contrário, quando o dado não estiver ligado a uma pessoa explicitar-se-á a sua anonimização ou a sua existência como mero dado estatístico.¹⁶⁹

2.2.2 Anonimização e pseudonimização de dados

Inicialmente, se faz necessário demonstrar a diferença entre os dois conceitos anonimização e pseudonimização para melhor entender suas implicações nas normas vigentes em especial no Regulamento em vigor em toda a Europa, fazendo também um comparativo com a legislação do Brasil que entrará em vigor em fevereiro de 2020.

A expressão “anonimização” é ela própria vaga, uma vez que abrange uma diversidade de técnicas que podem ser usadas para converter dados pessoais em dados anonimizados¹⁷⁰. Partindo da definição do Grupo de Trabalho sobre a proteção de Dados do artigo 29.º dados anonimizados são dados relativos a uma pessoa identificada ou identificável que não pode, razoavelmente, voltar a ser identificada ou identificável. O critério da razoabilidade significa que o processo de anonimização deve ser suficientemente robusto, de tal modo que a reversão deste processo seja “razoavelmente impossível”.¹⁷¹

Danilo Doneda¹⁷², elucida o conceito de dado anônimo quando este se refere a uma pessoa indeterminada. Anonimização de dados pessoais como a retirada do vínculo da informação com a pessoa a qual se refere. Prossegue nessa linha, inferindo que o “dado anônimo ainda pode apresentar-se útil em outras hipóteses, como aquela na qual possibilita a comunicação e expressão de sujeitos que estariam impedidos, por vínculos e limitações políticas e sociais, de exprimir-se livremente”.

Dados anonimizados são excluídos da proteção jurídica do RGPD, conforme depreende-se do considerando 26 que firma entendimento no sentido de que os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado, inclusive para fins estatísticos ou de investigação. O dado sendo anônimo, já se sabe de antemão que não é possível identificar o titular dos dados pessoais. Quem será o titular que terá o seu

¹⁶⁹ SILVA, Carlos Bruno Ferreira da – **Proteção de Dados e Cooperação Transacional: Teoria e Prática na Alemanha, Espanha e Brasil**. 2014. p. 24.

¹⁷⁰ RUIVO, Inês de Castro - **Anonimização de dados pessoais: o que deve saber**. Portugal: Coluna Jurídica, 2016. p. 16.

¹⁷¹ *Idem* – **Op. Cit.** p. 16.

¹⁷² DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar. 2006. p. 157-8.

direito violado se esses dados anônimos forem utilizados? Não se tem como saber quem é o titular dos dados anônimos. Se o dado já é anônimo na sua composição, inviável a identificação de quem é o titular.

O artigo 4º item 5 do Regulamento Geral de Proteção de Dados¹⁷³ da Europa, clarifica a definição do que vem a ser Pseudonimização:

O tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

A pseudonimização funciona como uma técnica a ser lançada pelo responsável pelo tratamento e o subcontratante para proteger e garantir a segurança dos titulares dos dados pessoais conforme disposto nos artigos 25.º 1 e artigo 31.º 1. Alicerçado no considerando 28 do RGPD¹⁷⁴: “A aplicação da pseudonimização aos dados pessoais pode reduzir os riscos para os titulares de dados em questão e ajudar os responsáveis pelo tratamento e os seus subcontratantes a cumprir as suas obrigações de proteção de dados. A introdução explícita da “pseudonimização” no presente regulamento não se destina a excluir eventuais outras medidas de proteção de dados”. Dados pseudonimizados têm a proteção do RGPD.

Cada vez mais, as atividades de processamentos de dados têm ingerência na vida das pessoas. Hoje vivemos em uma sociedade e uma economia que se orientam e movimentam a partir desses signos identificadores do cidadão.¹⁷⁵

Daniel J. Solove¹⁷⁶ qualifica o novo tipo de identidade como dossiês digitais, consistentes em uma coleção dados detalhados sobre um indivíduo. Hoje através do uso de computadores, dossiês estão sendo construídos sobre todos nós. Existem centenas de empresas que estão construindo gigantescas bases de dados de perfis psicológicos, acumulando dados sobre a raça, o gênero, a renda, os hobbies e as compras de um indivíduo. Fragmentos de dados da nossa existência diária estão agora sendo reunidos e analisados - para investigar origens,

¹⁷³ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE**. [Em linha]. [Consult. 18 mar. 2019]. Disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN>>.

¹⁷⁴ FAZENDEIRO, Ana – **Regulamento Geral sobre a Proteção de Dados**. 2.ª ed. Coimbra: Almedina, 2018. ISBN 978-972-40-7154-1, p. 78.

¹⁷⁵ BIONI, Bruno RICARDO – **Proteção de Dados Pessoais a função e os limites do consentimento**. 2019. p. 65.

¹⁷⁶ “A dossier is a collection of detailed data about an individual. There are hundreds of companies that are constructing gigantic databases of psychological profiles, amassing data about an individual’s race, gender, income, hobbies, and purchases. Shards of data from our daily existence are now being assembled and analyzed—to investigate backgrounds, check credit, market products, and make a wide variety of decisions affecting our lives”. SOLOVE, Daniel J. - **The Digital Person Technology and Privacy in the Information Age**. 2004. p. 1.

verificar crédito, comercializar produtos e tomar uma ampla variedade de decisões que afetam nossas vidas. Mesmo que não estejamos conscientes disso, o uso de dossiês digitais está dando forma as nossas vidas¹⁷⁷. (Tradução nossa).

Os dados pessoais não estão relacionados somente com a privacidade, transitando dentre mais de uma das espécies dos direitos da personalidade. Seria contraproducente e até mesmo incoerente pensar a proteção de dados pessoais somente sob as lentes do direito à privacidade. O eixo da privacidade está ligado ao controle de informações pessoais do que seja algo íntimo ou privado do sujeito¹⁷⁸.

Pablo Lucas Murillo de la Cueva¹⁷⁹, leciona que o controle que esse direito fundamental nos oferece repousa em dois elementos principais. A primeira é a do consentimento dos afetados como condição de legalidade das atividades de captura e utilização de dados pessoais por terceiros. Consentimento inequívoco, livre e informado que permite que a pessoa a quem se referem autodeterminar-se informativamente. No entanto, é claro que, em certas ocasiões, deve ser possível processar informações pessoais sem a autorização da parte afetada. Por essa razão, e aí vem o segundo elemento, a lei pode expressamente autorizá-lo, seja de um modo geral, quando as circunstâncias são previstas por ele, ou caso a caso. Assim, consentimento e autorização legal são os títulos que justificam o processamento de dados pessoais.

2.2.3 Consentimento - o baluarte da proteção de dados pessoais como forma de empoderar o titular dos dados pessoais

A importância do consentimento vem reforçada por sua menção expressa tanto na Carta de Direitos Fundamentais da União Europeia¹⁸⁰ como no texto da Constituição Europeia aludindo em ambos os artigos o tratamento de dados de modo leal, para fins concretos e sobre a base do consentimento da pessoa afetada em virtude de outro fundamento legal previsto pela lei. Reconhecendo o direito da pessoa ao acesso de seus dados e possibilitando a sua retificação, (artigo 8º).

¹⁷⁷ “Even if we’re not aware of it, the use of digital dossiers is shaping our lives. Companies use digital dossiers to determine how they do business with us; financial institutions use them to determine whether to give us credit; employers turn to them to examine our backgrounds when hiring; law enforcement officials draw on them to investigate us; and identity thieves tap into them to commit fraud”. SOLOVE, Daniel J. - **The Digital Person Technology and Privacy in the Information Age**. 2004. p. 3.

¹⁷⁸ BIONI, Bruno RICARDO – **Proteção de Dados Pessoais a função e os limites do consentimento**. 2019. p. 66.

¹⁷⁹ LUCAS, Pablo Murillo de La Cueva - **O direito à autodeterminação informativa**. Madrid: Tecnos, 1990. p. 207.

¹⁸⁰ EUROPA. Carta de Los Derechos Fundamentales de la Unión Europea (2000/C 364/01). **Diário Oficial de las Comunidades Europeas** [Em Linha]. [Consult. 18 abr. 2019]. Disponível em WWW:<URL: http://www.europarl.europa.eu/charter/pdf/text_es.pdf>.

O consentimento é o primeiro pilar das normas de proteção de dados, onde a liberdade e dignidade humanas se apresentam nesse espaço da nossa existência.¹⁸¹ O consentimento, figura e prevalece como protagonista ao longo de todo seu ciclo evolutivo.¹⁸² É considerado por um dos teóricos espanhóis que assevera “*es la piedra angular a partir del cual se construye el sistema de protección de datos personales*”.¹⁸³

Tanto assim que em 1983, já se vislumbrava a importância crucial da manifestação da vontade do titular de forma expressa e clara dos dados para a sua utilização, onde a partir de um histórico julgamento, no Tribunal Constitucional Federal Alemão, do caso envolvendo a “Lei do Censo” (originalmente denominado *Volkszählungsurteil*), em que foi julgada inconstitucional a lei que determinava o recenseamento geral da população, o qual tinha objeto a coleta de dados para confrontá-los com os existentes no registro civil e repassá-los a autoridades públicas. Houve o reconhecimento do direito fundamental à autodeterminação informativa sobre os dados de caráter pessoal (originalmente denominado *Recht auf informationelle selbstbestimmung*), estabelecendo um corolário do direito geral de personalidade e dignidade humana¹⁸⁴. Este julgamento é considerado um marco para a proteção jurídica de dados pessoais, visto que significou o direito que os indivíduos passaram a ter de decidir quando e em que medida a informação pessoal pode ser publicada.¹⁸⁵

Quem desconhece quem, o que, e quando conhece sobre si e sua existência, perde a segurança de atuar socialmente e de se expressar sem restrições. Daí que autodeterminar o fluxo de dados pessoais é um requisito, uma exigência, ao livre desenvolvimento da personalidade.¹⁸⁶

Cabe acrescentar que essa renovada preferência pelo consentimento se explica também pelas dificuldades, ou desconfianças, relacionadas à possibilidade de estabelecer um completo sistema de autorizações e proibições por via legislativa.¹⁸⁷

¹⁸¹ PERÉZ, Maria Mercedes Serrano - El derecho fundamental a la Protección de Datos. Su contenido esencial. Nuevas políticas públicas [Em linha]. (2005). [Consult. 10 abr 2019]. p. 225. Disponível em WWW:<URL:https://dialnet.unirioja.es/servlet/revista?codigo=7332>.

¹⁸² BIONI, Bruno RICARDO - **Xequemate o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. 2015. p. 43.

¹⁸³ CUEVA, Pablo Lucas Murillo - **Informática y protección de datos personales (estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal)**. España: Centro de Estudios Políticos y Constitucionales (España), 1993. ISBN: 84-259-0940-6.

¹⁸⁴ FORTES, Vinicius Borges - **Os Direitos de Privacidade e a Proteção de Dados Pessoais na Internet**. Rio de Janeiro: Lumen Juris, 2016. ISBN978-85-8440-563-3, p. 154.

¹⁸⁵ GUERRA, Gustavo Rabay. Direito a Inviolabilidade e sigilo de comunicações privadas armazenadas: um grande salto rumo à proteção da privacidade na rede in: LEITE, George Salomão; LEMOS, Ronaldo. (Coord.). **Marco civil da internet**. São Paulo: Atlas, 2014. p. 392-416.

¹⁸⁶ SILVA, Carlos Bruno Ferreira da - **Proteção de Dados e Cooperação Transacional: Teoria e Prática na Alemanha, Espanha e Brasil**. 2014. p. 40.

¹⁸⁷ RODOTÀ, Stefano - **A Vida na Sociedade de Vigilância – A privacidade hoje**. Rio de Janeiro: Renovar, 2008. ISBN 978857147-688-2, p. 76.

Foi o próprio tratamento automático dos dados a demonstrar, à evidência, que nenhuma informação tem valor por si mesma, mas em virtude do contexto no qual está inserida, ou pelas finalidades para as quais é utilizada, ou pelas outras informações às quais tem sido associada. As regras sobre circulação dos dados então tendem a ser cada vez mais orientadas para a consideração de contextos, funções, associações.¹⁸⁸

A diretiva europeia irá adjetivar o consentimento na tentativa de operacionalizá-lo. O consentimento deve ser livre, informado, transparente, individual, com finalidade determinada, características essas que devem permear toda a legislação de proteção de dados pessoais. A diretiva não só determina o direito dos titulares dos dados em exercer o controle sobre os mesmos, mas também delega aos responsáveis pelo tratamento.

A problemática gira em torno de como esse controle deve ganhar vida. Tal como na seara contratual em que o consentimento pode se vestir de várias roupagens, não é diferente quanto à proteção de dados pessoais. Essa é a questão que está por trás da adjetivação que lhe é atribuída, fornecendo-se pistas sob qual deve ser a carga participativa exigida do cidadão para a circulação de seus dados pessoais. Para que um indivíduo possa controlar seus dados pessoais, ele precisa ter ciência quanto a sua coleta, uso e compartilhamento.

Ou seja, o fluxo informacional precisa tomar forma (ser informado), sendo a etapa prévia e necessária para que o consentimento comece a ser gestado. E uma vez informado, o cidadão pode, então, racionalizar a sua intenção em controlar seus dados pessoais. Não pode o cidadão consentir que seus dados pessoais sejam tratados com base em propósitos totalmente genéricos, emitindo-se uma espécie de verdadeiro “cheque em branco” que esvaziaria qualquer esfera de domínio sobre seus dados¹⁸⁹. A hipótese de interesses legítimos deve ser desenhada de forma cuidadosa para que o consentimento permaneça sendo a regra geral da dinâmica da proteção dos dados pessoais, sob pena de tornar, de forma incoerente, artificial a mencionada adjetivação a ele empregada.¹⁹⁰

O consentimento exerce um papel central no Regulamento de Proteção de dados onde funciona como condição de licitude da recolha e tratamento de dados¹⁹¹. O consentimento só pode ser considerado válido se o titular dos dados tiver a informação precisa da finalidade da recolha e tratamento dos dados. No entanto, o consentimento poderá ser preterido quando se

¹⁸⁸ RODOTÀ, Stefano - **A Vida na Sociedade de Vigilância – A privacidade hoje**. 2008. p. 77.

¹⁸⁹ BIONI, Bruno RICARDO - **Xequemate o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. 2015. p. 44.

¹⁹⁰ *Idem* – **Op. Cit.** p. 50.

¹⁹¹ BARBOSA, Mafalda Miranda - Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil. **Revista de Direito Comercial**. [Em linha]. [Consult. 6 jun.2019]. Disponível em WWW: <URL:https://www.revistadedireitocomercial.com/data-controllers-e-data-processors>.

fizer necessário um tratamento de dados necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento ou ainda por interesse legítimo do responsável pelo tratamento ou de terceiros, sendo garantido ao titular dos dados o direito de se opor ao tratamento dos dados que digam respeito à sua situação específica. (considerando 69)¹⁹².

O consentimento pode ser suprimido a qualquer altura como preceitua o artigo 7º -3 do RGPD, com a ressalva de que a retirada do consentimento não compromete a licitude do tratamento com base no consentimento previamente dado. E a retirada deverá ser feita de forma simples e rápida.

É possível afirmar que a autodeterminação informativa está intrinsicamente ligada ao conceito de privacidade de dados, que enseja uma esfera de proteção de dados pessoais ou sensíveis, e a de que forma o seu titular deseja expô-los para a sociedade de informação¹⁹³.

2.3 A proteção de dados pessoais no Brasil e na América Latina

No Brasil, a partir da década de 90 do século passado, intensifica-se uma preocupação sobre os perigos de certas informações arquivadas sobre a integridade da esfera individual do ser humano, igualmente influenciada pela espantosa redução dos equipamentos combinada com um equivalente aumento das suas capacidades, como se vê nos aparelhos de captação de imagem e processamento de dados¹⁹⁴. Pela ausência de uma legislação própria, assim como do reconhecimento pelo Supremo Tribunal Federal de uma direito à proteção de dados autônomos com substrato constitucional, há bastante insegurança jurídica na proteção geral de dados no Brasil, ou seja, relativamente àqueles onde não há disposições específicas que determinem o sigilo em relação aos terceiros que deles tomem conhecimento.¹⁹⁵

A proteção de dados pessoais no Brasil é realizada na legislação infraconstitucional de uma forma breve e fragmentária, uma vez que até a promulgação da Lei 12.965/14 – Marco Civil da Internet, não havia uma legislação específica que versava sobre relações virtuais no campo do Direito Digital, estabelecendo direitos e deveres a usuários e prestadores de serviços no País. Trata-se da primeira proposta de marco civil do mundo, uma espécie de “constituição

¹⁹² UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. [Em linha]. [Consult. 18 mar. 2019]. Disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN>>.

¹⁹³ MORAES, Melina Ferracini - **Direito ao Esquecimento na Internet**. 2018. p. 114-5.

¹⁹⁴ SILVA, Carlos Bruno Ferreira da – **Proteção de Dados e Cooperação Transacional: Teoria e Prática na Alemanha, Espanha e Brasil**. 2014. p. 213.

¹⁹⁵ *Idem* – **Op. Cit.** p. 214.

da internet” que regulamenta direitos, deveres e garantias do uso da rede de computadores no país. O principal objetivo é garantir os interesses dos usuários e promover a cidadania. Por essa razão, foi elaborado de forma colaborativa com a participação de diversos segmentos da sociedade civil.¹⁹⁶

No Brasil, com a Lei 12.965/14 – Marco Civil da Internet, já demos um passo adiante no sentido de resguardar os direitos e deveres dos usuários da internet. A respectiva Lei está alicerçada em 3 pilares fundamentais: a liberdade de expressão, neutralidade de rede e a privacidade dos usuários. Entretanto, não adianta o endurecimento da punição se as pessoas não se conscientizarem de que estão se expondo demais sem se importar com os riscos que estão correndo. É necessário a implementação de políticas públicas, educacionais e sociais no sentido de esclarecer os riscos que as pessoas correm ao publicarem fotos, vídeos pessoais, conversas sobre a sua vida, sua rotina. Fotos e vídeos na Web jamais são excluídos na medida em que o protagonista perde o controle de tudo que publica, e os dados podem ser salvos por usuários mal-intencionados.

Dentro do ordenamento jurídico brasileiro podemos relacionar as leis infraconstitucionais de proteção de dados pessoais: Lei 8.078 de 11 de setembro de 1990 - Código de Defesa do Consumidor. Os artigos 43 e 44 dizem respeito a proteção de dados pessoais voltados para o consumo. Lei do Cadastro Positivo – Lei 12.414/2011 que disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, Lei nº 12.527/2011 - artigo 31¹⁹⁷ que regulamenta o inciso XXXIII da Constituição da República Federativa do Brasil¹⁹⁸ garantindo ao cidadão acesso as informações dos órgãos públicos de assuntos de seus interesses:

“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”.

¹⁹⁶ SEGURADO, Rosemary; LIMA, Carolina Silva Mandú de; AMENI, Cauê S. Regulamentação da internet: perspectiva comparada entre Brasil, Chile, Espanha, EUA e França. **História, Ciências, Saúde – Manguinhos**. Rio de Janeiro. ISSN 0104-5970. 22 (2015), p.1560.

¹⁹⁷ BRASIL. Lei nº 12.527, de 18 de novembro de 2011. **Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências** [Em linha]. [Consult. 19 abr. 2019]. Disponível em WWW: <URL: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/12527.htm>.

¹⁹⁸ BRASIL. **Constituição da República Federativa do Brasil**, de 05 de outubro de 1988. [Em linha]. [Consult. 05 de jan. de 2018]. Disponível em WWW: <URL: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.html>.

Em 2013 o escândalo provocado pelas revelações de Edward Snowden, ex-analista de sistemas da *National Security Agency* (NSA) sobre a existência de espionagem por parte do governo norte americano nos Estados Unidos, Europa e alguns países da América Latina, que incluíram o Brasil, foi determinante para o encaminhamento do Marco Civil da Internet. De forma surpreendente, o Marco Civil foi escolhido como parte da resposta nacional aos escândalos envolvendo o aumento indiscriminado de vigilância e espionagem. Vale dizer que efetivamente havia pouco no Marco Civil da Internet que atacasse diretamente as questões envolvidas nos escândalos de espionagem, mas uma vez eleito pelo governo como uma ferramenta de resposta à situação colocada, o texto legal passou por algumas modificações.¹⁹⁹

Duas foram as mudanças mais significativas empreendidas no texto do projeto de lei. A primeira dizia respeito ao incremento do atual artigo 7º, que trata da proteção da privacidade e dos dados pessoais. Compreensivelmente, ao Marco Civil foram acrescidos dispositivos que traziam para o corpo do projeto questões envolvendo a coleta e o tratamento de dados pessoais. Um segundo tema que passa a constar dos debates sobre o Marco Civil é a possibilidade de se obrigar empresas estrangeiras que coletam dados pessoais de brasileiros a manter servidores no Brasil. Esse dispositivo de localização forçada de dados foi bastante comentado por ser, na época, um desejo expresso do governo federal como resposta aos escândalos de espionagem.²⁰⁰

Enfim, em 23 de abril de 2014, finalmente foi aprovado o Marco Civil da Internet²⁰¹ brasileira, lei infraconstitucional, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil resultado de uma consulta pública idealizada em 2009, que tramitou no Congresso Nacional entre 2011 e 2014. O projeto de lei passou pelo controle e revisão de diferentes setores da sociedade, entre empresas, organizações da sociedade civil, ativistas e comunidade técnica²⁰². Primeira lei criada de forma colaborativa entre sociedade e governo, com utilização da internet como plataforma de debate, impondo uma série de direitos e deveres a usuários e prestadores de serviços no País, além de impor o direito de inclusão digital ou de acesso a todos.²⁰³

¹⁹⁹ LEMOS, Roberto - O marco civil como símbolo do desejo por inovação no Brasil *in*: LEITE, George Salomão; LEMOS, Ronaldo. (Coord.). **Marco civil da internet**. 2014. p. 25.

²⁰⁰ *Idem* – **Op. Cit.** p. 24-8.

²⁰¹ BRASIL. **Lei n.º 12.965**, de 24 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. [Em linha]. [Consult. 15 abr. 2019]. Disponível em WWW: <URL: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

²⁰² LEMOS, Roberto - O marco civil como símbolo do desejo por inovação no Brasil *in*: LEITE, George Salomão; LEMOS, Ronaldo. (Coord.). **Marco civil da internet**. 2014. p. 13.

²⁰³ JESUS, Damasio; MILAGRE, Jose Antonio – **Marco Civil da Internet Comentários à Lei 12.965/14**. São Paulo: Saraiva, 2014. ISBN 978-85-02-23018-7, p. 15-24.

O acesso à internet passa a ser condição para a cidadania. A suspensão da conexão à internet, que não seja por motivo de débito decorrente de sua utilização, é violação a direitos dos usuários, sendo cabível reparação por danos morais e materiais decorrentes e comprovados, e ainda no que tange à qualidade e velocidade de tráfego da internet. No Brasil é um direito do usuário que sua velocidade contratada seja igual à sua velocidade constatada²⁰⁴. O artigo 3º estatui oito princípios basilares do uso da internet no Brasil, dentre outros em especial: garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; proteção da privacidade, proteção dos dados pessoais, preservação e garantia da neutralidade de rede²⁰⁵.

A neutralidade de rede, prevista no artigo 9º, pressupõe que todas as informações que trafegam pela internet, independentemente de qualquer formato, devem ser tratadas de forma isonômica, ou seja, não pode haver distinção de velocidade ou pacotes sem distinção em relação ao conteúdo, à origem, ao destino, ao serviço, ao terminal ou à aplicação. Os pacotes de dados devem ter o mesmo tratamento no que tange à velocidade de tráfego, não podendo o provedor reduzir a velocidade de acordo com o conteúdo acessado, sua origem e destino, o serviço ou à aplicação utilizada, ou mesmo de acordo com o “terminal que acessa” determinado serviço²⁰⁶.

A quebra da neutralidade de rede permitirá às empresas de internet fazerem diferenciação na oferta de serviços, conforme podemos ver no funcionamento da TV a cabo, que diferencia o acesso à programação a partir da organização de pacotes que são oferecidos aos clientes separadamente. No caso da internet, por exemplo, para acessar vídeos, os usuários teriam que pagar um pacote diferenciado, para acessar música, outro pacote. Desse modo, verifica-se o rompimento com a isonomia em relação aos diferentes formatos de informações existentes na rede. Assim, podemos afirmar que a neutralidade garante que a internet continue livre e que os que controlam a infraestrutura da rede não têm o direito de controlar o fluxo de informações.²⁰⁷

O Marco Civil da Internet apresenta um novo cenário no qual o conceito de “Internet livre” está ligado não à ausência de leis, mas sim à existência de leis que possam garantir e preservar as liberdades que são usufruídas por todos justamente por causa da tecnologia e mais especificamente pelo desenvolvimento da Internet. Foi com essa motivação que o Marco Civil

²⁰⁴ ²⁰⁴ JESUS, Damasio; MILAGRE, Jose Antonio – **Marco Civil da Internet Comentários à Lei 12.965/14**. São Paulo: Saraiva, 2014. ISBN 978-85-02-23018-7, p. 33-4.

²⁰⁵ *Idem* – **Op. Cit.** p. 20-1.

²⁰⁶ *Idem* – **Op. Cit.** p. 42-3.

²⁰⁷ SEGURADO, Rosemary; LIMA, Carolina Silva Mandú de; AMENI, Cauê S. Regulamentação da internet: perspectiva comparada entre Brasil, Chile, Espanha, EUA e França. **História, Ciências, Saúde – Manguinhos**. 2015. p.1560.

foi concebido: como uma lei que pudesse preservar as bases para a promoção das liberdades e dos direitos na Internet no Brasil²⁰⁸.

Algumas críticas foram feitas por doutrinadores especializados, no sentido de que o Marco Civil teve falha grave, em não especificar (detalhar) o que é dado pessoal(cadastral) e sua diferença em relação a dado ou registro de conexão, em relação ao assinante. Os dados de conexão ou de acesso a aplicações (com o fornecimento de IPs) não identificam, em um primeiro momento, um usuário. Já, por sua vez, os dados cadastrais qualificam e identificam o usuário²⁰⁹.

A situação pré-Marco Civil era de completa ausência de regulamentação civil da internet no país. Ao contrário do que alguns entusiastas libertários poderiam achar, a ausência de leis nesse âmbito não representa a vitória da liberdade e do laissez-faire. Ao contrário, a ausência de uma legislação que trate das questões civis da rede leva a uma grande insegurança jurídica. Uma das razões é que juízes e tribunais, sem um padrão legal para a tomada de decisões sobre rede, acabam decidindo de acordo com regras muitas vezes criadas ad hoc, ou de acordo com suas próprias convicções.²¹⁰

Uma das funções do Marco Civil Brasileiro era gerar segurança jurídica, oferecendo base legal ao Poder Judiciário quando se deparar com questões envolvendo internet e tecnologia da informação, evitando-se decisões contraditórias sobre temas idênticos, o que era muito comum.²¹¹

O Marco Civil da Internet, aborda a garantia do acesso à internet como essencial ao exercício da cidadania (artigo 7º), trazendo também em seu bojo a salvaguarda da proteção da intimidade e da vida privada no âmbito da internet e a reparação através de indenizações resultantes de suas violações. Já o artigo 2º traduz de forma explícita o fundamento basilar da legislação, a liberdade de expressão, que norteará sempre desde que não lesione direito de terceiros. Nota-se também presente o princípio da proteção da privacidade e a proteção dos dados pessoais (artigo 3º incisos II, III).

Além de proteger a privacidade em geral, o Marco Civil dá ênfase à proteção dos dados pessoais, informações que podem identificar uma pessoa e que comumente são utilizadas ou requeridas pelos provedores de acesso à internet ou provedores de serviços no Brasil.²¹² O

²⁰⁸ LEMOS, Roberto - O marco civil como símbolo do desejo por inovação no Brasil in: LEITE, George Salomão; LEMOS, Ronaldo. (Coord.). **Marco civil da internet**. 2014. p. 16.

²⁰⁹ *Idem* - **Op. Cit.** p. 49-9.

²¹⁰ *Idem* - **Op. Cit.** p. 10.

²¹¹ *Idem* - **Op. Cit.** p. 18.

²¹² *Idem* - **Op. Cit.** p. 22.

inciso VI do artigo 3º comanda a responsabilização dos agentes de acordo com suas atividades no caso de causarem danos ao seus usuários. Não se admitindo que provedores aleguem usos e costumes para relativizar suas responsabilidades trazidas com esta nova legislação, como o estrito respeito à privacidade dos cidadãos.²¹³ Registros de aplicações de internet são gerados por provedores de aplicações (ou serviços) e correspondem ao conjunto de informações referente à data e hora do uso de uma determinada aplicação, a partir de um determinado endereço de IP. Mesmo que o usuário não queira, tais registros são automaticamente coletados, quando ele interage com algum serviço oferecido na internet.²¹⁴

O consentimento, pedra angular de qualquer norma de proteção de dados, também está presente no Marco Civil da Internet, no artigo 7º incisos VII e IX, onde verifica-se a adjetivação do consentimento o qual deverá ser livre, expresso e informado, vedado o fornecimento ou compartilhamento com terceiros.

O Marco Civil da internet estabelece dois tipos de provedores: provedores de conexão e provedores de aplicação. Na seara da responsabilidade civil dos provedores da internet, o artigo 18 do Marco Civil²¹⁵, é explícito no sentido de que não há responsabilidade por parte dos provedores de conexão à internet por danos decorrentes de conteúdo gerado por terceiros, a exceção está prevista no artigo 19²¹⁶ onde será responsabilizado civilmente o provedor, após ordem judicial, não tomar providências para, no âmbito e limites técnicos de seu serviço e dentro do prazo assinalado.

Em virtude da existência de alguns hiatos na Lei Marco Civil em relação a diversidade de provedores de serviços na internet, a jurisprudência pátria já firmou entendimento em relação a responsabilidade civil dos provedores da internet, definindo os diversos tipos de provedores de serviços.

A terceira turma do Superior Tribunal de Justiça no Recurso especial REsp 1.316.921/RJ julgado em 26/06/2012, DJe 29/06/2012, foi delineado várias espécies de provedores de serviços assim conceituados como aqueles que fornecem serviços ligados ao funcionamento dessa rede mundial de computadores, ou por meio dela:

Trata-se de gênero do qual são espécies as demais categorias, como: (i) provedores de backbone (espinha dorsal), que detêm estrutura de rede capaz de processar grandes volumes de informação. São os responsáveis pela conectividade, oferecendo sua infraestrutura a terceiros, que repassam aos usuários finais acesso à

²¹³ JESUS, Damásio; MILAGRE, Jose Antonio – **Marco Civil da Internet Comentários à Lei 12.965/14**. 2014. p. 29.

²¹⁴ *Idem* – **Op. Cit.** p. 27.

²¹⁵ BRASIL. **Lei n.º 12.965**, de 24 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil [Em linha]. [Consult. 15 abr. 2019]. Disponível em WWW: <URL: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

²¹⁶ *Idem* – **Op. Cit.**

rede; (ii) provedores de acesso, que adquirem a infraestrutura dos provedores backbone e revendem aos usuários finais, possibilitando a estes conexão com a Internet; (iii) provedores de hospedagem, que armazenam dados de terceiros, conferindo-lhes acesso remoto; (iv) provedores de informação, que produzem as informações divulgadas na Internet; e (v) provedores de conteúdo, que disponibilizam na rede os dados criados ou desenvolvidos pelos provedores de informação ou pelos próprios usuários da web. É frequente que provedores ofereçam mais de uma modalidade de serviço de Internet; daí a confusão entre essas diversas modalidades. Entretanto, a diferença conceitual subsiste e é indispensável à correta imputação da responsabilidade inerente a cada serviço prestado.²¹⁷

Um dos pontos cruciais dessa legislação é a questão da responsabilidade civil dos provedores de internet, onde a matéria é polêmica, uma vez que se faz necessário identificar de forma concreta a atuação do provedor bem como identificar com especificidade a atuação do provedor pelos danos causados por conteúdo gerado por terceiros. No âmbito da jurisprudência dos tribunais brasileiros, conforme exposto pela doutrina, surgiram três entendimentos sobre a responsabilidade civil dos provedores de aplicações de Internet por conteúdos gerados por terceiros: (i) a irresponsabilidade pelas condutas de seus usuários; (ii) a responsabilidade civil objetiva; e (iii) a responsabilidade subjetiva, que pode ser subdividido a partir do momento em que o provedor de aplicação seria responsável pelo conteúdo gerado por terceiro.²¹⁸

Em seus mais recentes posicionamentos sobre o tema, o Superior Tribunal de Justiça, do Brasil, tem defendido a tese da responsabilidade subjetiva dos provedores justamente pela não remoção do conteúdo reputadamente ilícito quando ciente de sua existência por uma notificação da vítima. Aqui são considerados em conjunto tanto os casos em que o provedor se omite em responder à notificação da vítima ou de forma ativa responde a notificação afirmando que não vê motivos para retirar o conteúdo do ar. Nesses casos a responsabilidade, além de subjetiva, seria também solidária com o autor do dano²¹⁹.

O Marco Civil da internet, em seu artigo 19, aponta a responsabilidade do provedor de aplicações, somente, no caso de perpetrar danos por conteúdos gerados por terceiros após o não cumprimento da ordem judicial específica para remoção de conteúdo ou similar.

Não há dúvida que o Marco Civil da Internet é uma medida legislativa audaciosa do governo brasileiro para regular o mundo virtual, cuja edição ainda vem acompanhada por doses exageradas de otimismo, ceticismo ou mera perplexidade nos atores governamentais ou não, de

²¹⁷ BRASIL. Superior Tribunal de Justiça. **REsp. nº 1.316.921 RJ**. [Em linha]. [Consult. 22 abr. 2019]. Disponível em WWW:<URL:https://stj.jusbrasil.com.br/jurisprudencia/22026857/recurso-especial-resp-1316921-rj-2011-0307909-6-stj/relatorio-e-voto-22026860?ref=juris-tabs>.

²¹⁸ BRASIL, Superior Tribunal de Justiça. **REsp. nº 1.501.603 RJ**. [Em linha]. [Consult. 22 Abr. 2019]. Disponível em WWW:<URL:https://ww2.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=1668833&tipo=0&nreg=201402900716&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20171218&formato=PDF&salvar=false>.

²¹⁹ SOUZA, Carlos Affonso; LEMOS Ronaldo - **Marco civil da internet: construção e aplicação**. Juiz de Fora: Editar, 2016. ISBN: 978-85-7851-156-2, p. 81.

outros países. Porém, não há como não ser elogiado o objetivo de começar a situar o Brasil dentro da regulação de proteção de dados conforme o que foi proposto no cenário europeu, além do estímulo final a sedimentação de um cenário de Administração Eletrônica dentro dos Poderes Políticos brasileiros.²²⁰

Em relação à América do Sul, em agosto de 2010, o Chile se tornou o primeiro país do mundo a aprovar uma lei de regulamentação da internet baseada no princípio de neutralidade na rede. Nesse sentido, a lei promoveu o redimensionamento das relações entre o Estado, as empresas de telecomunicações, os provedores e os usuários da internet, considerando que a neutralidade de rede estabelece que as empresas provedoras de internet não podem interferir no tráfego de informações na rede, não sendo, portanto, autorizada a retirada, a priorização ou discriminação de qualquer tipo de conteúdo que nela circula²²¹.

A Argentina, o primeiro país latino-americano a receber o reconhecimento, pela Comissão da União Europeia, da adequação de seu sistema de proteção de dados pessoais, em junho de 2003²²². A Lei 27.275 – Direito de acesso à informação pública tem por fim garantir o efetivo exercício do direito de acesso à informação pública, promover a participação cidadã e a transparência da gestão pública, ancorado nos princípios: presunção de publicidade, transparência e máxima divulgação, informalismo, máximo acesso, abertura, dissociação, sem discriminação, máxima pressa, gratuidade, controle, responsabilidade, âmbito limitado das exceções, na dúvida pro petitor, facilitação e boa-fé²²³. Foi promulgada, na Argentina, em outubro de 2000, a Lei de Proteção de Dados Pessoais -Lei 25.326²²⁴ com escopo de garantir proteção integral dos dados pessoais assentados em arquivos, registros, banco de dados, ou outros meios técnicos de tratamento de dados, seja estes públicos, privados, destinados a dar informes, para garantir o direito a honra e a intimidade das pessoas, bem como o acesso às informações registradas sobre eles, de acordo com as disposições do artigo 43, terceiro parágrafo da Constituição Nacional. (artigo 1º).

²²⁰ SILVA, Carlos Bruno Ferreira da – **Proteção de Dados e Cooperação Transacional: Teoria e Prática na Alemanha, Espanha e Brasil**. 2014. p. 243.

²²¹ *Idem* – *Ibidem*.

²²² **EUR-LEX 32003D0490**. [Em linha]. [Consult. 11maio 2019]. Disponível em WWW:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32003D0490&from=EN>.

²²³ ARGENTINA. Ley 27275. Artigo 1º. **Derecho de Acceso a La Información Pública**. [Em linha]. [Consult. 11 maio 2019]. Disponível em WWW: <URL:http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/norma.htm>.

²²⁴ ARGENTINA. Lei 25.326. **Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales**. [Em linha]. [Consult. 11 maio 2019]. Disponível em WWW:<URL:http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm>.

A autoridade de controle denominada *Agência de Acceso a la Información Pública* (Agência de Acesso à Informação Pública) tem previsão legal no artigo 29. 1 da Lei 25.326, onde estabelece normas e regulamentos para o correto desempenho das atividades previstas na lei de proteção de dados pessoais, fiscaliza a integridade e segurança dos bancos de dados alcançados por tal lei, solicita informações a entidades públicas e privadas a respeito dos tratamentos de dados por elas conduzidos, impondo sanções administrativas por descumprimentos da referida lei, inicia ações penais por violações da lei de proteção de dados e assiste e assessora titulares, dos dados com vistas à defesa dos direitos que a lei de proteção de dados pessoais lhes garante²²⁵.

Na mesma rota, o Uruguai igualmente teve a chancela do Parlamento Europeu e do Conselho para reconhecer que a República Oriental do Uruguai assegura um nível adequado de proteção dos dados pessoais no que se refere ao tratamento automatizado de dados, transferidos a partir da União Europeia consoante Decisão de Execução da Comissão Europeia de 21 de agosto de 2012 nos estertores do artigo 25.º, n.º 2, da Diretiva 95/46/CE.²²⁶

2.3.1 A influência do marco civil da internet nos países da Itália e França

“Declaração de Direitos da Internet” - um pequeno passo para o homem, um grande passo para a humanidade²²⁷. A declaração de direitos da internet nasce na Itália fortemente influenciada pelo Marco Civil da internet do Brasil, aprovada por unanimidade pela Câmara dos Deputados em 3 de novembro de 2015, após vários meses de consulta pública. É uma Constituição moderna e progressista on-line que pretende regular, mas não censurar, proteger liberdades individuais e coletivas, acesso, uso não-distorcido ou violento, segurança da privacidade, neutralidade da rede, o direito de esquecimento²²⁸.

²²⁵ ARGENTINA. Lei 25.326. **Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales.** [Em linha]. [Consult. 11 maio 2019]. Disponível em WWW:<URL: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm>>.

²²⁶ UNIÃO EUROPEIA. Decisão de Execução da Comissão de 21 de agosto de 2012. **Jornal Oficial da União Europeia.** [Em linha]. [Consult. 11 maio 2019]. Disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32012D0484&from=EN>>.

²²⁷ NAVARRI, Veronica - **Internet Bill of Rights: un piccolo passo per l'uomo, un grande passo per l'umanità.** [Em linha]. [Consult. 21 abr. 2019]. Disponível em WWW: <URL: <https://medium.com/argomenti-di-diritto-dei-media-digitali/internet-bill-of-rights-un-piccolo-passo-per-luomo-un-grande-passo-per-l-umanit%C3%A0-5442af2a3750>>.

²²⁸ RODOTÁ, Stefano - **“La Carta dei Diritti in Internet” – Privacy Italia.** [Em linha]. [Consult. 26 abr. 2019]. Disponível em WWW: <URL: <https://www.privacyitalia.eu/rodota-un-profeta-dei-diritti-sulla-rete/3483/>>.

Diferente do Brasil, que optou pela aprovação de uma lei federal, a Declaração italiana, aprovada pelo Parlamento, não tem força de lei. Ela atua como uma carta de princípios que guia a futura produção legislativa e pode orientar a resolução de conflitos judiciais.²²⁹

A redação italiana guarda algumas semelhanças com o texto do Marco Civil brasileiro, embora seja digna de destaque a inserção na cláusula da chamada “neutralidade de dispositivos”, garantindo assim que não exista discriminação no fluxo de dados de acordo com o dispositivo utilizado pelo usuário.²³⁰ Essa Declaração de Direitos na Internet, um ativo básico na era digital, coloca a proteção da pessoa e do usuário da Web no centro. De fato, os principais pilares que a constituem são acesso livre, neutralidade da rede e privacidade de dados, educação no uso da Internet, autodeterminação pessoal, não ser discriminado, dignidade, etc.²³¹

Os modestos 14 artigos da referida declaração tem como elementos de base: Reconhecimento e garantia de direitos, Direito de acesso; Direito ao conhecimento e educação online; Neutralidade da rede; Proteção de dados pessoais; Direito à autodeterminação informacional; Direito à inviolabilidade dos sistemas, dispositivos e domicílios de TI; Tratamentos automatizados; Direito à identidade ; Proteção do anonimato ; Direito ao esquecimento ; Direitos e garantias das pessoas nas plataformas ; Segurança na Rede; governança de rede ;

Seguindo essa linha a França, em seguida, realizou uma ampla consulta para a modificação de leis em vigor de forma a prever questões relacionadas à proteção de direitos na Internet. Através de um conceito amplo de criação de uma “República Digital” – “*République Numérique*”, as propostas de modificação legislativas francesas foram debatidas em uma plataforma que representa um passo adiante na forma de apresentação dos temas e do debate em si, com gráficos que demonstram a evolução da discussão e metodologia que evidencia os momentos de *feedback* aos participantes da consulta e a produção de sínteses.²³² Consagra também na lei 2016-1321 de 7 outubro 2016 para uma Republica Digital, o princípio decisivo da neutralidade da Internet: define e estabelece uma regra de estruturação que deve governar a operação da rede digital. A neutralidade da Internet é um componente essencial da confiança e proteção usos e inovação no ecossistema digital²³³.

²²⁹ SOUZA, Carlos Affonso; LEMOS Ronaldo - **Marco civil da internet: construção e aplicação**. 2016. p. 32.

²³⁰ *Idem - Ibidem*.

²³¹ NAVARRI, Veronica - **Internet Bill of Rights: un piccolo passo per l'uomo, un grande passo per l'umanità**. [s.d.].

²³² SOUZA, Carlos Affonso; LEMOS Ronaldo - **Marco civil da internet: construção e aplicação**. 2016.. p. 36.

²³³ FRANÇA. **LOI n° 2016-1321**, du 7 Octobre 2016. [Em linha]. [Consult. 25abr.2019]. Disponível em WWW: <URL:https://www.legifrance.gouv.fr/affichLoiPubliee.do?idDocument=JORFDOLE000031589829&type=general&legislature=14>.

2.3.2 Lei 13.709/2018 – Lei de proteção de dados pessoais no Brasil

O Marco Civil da internet foi o pontapé inicial dado pelo Brasil usando a internet como plataforma estabelecendo princípios, garantias, direitos e deveres para o uso da internet²³⁴ na sociedade da informação onde a facilidade de acesso para navegar em diversos sites faz com que os provedores recolham dados sobre as características de seus usuários, preferências, hábitos, quando estes interagem visitando determinados sites. Na verdade, o usuário da internet de forma involuntária vem contribuindo para alimentar o banco de dados daqueles que exploram a informação pessoal em benefício próprio, penetrando na privacidade de seus usuários que acabam permitindo de forma involuntária.

Há na internet um foco privilegiado para essa coleta involuntária, e quando estamos identificados (seja por meio de um login ou de um IP já conhecido) durante o acesso a um site da Internet, é possível à empresa ver através de troca de páginas ou mesmo do deslizar do cursor, todos aqueles elementos que atarem o nosso interesse. Consequentemente pode estabelecer projetos de atendimento personalizado em nossa próxima visita e estimular vontades que talvez fossem até inconscientes em nós mesmos²³⁵.

Até então não havia uma legislação protetiva no que tange ao direito de proteção dos dados pessoais, para garantir e preservar o direito à privacidade na era da sociedade informação. Os elementos de maior destaque para atuação da proteção de dados no ordenamento brasileiro são a ação de *habeas data*, introduzida pela Constituição de 1988 e regulamentada pela Lei 9507/97, e os preceitos sobre a proteção aos dados pessoais em relações de consumo, determinadas pelo Código de Defesa do Consumidor em seus artigos 43 e 44. Foi concebido o *habeas data*, para proporcionar, portanto, ao cidadão um instrumento para conhecer diretamente e, se necessário, retificar as informações sobre sua pessoa armazenadas em banco de dados.²³⁶

Em 14 de agosto de 2018 nasce para o Brasil a Lei 13.709 que dispõe sobre a proteção de dados, (LGPD), alterando a Lei 12.965/14, o Marco Civil da internet. Sua vigência foi desmembrada em dois blocos, através da Medida Provisória 869 de 27 de dezembro de 2018:

²³⁴ BRASIL. Lei 12.965 de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. [Em linha]. [Consult. 10 abr. 2019]. Disponível em WWW: <URL: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

²³⁵ SILVA, Carlos Bruno Ferreira da – **Proteção de Dados e Cooperação Transacional: Teoria e Prática na Alemanha, Espanha e Brasil**. 2014, p. 14.

²³⁶ DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar. 2006. p. 326-8.

vigência em 28/12/2018, para os artigos que recriam a autoridade de fiscalização; e Vigência em 24 meses, a contar da publicação da LGPD, para os demais artigos. O surgimento dessa lei, nada mais é do que o efeito dominó que o Regulamento Geral de Proteção de Dados em vigor na Europa desde 25 de maio de 2018 causou nos demais países do mundo que mantêm relações econômicas com a União Europeia, impondo-lhes a necessidade de uma legislação do mesmo cunho do Regulamento em vigor, para que num futuro não sofresse sanções .

A Lei 13.709/2018 é um novo marco legal brasileiro de grande impacto, tanto para instituições privadas como para as públicas, por tratar de proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica. É uma regulamentação que traz princípios, direitos e obrigações relacionadas ao uso de um dos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas.²³⁷

A base desse pacto é a liberdade, mas o fiel da balança é a transparência. Sendo assim, as lei sobre a proteção de dados pessoais tem uma característica muito peculiar de redação principiológica e de amarração com indicadores mais assertivos, de ordem técnica, que permitam auferir de forma audível se o compromisso está sendo cumprido, por meio da análise de trilhas de auditoria e da implementação de uma série de itens de controle para uma melhor governança dos dados pessoais.²³⁸

O artigo 2º disciplina os fundamentos da Lei de proteção de dados, o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais²³⁹.

Como princípios relativos as atividades do tratamento, está disposto no artigo 6º: devem primar pela boa fé; finalidade clara e transparente; adequação em função da finalidade a que se destina; necessidade limitação do tratamento para atingir a sua finalidade livre acesso onde os titulares dos dados pessoais terão garantido a consulta integral de fácil acesso e gratuita; qualidade dos dados visando assegurar exatidão, clareza, relevância e atualização dos dados dos

²³⁷ PINHEIRO, Patricia Peck – **Proteção de Dados Pessoais Comentários à Lei 13.709/2018 (LGPD)**. 2018. p. 15.

²³⁸ *Idem* – **Op. Cit.** p. 17-8.

²³⁹ BRASIL. **Lei n.º 13.709**, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet)** [Em linha]. [Consult. 10 abr. 2019]. Disponível em WWW: <URL:http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>.

titulares, sempre relacionado a finalidade a que se destina; transparência; segurança, prevenção com vistas a evitar danos em virtude do tratamento de dados pessoais; não discriminação impedindo realização de tratamento para fins discriminatórios ilícitos ou abusivos e responsabilização e prestação de contas²⁴⁰. Enquanto os artigos 12,13 e 14 do regulamento europeu, RGPD, pontuam de maneira mais explícita os requisitos, limites e as regras para promoção da transparência das informações, das comunicações e exercício dos titulares dos dados.

A Lei de Proteção de Dados Brasileira contempla os alicerces que devem conter qualquer norma jurídica que verse sobre dados pessoais: definição de dados pessoais, dados anônimos e consentimento do titular dos referidos dados.

A legislação brasileira, Lei 13.709/2018 de Proteção de Dados(LGPD), delimita três categorias de dados: dado pessoal, dado pessoal sensível e dado anonimizado, conforme disposto no artigo 5º, em especial, nos detemos no inciso III²⁴¹ onde a definição de dado anonimizado é tido como dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento e inciso IX anonimização como utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

O critério da razoabilidade nada mais é do que uma diretriz acerca do que venha a ser um risco aceitável em torno da reversibilidade do processo de anonimização, a fim de que os dados anonimizado estejam fora do conceito de dados pessoais.²⁴²

O consentimento descrito no artigo 8º da Lei 13.709/2018, tem a preocupação de garantir que os usuários tenham ciência de que devem consentir o uso dos dados, assim como tenham direito de saber a finalidade da coleta e acesso ao seu conteúdo em qualquer momento, é primordial para assegurar a liberdade e privacidade.²⁴³ O consentimento tem que ser expresso, claro, não se admitindo a interpretação de seu silêncio ou omissão como anuência, como consentimento.

²⁴⁰ BRASIL. **Lei n.º 13.709**, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet)** [Em linha]. [Consult. 10 abr. 2019]. Disponível em WWW: <URL:http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>.

²⁴¹ *Idem* – *Ibidem*.

²⁴² BIONI, Bruno RICARDO - **Xequemate o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. 2015. p. 32.

²⁴³ PINHEIRO, Patricia Peck – **Proteção de Dados Pessoais Comentários à Lei 13.709/2018 (LGPD)**. 2018. p. 65.

No próximo capítulo abordaremos a temática da violação de dados na Europa, a partir de caso concretos, onde o direito ao esquecimento objetiva minimizar os danos irreversíveis ao direito à privacidade no contexto da atual indústria da vigilância sem precedentes.

CAPÍTULO III

3 DATA BREACH - VIOLAÇÃO DE DADOS PESSOAIS

3.1 Um panorama na Europa e na América do Sul

A violação de dados pessoais, nada mais é que o acesso não autorizado a dados pessoais de uma pessoa. Hoje, no mundo moderno somos todos, sem distinção Cidadãos Digitais, cibercidadãos, estamos conectados 24 horas por dia, por telefone, nas redes sociais, nos computadores, na vida diária com transações bancárias via aplicativos em celulares, compras com cartão de crédito on line, interagindo através de diversos aplicativos para pegar um táxi, pedir uma refeição ou um lanche, colocar um combustível em seu veículo, enfim em quase tudo que fazemos, conscientes ou não estamos disseminando dados pessoais em diferentes canais. Chegamos ao ponto de confienciarmos nossos dados pessoais, nossas imagens, nossos vídeos em provedores de serviços na nuvem, mesmo sem termos conhecimento onde e como esses dados estão sendo armazenados e processados. Os dados pessoais converteram-se em um fator vital para a engrenagem da economia da informação²⁴⁴.

As informações pessoais que o cidadão digital propaga são valiosas para o mercado do consumo dos grandes empresários, revolucionando a economia digital global. Toda vez que o cidadão acessa um determinado site, através do computador ou do seu celular, as informações ficam registradas construindo um perfil do usuário. É dessa forma que as empresas absorvem esses dados para si, repassam, na verdade vendem a terceiros, sem o consentimento do cidadão, caracterizando assim, a violação de dados.

O Regulamento Geral de Proteção de Dados, define violação de dados em seu artigo 4.º, item 12²⁴⁵ : “Violação de dados pessoais”, uma violação da segurança que provoque, de modo accidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento” .

Dessa definição podemos extrair a existência de três tipos de violação de dados, o chamado CIA, que já existia desde a Directiva 95/46: Confidencialidade, Integridade e

²⁴⁴ BIONI, Bruno RICARDO – **Proteção de Dados Pessoais a função e os limites do consentimento**. 2019. p. 13.

²⁴⁵ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. [Em linha]. [Consult. 5 mai. 2019]. Disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN>>.

Acessibilidade²⁴⁶, configurando-se os três pilares da segurança da informação. Cada um desses itens tem vital importância para os processos de proteção de dados, sendo essenciais em qualquer política interna de Tecnologia da Informação voltada a garantir que os processos internos fluam corretamente. Os três termos estão interligados, porém possuem diferenças. O primeiro deles tem a ver com o sigilo dos dados da empresa, enquanto o segundo se refere à consistência deles. Por fim, o terceiro tem a ver com manter o acesso a eles de modo constante, evitando interrupções. Garantir confidencialidade, integridade e disponibilidade é fundamental para garantir a segurança e a consistência dos dados corporativos. Sem o devido cuidado com esses três pontos, a empresa pode ser vítima de ataques virtuais que podem ocasionar um grande prejuízo, além de ficar à mercê de falhas que geram retrabalhos e perdas de dados estratégicos²⁴⁷.

Confidencialidade quando existe uma divulgação ou acesso acidental ou não autorizado a dados pessoais. Para garantir confidencialidade a informação deve ser protegida para evitar a perda e a divulgação indevida. As ações incluem a aplicação de diversos controles. Uma das ações é a aplicação de um algoritmo de criptografia forte. A criptografia deve ser usada para proteger dados em trânsito e enquanto estiver sendo armazenado. Outras técnicas para garantir confidencialidade incluem a ocultação de dados, a exclusão segura dos dados após o uso e o uso de sistemas de autorização e autenticação fortes²⁴⁸; Integridade quando existe uma alteração acidental ou não autorizado dos dados pessoais. Disponibilidade deve garantir a acessibilidade a todo o hardware, software e dados através dos sistemas. O conceito de disponibilidade inclui hardware, dados, conexões e transmissões em alta disponibilidade²⁴⁹. A disponibilidade é também garantida através da redução das vulnerabilidades em sistemas computacionais, sejam elas quais forem e Propriedade de estar acessível e utilizável quando demanda por uma entidade autorizada²⁵⁰.

Mesmo antes do início da vigência do Regulamento Geral de Proteção de Dados Pessoais na Europa, em maio de 2018 e logo após sua entrada em vigor, tem-se noticiado

²⁴⁶ RBADMIN, RGPD – **Violação de Dados: Cia (Confidencialidade, Integridade e Acessibilidade)**. [Em linha]. [Consult. 2 maio 2019]. Disponível em WWW:<URL:https://www.rbconsulting.pt/tag/rgpd/>.

²⁴⁷ ALERTA SECURITY. Os Pilares da Segurança da Informação. [28 Mar 2016]. [Em linha]. [Consult. 2 maio 2019]. Disponível em WWW:<URL:https://alertasecurity.com.br/blog/31-base-capitulo-1-os-pilares-da-seguranca-da-informacao>.

²⁴⁸ RBADMIN, RGPD – **Violação de Dados: Cia (Confidencialidade, Integridade e Acessibilidade)**. [s.d.].

²⁴⁹ *Idem* – **Op. Cit.**

²⁵⁰ PALMA, Fernando - **CID: Confidencialidade, Integridade e Disponibilidade**. [Em linha]. [Consult. 2 maio 2019]. Disponível em WWW:<URL:https://www.portalgsti.com.br/2016/11/cid-confidencialidade-integridade-e-disponibilidade.html>.

diversos acontecimentos de violação de dados pessoais de grande monta os quais serão aqui considerados:

O Diário de Notícias, em Portugal, 28 de março de 2018, revelou que três utilizadores do serviço de mensagens instantâneas do Facebook (Messenger) iniciaram um processo judicial contra a rede social fundada por Mark Zuckerberg por alegada violação de privacidade. O Facebook reconheceu que começou em 2015 a fazer 'upload' (envio de dados de um computador local para um computador remoto) das chamadas e das mensagens de texto dos telefones com o sistema operativo Android (desenvolvido pela empresa de tecnologia Google).²⁵¹

Em abril de 2018 a imprensa disseminou que a Cambridge Analytica teve acesso indevido a dados de 63 mil utilizadores portugueses do Facebook. O Facebook, admitiu que, afinal, terão sido lesados 87 milhões de utilizadores e não 50 milhões, cujas informações privadas foram partilhadas sem autorização com a empresa de marketing digital, que é acusada de ter utilizado para elaborar um programa informático destinado a influenciar o voto dos eleitores, nomeadamente nas últimas eleições presidenciais norte-americanas, que ditaram a nomeação de Donald Trump para a Casa Branca, e no referendo sobre o 'Brexit'. Um dos países mais afetados com os Estados Unidos a liderar a tabela (70,6 milhões de pessoas lesadas). Seguem-se as Filipinas (1,175 milhões), Indonésia (1,096 milhões) e o Reino Unido (1,079 milhões).²⁵²

Em 03 de junho de 2018, o Centro Hospitalar do Barreiro Montijo (CHBM), em Lisboa foi alvo de acesso irregular a dados clínicos, onde foram criados "falsos perfis médicos" para acesso ao sistema informático clínico, que serão usados por assistentes sociais da instituição que, assim, "passaram a ter acesso ao processo clínico dos doentes e a registar aí as suas observações", é uma matéria "de enorme importância", podendo estar em causa a segurança dos dados clínicos e dos dados pessoais dos doentes e também dos médicos. Os Inquéritos vão ser conduzidos pela Comissão de Proteção de Dados e pela Inspeção-Geral das Atividades em Saúde²⁵³.

²⁵¹ RUVIC, Dado - **Três utilizadores processam Facebook** [Em linha]. [Consult. 2 maio 2019]. Disponível em WWW:<URL:https://www.dn.pt/media/interior/facebook-tres-utilizadores-processam-rede-social-por-alegada-violacao-de-privacidade-9220044.html>.

²⁵² LAM, Stephen - **Cambridge Analytica pode ter usado dados de 63 mil utilizadores portugueses**. [Em linha]. [Consult. 2 maio 2019]. Disponível em WWW:<URL:https://www.dn.pt/media/interior/cambridge-analytica-pode-ter-usado-dados-de-63-mil-utilizadores-portugueses-9235928.html>.

²⁵³ RENASCENÇA - **Acesso irregular a dados do Hospital do Barreiro “pode não ser caso único” e vai ser investigado**. [Em linha]. [Consult. 2 maio 2019]. Disponível em WWW:<URL:https://rr.sapo.pt/noticia/117635/acesso-irregular-a-dados-do-hospital-do-barreiro-pode-nao-ser-caso-unico-e-vai-ser-investigado>.

A Comissão Nacional de Proteção de Dados (CNPd) aplicou coimas num valor de 400 mil euros ao Centro Hospitalar Barreiro-Montijo, devido às políticas de acesso às bases de dados, que permitiam que técnicos e médicos consultassem processos clínicos dos doentes sem a devida autorização. A CNPD também justificou a aplicação das coimas com o facto de estarem registados 985 médicos com contas ativas que davam acesso aos ficheiros clínicos, apesar de os quadros do Hospital do Barreiro apenas contarem com 296 médicos (a disparidade entre número de contas e número de médicos estará relacionada com as passagens temporárias determinadas pelo sistema de colocação dos profissionais de saúde). A deliberação da CNPD identificou três infrações: violação do princípio da integridade e confidencialidade, violação do princípio da minimização de dados que deveria impedir o acesso indiscriminado a dados clínicos dos doentes, e incapacidade do responsável pelo tratamento dos dados para assegurar a confidencialidade e a integridade dos dados. As duas primeiras infrações foram punidas com coima 150 mil euros cada, enquanto a terceira representou um acréscimo de 100 mil euros²⁵⁴.

No espaço de cinco meses foram comunicados à Comissão Nacional de Proteção de Dados (CNPd) 123 casos de violação de dados pessoais. São quebras de segurança reportadas por empresas e entidades públicas desde maio, quando entrou em vigor o Regulamento Geral de Proteção de Dados, contudo o número real será muito superior, mas a CNPD vive com uma crónica falta de meios, que a impedem de fazer a fiscalização que manda a lei, assim propalou o Jornal de Notícias em 08 de dezembro de 2018²⁵⁵.

Em janeiro de 2019, a autoridade nacional encarregada pela proteção de dados da França (CNIL)²⁵⁶, instituída em 1978, ou seja, há nada menos que quatro décadas²⁵⁷, impôs uma multa de 50 milhões de euro (R\$ 216 milhões) ao Google por problemas no tratamento de dados de seus usuários, como falta de transparência, informações inadequadas e insuficiências de obtenção de consenso para a personalização de anúncios. Foi a primeira vez que o órgão aplicou

²⁵⁴ SÉNECA, Hugo - **CNPd: Hospital do Barreiro multado em 400 mil euros por permitir acessos indevidos a processos clínicos**. [Em linha]. [Consult. 01 Nov. 2018]. Disponível em WWW:<URL: <http://exameinformatica.sapo.pt/noticias/mercados/2018-10-19-CNPd-Hospital-do-Barreiro-multado-em-400-mil-euros-por-permitir-acessos-indevidos-a-processos-clinicos>>.

²⁵⁵ FIGUEIRA, Alexandra - **Todos os dias há uma violação de dados pessoais**. [Em linha]. [Consult. 2 maio 2019]. Disponível em WWW:<URL: <https://www.jn.pt/inovacao/interior/todos-os-dias-ha-uma-violacao-de-dados-pessoais-10146047.html>>.

²⁵⁶ CNIL - Commission. Nationale de l'Informatique et des Libertés. **Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelle**.

²⁵⁷ “A implementação da referida autoridade se deu por meio da Lei n. 78-17 de janeiro de 1978, conhecida como a Loi Informatique et Libertés. Tal diploma legal sofreu diversas alterações com o passar dos anos para se adaptar a novas demandas e textos legais, bem como para se adequar ao Regulamento Europeu sobre a Proteção de Dados”. ITS - **Proposta para a criação da Autoridade Brasileira de Proteção aos Dados Pessoais**. [Em linha]. [Consult. 2 maio 2019]. Disponível em WWW:<URL: <https://itsrio.org/wp-content/uploads/2018/12/autoridade-protecao-de-dados.pdf>>.

a multa no valor máximo previsto pela legislação²⁵⁸. As informações sobre o tratamento de dados que será feito por meio do uso da referida conta, segundo a CNIL, não são facilmente acessíveis. Informações essenciais, tais como a finalidade do tratamento e a duração da conservação dos dados encontram-se espalhadas em diversos documentos e só são encontradas após diversas etapas, exigindo do usuário um grau de esforço rechaçado pelo Regulamento. As informações fornecidas pelo Google não são claras e compreensíveis, de modo que os usuários não são capazes de entender a amplitude dos tratamentos realizados pelo Google, que, de acordo com a autoridade, são “massivos e intrusivos, em razão do número de serviços propostos, da quantidade e da natureza dos dados tratados e combinados”.²⁵⁹

O pilar do Regulamento de proteção de dados, o Consentimento, deve ser específico em função da finalidade a que se propõe, o consentimento de forma genérica fere o Regulamento Geral de Proteção de Dados. O Google concebe o consentimento de seus usuários como presumido, contrariando o Regulamento, o que ensejou o arbitramento das coimas. Ademais, a autoridade estima que o consentimento também não é específico e inequívoco, já que os usuários são obrigados a explorar diversos documentos fornecidos pelo Google para que ter acesso à opção de não consentir com o tratamento para fins de publicidade personalizada. Ou seja, o ato de consentimento não é um “ato positivo”. Pelo contrário, o padrão adotado na política da empresa considera-o presumido²⁶⁰.

A autoridade nacional de proteção de dados francesa (“CNIL”), consideram as violações perpetradas pelo Google de natureza grave, além de ocorrerem de forma recorrente e não pontual e atingirem um número altamente expressivo de usuários. A autoridade também reitera que o tratamento de dados pessoais é uma das principais atividades desempenhadas pelo do Google, o que deveria resultar em atenção especial à conformidade da empresa ao GDPR.

A empresa Altaba, formada pela venda da Yahoo à Verizon, foi condenada nos Estados Unidos à multa de U\$ 35.000.000,00, em razão da Yahoo não ter comunicado o vazamento de dados de ao menos 500 milhões de usuários ainda em 2014¹, além disso, o

²⁵⁸ VALENTE, Jonas - **França aplica multa máxima ao Google por violação de legislação**. [Em linha]. [Consult. 2 maio 2019]. Disponível em WWW:<URL:<http://agenciabrasil.ebc.com.br/internacional/noticia/2019-01/franca-aplica-multa-maxima-ao-google-por-violacao-de-legislacao>>.

²⁵⁹ OLIVEIRA, Jaqueline Simas de - **Google é multado em 50 milhões de euros na França por violação ao GDPR**. [Em linha]. [Consult. 2 maio 2019]. Disponível em WWW:<URL:<https://www.jota.info/opiniao-e-analise/artigos/google-e-multado-em-50-milhoes-de-euros-na-franca-por-violacao-ao-gdpr-24012019>>.

²⁶⁰ *Idem* – **Op. Cit.**

referido vazamento gerará indenização estimada em 50 milhões de dólares para cerca de 200 milhões de pessoas, vítimas do vazamento, onde a comunicação somente ocorreu em 2016²⁶¹.

A UBER, por sua vez, em outubro de 2016 teve dados vazados de 57 milhões de usuários e motoristas em todo o mundo. A empresa demorou um ano para comunicar a respeito do incidente e esta postura já lhe custou um acordo com o governo dos Estados Unidos em US\$ 500.000.000,00 e R\$ 4,5 milhões a autoridades de proteção de dados da Holanda e Reino Unido³. No Brasil, a UBER é investigada pelo Ministério Público do Distrito Federal e Territórios (MPDFT) a respeito do mesmo vazamento²⁶².

No Brasil, o Banco Inter, após uma ação civil pública, firmou acordo com o Ministério Público do Distrito Federal e Territórios, por vazar dados pessoais de cerca de 19 mil correntistas, onde dados cadastrais tais como nome, CPF, CNPJ, agência, número de contas de pessoas físicas e jurídicas foram expostas na internet²⁶³. O Banco pagará uma multa de R\$ 1.500.000,00. Sendo 1 milhão destinados a órgãos públicos, que combatem crimes cibernéticos e R\$ 500.000,00 a instituições de caridade. O acordo não previu indenização aos correntistas. Segundo a Promotoria a ação visou reparar danos morais coletivos de caráter nacional decorrentes do vazamento de dados²⁶⁴.

A Secretaria Nacional do Consumidor, do Ministério da Justiça e Segurança Pública, instaurou processo administrativo contra o Google Brasil depois de receber denúncia do Ministério Público Federal²⁶⁵. Há indícios de violação à privacidade dos consumidores brasileiros na análise do conteúdo dos e-mails pessoais, enviados pelo Gmail, sem o consentimento expresso do usuário e o processo vai apurar se houve, realmente, violação a dispositivos do Marco Civil da Internet e do Código de Defesa do Consumidor. A denúncia partiu do Ministério Público Federal do Piauí, que entrou com ação judicial em 2016²⁶⁶.

Pela lei brasileira, os dados pessoais são invioláveis e só podem ter seu sigilo levantado por ordem judicial ou consentimento expresso e destacado do interessado. A empresa foi

²⁶¹ HENRIQUE, Lygia Maria M.; ANDRADE, Vitor Moraes - **Vazamento de dados: uma preocupação da Lei Geral de Proteção de Dados** [Em linha]. [Consult. 01 nov. 2018]. Disponível em WWW:<URL:<<https://www.migalhas.com.br/dePeso/16,MI298452,101048-vazamento+de+dados+uma+preocupacao+da+Lei+Geral+de+Protecao+de+Dados>>.>

²⁶² *Idem* – **Op. Cit.**

²⁶³ SOPRANA, Paula - **Banco Inter fecha acordo e pagará R\$ 1,5 milhão por vazamento de dados** [Em linha]. [Consult. 23 dez. 2018]. Disponível em WWW:<URL:<<https://www1.folha.uol.com.br/tec/2018/12/banco-inter-pagara-multa-de-r-15-milhao-por-vazamento-de-dados.shtml>>.>

²⁶⁴ *Idem* – **Ibidem.**

²⁶⁵ MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA - **Senacon instaura processo contra a Google Brasil**. [Em linha]. [Consult. 23 dez. 2018]. Disponível em WWW:< <https://www.justica.gov.br/news/collective-nitf-content-1549544998.05>>.

²⁶⁶ *Idem* – **Op. Cit.**

oficiada em razão da informação de que analisa o conteúdo dos e-mails com objetivos comerciais, ou seja, para produzir publicidade específica para determinado usuário²⁶⁷.

Inúmeros fatos de violação de dados sucedem nos diversos cantos do mundo, uma vez que estamos num mundo globalizado, com uma economia digital universal, e por conseguinte a violação de dados transcende a Europa, mesmo dispondo de uma legislação de ponta, com cunho de proteção de dados pessoais dos cidadãos, não se pode negar que a violação de dados pessoais por parte de grandes empresas é fato, é real, e, traz consequências consideráveis atingindo bens personalíssimos como o direito à privacidade e intimidade, direitos esses inalienáveis, imprescritíveis e irrenunciáveis.

Em todos os casos trazidos a colação temos, em sua grande maioria, os gigantes da internet como protagonistas da ação de violação de dados de seus usuários. Os dados coletados dos usuários, sem seu consentimento expresso foi disseminado para outras grandes empresas com intuito meramente publicitário e comercial, incorrendo em flagrante desrespeito à legislação vigente o que ocasionou penalização pelas autoridades aplicando sanções pecuniárias. Os gigantes da internet Facebook, Google, Instagram, entre outros têm o compromisso, o comprometimento de salvaguardar os dados pessoais de seus usuários, que depositam neles sua confiança de que seus dados não seriam levemente repassados a terceiros por puro interesse comercial, é imprescindível o uso eticamente responsável dos dados que o usuário lhes confia. O consentimento qualificado é a pedra angular da relação no mundo virtual e esta deve ser honrada na forma do artigo 4.º-11 do RGPD, consentimento inequívoco, claro e adstrito às finalidades específicas que justificam o tratamento de dados.

A violação de dados pessoais está longe de findar, mesmo com a legislação protetiva, tem-se descortinado um cenário de muitas dúvidas por parte das empresas. Noticiou o Jornal de notícias, em Portugal, que num espaço de cinco meses, foram comunicados à Comissão Nacional de Proteção de Dados (CNPd) 123 casos de violação de dados pessoais e 186 queixas. Estes casos são considerados como quebras de segurança reportadas por empresas e entidades públicas desde 25 de maio, quando entrou em vigor o Regulamento Geral de Proteção de Dados. A CNPD sofre de falta de recursos humanos para se fazer a fiscalização que manda a lei²⁶⁸.

²⁶⁷ POMPEU, Ana - **MJ instaura processo contra Google Brasil por violação de privacidade**. [Em linha]. [Consult. 01 nov. 2018]. Disponível em WWW:<URL:https://www.conjur.com.br/2019-fev-07/ministerio-abre-processo-google-violacao-privacidade#author>.

²⁶⁸ PORTUGAL SEM MEIOS DE PROTEÇÃO DE DADOS PESSOAIS, CNPD ALERTA O AGRAVAMENTO DA SITUAÇÃO. [Em linha]. [Consult. 30 abr. 2018]. Disponível em WWW:<URL:https://jornaleconomico.sapo.pt/noticias/portugal-sem-meios-de-protecao-de-dados-pessoais-cnpd-alerta-o-agravamento-da-situacao-375383>.

Observou-se da mesma forma que, em nome do novo Regulamento Geral de Proteção de Dados, algumas entidades públicas em Portugal, inovaram, dando uma interpretação desacertada ao RGPD diferente do fim a que se destina, quando em seus contratos públicos com diversas entidades privadas, passaram a adotar a “omissão” de nomes das partes envolvidas (formas de identificação). “A maioria das instituições públicas, incluindo ministérios (como o Ministério da Justiça), autarquias (Lisboa, Porto, Sintra...), empresas públicas (como a Infraestruturas de Portugal), direções-gerais ou até tribunais tapam quase tudo o que são dados pessoais, **nomeadamente os nomes dos representantes das empresas**”²⁶⁹. Sem embargo, a Comissão Nacional de Proteção de Dados, se posicionou no sentido de que o princípio da transparência deve prevalecer fazendo com que as partes envolvidas no contrato estejam devidamente identificadas.

Na Áustria, em outubro de 2018 uma casa de apostas obteve a primeira multa de 4.800 Euros por ter uma câmara de vigilância que gravava parte da calçada, onde a vigilância em larga escala de espaços públicos é proibida pelo Regulamento.²⁷⁰

A autoridade nacional encarregada pela proteção de dados francesa (“CNIL”), em 15 de abril de 2019 veiculou relatório de atividades de 2018²⁷¹ e das edições de 2019 onde concluiu que a entrada em vigor do RGPD, trouxe uma consciência inédita de questões de proteção de dados para profissionais e particulares. Resultando num aumento de reclamações para a CNIL. Em 2018, recebeu um número recorde de 11.077 reclamações, sendo 32,5% a mais em relação ao ano de 2017, sendo o ano de 2018 considerado um ano excepcional para a proteção de dados.

Foi realizada em abril uma pesquisa do IFOP²⁷² onde foi levantado que 70% dos cidadãos franceses estão mais perceptíveis no que se refere a proteção de dados do que nos últimos anos. E, uma das maiores reclamações (35,7%) dizia respeito ao pedido dos usuários da internet para remoção de dados tais como nomes, fotos, contas, vídeos etc. O que exprime a dificuldade das pessoas para exercerem o seu direito de gerir sua vida digital e notadamente sua

²⁶⁹ “A proteção de dados pessoais é para ser levada a sério, mas não pode servir como desculpa para não publicitar informação necessária ao controlo democrático da atividade das entidades públicas”. **ESTADO TAPA NOMES EM CONTRATOS PÚBLICOS. PROTEÇÃO DE DADOS DIZ QUE “NÃO FAZ QUALQUER SENTIDO”**. TSF Radio Noticias. [Consult. 04 maio 2019]. Disponível em WWW:<URL:<<https://www.tsf.pt/sociedade/interior/estado-tapa-nomes-em-contratos-publicos-protecao-de-dados-diz-que-nao-faz-qualquer-sentido-10783457.html>>.>

²⁷⁰ BLOG DE PROTECCIÓN DE DATOS PARA EMPRESAS Y AUTÓNOMOS - **Cuál fue el importe de la multa a las primeras empresas que incumplieron el RGPD?** [Em linha]. [Consult. 04 maio 2019]. Disponível em WWW:<URL:<https://protecciondatos-lopd.com/empresas/multa-empresas-incumplieron-rgpd/#Nuevos_importes_para_2019>.>

²⁷¹ CNIL. **Présentation du Rapport d’activité 2018 et des enjeux 2019 de la CNIL** [Em linha]. [Consult. 7 maio 2019]. Disponível em WWW:<URL:<<https://www.cnil.fr/fr/presentation-du-rapport-dactivite-2018-et-des-enjeux-2019-de-la-cnil>>.>

²⁷² Institut d’Etudes Opinion et Marketing en France et a l’International.

reputação on line. O ano 2019 será decisivo para dar credibilidade ao novo quadro jurídico e transformar esta ambiciosa aposta europeia em sucesso operacional. As expectativas da sociedade civil e dos atores econômicos são muito fortes e esse modelo desperta interesse em todo o mundo. A CNIL articulará sua ação em torno de dois eixos principais: pedagogia e dissuasão.²⁷³

Como se pode verificar a figura da Autoridade Europeia para a Proteção de Dados (AEPD) foi criada em 2004 em Bruxelas, e sempre foi e ainda é considerada de grande relevância para garantir que todas as instituições e organismos da UE respeitem o direito à privacidade dos cidadãos quando processam os seus dados pessoais. Na forma do artigo 52.º do RGPD, age com total independência nas suas atribuições e no exercício de seus poderes. Tem como atuação o controle do tratamento dos dados pessoais, a fim de garantir o cumprimento das regras de privacidade; aconselha as instituições e os organismos da UE sobre todos os aspetos do tratamento dos dados pessoais, das políticas e da legislação neste domínio; processa queixas e conduz inquéritos; trabalha com as autoridades nacionais dos países da UE para garantir coerência na proteção de dados; monitoriza as novas tecnologias suscetíveis de ter um impacto em matéria de proteção de dados²⁷⁴.

É mais um meio que o cidadão Europeu tem para invocar na hipótese do seu direito à privacidade ter sido violado por uma instituição ou um organismo da U.E, após ter contactado em primeira linha o responsável pelo tratamento de dados, se o resultado for insatisfatório e apelado ao encarregado da proteção de dados da instituição ou do organismo da UE onde pensa que foi cometida a infração. Se ainda assim restar infrutífero o caminho percorrido, poderá ainda apresentar queixa à AEPD (Autoridade Europeia para a Proteção de Dados), valendo-se do preenchimento de um formulário que levará a Autoridade Europeia para a Proteção de Dados investigar o caso e informá-lo-á da sua decisão quanto ao fundamento da queixa e à forma de corrigir a situação. Se apesar disso não concordar com a decisão da AEPD, pode remeter a questão para o Tribunal de Justiça da União Europeia²⁷⁵.

²⁷³Versão original: “L’année 2019 sera décisive pour crédibiliser le nouveau cadre juridique et transformer cet ambitieux pari européen en succès opérationnel. Les attentes de la société civile et des acteurs économiques sont très fortes et ce modèle suscite des intérêts à travers le monde. La CNIL articulera son action autour de deux axes principaux : la pédagogie et la dissuasion”. CNIL. **Présentation du Rapport d’activité 2018 et des enjeux 2019 de la CNIL**. [s.d.].

²⁷⁴UNIÃO EUROPEIA. **Autoridade Europeia para a Proteção de Dados (AEPD)**. [Em linha]. [Consult. 7 maio 2019]. Disponível em WWW:<URL:https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_pt>.

²⁷⁵UNIÃO EUROPEIA. **Autoridade Europeia para a Proteção de Dados (AEPD)**. [s.d.].

3.2 Direito ao esquecimento

O direito ao esquecimento, também chamado direito a ser esquecido, é o direito das pessoas físicas a fazer com que se apague a informação sobre elas depois de um período determinado. A internet traz consigo a necessidade de um novo equilíbrio entre a livre difusão da informação e a autodeterminação individual. Este equilíbrio é precisamente o que está em jogo com o direito ao esquecimento.²⁷⁶

O conceito de autodeterminação informativa tem igualmente contribuído para orientar a atividade do intérprete, ao reconhecer a autonomia do indivíduo tanto dirigida ao controle e à transmissão de informações personalíssimas como encaminhada à possibilidade de acesso a qualquer informação. Fundamental para identificar uma efetiva proteção às informações pessoais dos indivíduos numa sociedade informatizada é a possibilidade de que o controle sobre o armazenamento e a transmissão de dados possa ser realizado pelo titular da informação. O próprio armazenamento de dados pessoais está informado por um princípio de acesso amplo aos titulares das informações, seja para o reconhecimento de existência do próprio registro, seja para a verificação da extensão, veracidade e correção das informações armazenadas²⁷⁷.

A internet não esquece. Ao contrário dos jornais e revistas de outrora, cujas edições antigas se perdiam no tempo, sujeitas aos desgastes do seu suporte físico, as informações que circulam na rede ali permanecem indefinidamente. Pior: dados pretéritos vêm à tona com a mesma clareza dos dados mais recentes, criando um delicado conflito no campo do direito. De um lado, é certo que o público tem direito a lembrar fatos antigos. De outro, embora ninguém tenha direito de apagar os fatos, deve-se evitar que uma pessoa seja perseguida, ao longo de toda a vida, por um acontecimento pretérito²⁷⁸.

O direito ao esquecimento teve início na esfera das condenações criminais, onde buscava-se garantir ao prisioneiro, após cumprir toda a sua pena a possibilidade de se ver ressocializado na sociedade, procurando esquecer as memórias do delito cometido, sob pena de violar o princípio da dignidade da pessoa humana. É bem verdade que a existência de crimes que causaram comoção social, na maioria das vezes permanece na memória da sociedade, não

²⁷⁶ TERWANGNE, Cécile - Privacidad en Internet y el derecho a ser olvidado/derecho al olvido. [Em linha]. [Consult. 13 maio 2019]. Disponível em WWW:<URL:<http://www.redalyc.org/articulo.oa?id=78824460006>>.

²⁷⁷ CACHAPUZ, Maria Cláudia Mércio - Privacidade, proteção de dados e autodeterminação informativa [Em linha]. [Consult. 19 maio 2019]. Disponível em WWW:<URL:<https://revistajuridica.presidencia.gov.br/index.php/saj/article/view/126/118>>.

²⁷⁸ SCHREIBER, Anderson - **Direito da personalidade**. 2. ed. São Paulo: Atlas, 2013. ISBN. 978-85.224-7895-8, p. 170.

tendo o apenado o direito de requerer o apagamento das informações sobre o caso. Nesses casos, há de se mitigar a relação dos direitos envolvidos em prol do interesse da sociedade.

Como direito humano e direito fundamental, o assim chamado direito ao esquecimento encontra sua fundamentação na proteção da vida privada, honra, imagem e ao nome, portanto, na própria dignidade da pessoa humana e na cláusula geral de proteção e promoção da personalidade em suas múltiplas dimensões ²⁷⁹.

A abordagem desse tema, nos remete ao emblemático, caso ocorrido em 2012 na Espanha envolvendo Google Spain SL, Google Inc e Agencia Espanhola de Protección de Datos (AEPD) e o cidadão espanhol Mario Costeja González, fato que acabou por desaguar nas águas do Tribunal de Justiça da União Europeia, do qual o acórdão proferido fez eclodir em toda a comunidade debates sobre o direito ao esquecimento propriamente dito, resvalando inclusive na América Latina com repercussões de grande monta, já que as empresas envolvidas tem atuação global por valer-se da internet atingindo os 5 continentes.

O leading case González, C-131/12, originou-se quando em 5 de março de 2010 o cidadão espanhol M. Costeja González, protocolou uma reclamação junto a Agência Espanhola de Protección de Datos (AEPD) contra o jornal La Vanguardia e contra a Google Spain e a Google Inc., pelo fato de que quando um internauta inseria o nome “M. Costeja González”, num motor de busca num site do grupo do Google, imediatamente era remetido para duas páginas daquele jornal, respectivamente, 19 de janeiro e 9 de março de 1998, nas quais figurava um anúncio de uma venda de imóveis em hasta pública decorrente de um arresto com vista à recuperação de dívidas à Seguridad Social, que mencionava o nome de M. Costeja González ²⁸⁰.

O autor postulava que o jornal La Vanguardia retirasse ou modificasse as páginas para que seus dados pessoais não fossem divulgados, ou buscasse formas nos motores de buscas para que ficassem protegidos. Em relação à Google Spain e a Google Inc. que suprimissem ou ocultassem os seus dados pessoais, para que deixassem de aparecer nos resultados de pesquisa e de figurar nos links da La Vanguardia. Teve como embasamento de que o problema anterior referente ao arresto fora resolvido há vários anos atrás, e que a sua manutenção acabou por lhe

²⁷⁹ SARLET, Ingo Wolfgang - **Tema da moda, direito ao esquecimento é anterior à internet** [Em linha]. [Consult. 13 maio 2019]. Disponível em WWW:<URL:<https://www.conjur.com.br/2015-mai-22/direitos-fundamentais-tema-moda-direito-esquecimento-anterior-internet>>.

²⁸⁰ EUROPA. Tribunal de Justiça da União Europeia. Acórdão do Tribunal de Justiça (Grande Secção) de 13 de maio de 2014. **Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González**. [Em linha]. [Consult. 13 maio 2019]. Disponível em WWW:<URL:<https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0131>>.

causar diversos constrangimentos por ter revivido um passado já esquecido, que a época lhe causou muita dor e embaraço²⁸¹.

Em 30 de julho de 2010 a AEPD não acolheu o pleito de La Vanguardia, tendo em vista que o Ministério do Trabalho e dos Assuntos Sociais determinou maior publicidade para angariar o maior número de licitantes. Contudo foi dado provimento em relação à Google Spain e à Google Inc., provedores, eis que operadores de motores de busca estariam sujeitos à legislação em matéria de proteção de dados, uma vez que realizam um tratamento de dados pelo qual são responsáveis e atuam como intermediários da sociedade de informação²⁸².

A AEPD considerou que os operadores de motores de busca estão sujeitos à legislação em matéria de proteção de dados, uma vez que realizam um tratamento de dados pelo qual são responsáveis e atuam como intermediários da sociedade de informação, estando habilitada a ordenar a retirada dos dados e a interdição de aceder a determinados dados, por parte dos operadores de motores de busca, quando considere que a sua localização e a sua difusão são suscetíveis de lesar o direito fundamental de proteção dos dados e a dignidade das pessoas em sentido amplo, o que abrange também a simples vontade da pessoa interessada de que esses dados não sejam conhecidos por terceiros²⁸³.

Os provedores de motores de busca recorreram questionando quais as obrigações dos operadores de motores de busca para efeitos da proteção de dados pessoais das pessoas interessadas, que não tencionem que determinadas informações, publicadas em sítios web de terceiros e que contêm os seus dados pessoais, que permitem ligar essas informações a essas pessoas, sejam localizadas, indexadas e postas à disposição dos internautas indefinidamente²⁸⁴.

O órgão jurisdicional, levantou a necessidade de uma minuciosa análise da Diretiva 95/46/CE, em vigor, o que levou a suspensão da instância pela Audiência Nacional submetendo ao Tribunal de Justiça, as questões prejudiciais para melhor elucidação. A primeira questão prejudicial a ser apreciada dizia respeito à aplicação territorial da Diretiva 95/46 e a legislação espanhola em matéria de proteção de dados, em seguida a segunda questão prejudicial relacionada à atividade do motor de busca como fornecedor de conteúdos tendo em conta a

²⁸¹ EUROPA. Tribunal de Justiça da União Européia. Acórdão do Tribunal de Justiça (Grande Secção) de 13 de maio de 2014. **Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González**. [Em linha]. [Consult. 13 maio 2019]. Disponível em WWW:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0131>.

²⁸² CONSALTER, Zilda Mara – **Direito ao Esquecimento**. 2017. p. 202.

²⁸³ EUROPA. Tribunal de Justiça da União Européia. Acórdão do Tribunal de Justiça (Grande Secção) de 13 de maio de 2014. **Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González**. [s.d.].

²⁸⁴ *Idem* – **Op. Cit.**

Diretiva 95/46 relativa à proteção de dados, e a terceira que diz respeito ao direito de apagamento e/ou de oposição em conjugação com o ‘direito a ser esquecido’²⁸⁵.

Em referência a segunda questão prejudicial aludida em relação ao âmbito de aplicação material da Diretiva 95/46, a Google Spain e a Google Inc., replicaram, segundo transcrito no acórdão de que a atividade dos motores de busca não pode ser considerada um tratamento dos dados que aparecem nas páginas web de terceiros exibidas na lista de resultados da pesquisa, dado que esses motores tratam as informações acessíveis na Internet, no seu conjunto, sem fazer a seleção entre os dados pessoais e as outras informações. Além disso, mesmo admitindo que esta atividade deva ser qualificada de “tratamento de dados”, o operador de um motor de busca não pode ser considerado “responsável” por esse tratamento, uma vez que não conhece os referidos dados nem exerce controlo sobre os mesmos²⁸⁶.

O Tribunal se manifestou recorrendo que M. Costeja González, os Governos espanhol, italiano, austríaco e polaco e a Comissão Europeia entendem que a referida atividade implica claramente um “tratamento de dados” na aceção da Diretiva 95/46, que é distinto do tratamento de dados efetuado pelos editores de sítios *web* e prossegue objetivos diferentes deste. O operador de um motor de busca é responsável pelo tratamento de dados efetuado por esse motor, uma vez que é ele que determina a finalidade e os meios desse tratamento, considerando que o artigo 2.o, alínea d), da Diretiva 95/46 define esse responsável como “a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais”²⁸⁷.

Mediante as extensas argumentações o Tribunal concluiu no sentido de que se não há relevância na conexão do nome aos fatos pretéritos, não há que se proteger a informação, devendo haver a supressão das mesmas²⁸⁸. Em que pese, o acórdão ter mantido seu entendimento de que os operadores de motores de busca têm o dever de desindexar as informações relativas ao caso em questão, percebe-se também que o acórdão mitigou o direito do titular dos dados de ver seus dados apagados alicerçado na supremacia do interesse público em detrimento do privado, assim consignou o Tribunal: “No entanto, não será esse o caso se se

²⁸⁵ EUROPA. Tribunal de Justiça da União Européia. Acórdão do Tribunal de Justiça (Grande Secção) de 13 de maio de 2014. **Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González**. [Em linha]. [Consult. 13 maio 2019]. Disponível em WWW:<URL:<https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0131>>.

²⁸⁶ *Idem* – **Op. Cit.**

²⁸⁷ EUROPA. Tribunal de Justiça da União Européia. Acórdão do Tribunal de Justiça (Grande Secção) de 13 de maio de 2014. **Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González**. [s.d.].

²⁸⁸ CONSALTER, Zilda Mara – **Direito ao Esquecimento**. 2017. p. 203.

afigurar que, por razões especiais como, por exemplo, o papel desempenhado por essa pessoa na vida pública, a ingerência nos seus direitos fundamentais é justificada pelo interesse preponderante do referido público em ter acesso à informação em questão, em virtude dessa inclusão”²⁸⁹. O requerimento de desindexação autorizado pela decisão europeia é apenas uma das expressões do exercício do direito ao esquecimento e não o direito em si²⁹⁰.

A sentença foi imperativa no sentido de estabelecer requisitos mínimos para o reconhecimento do direito ao esquecimento em relação aos gestores dos motores de busca da internet onde o interessado deverá fornecer os elementos, tais como endereços eletrônicos, os links, informação detalhada, motivação do interesse do bloqueio, entre outros dados. Os parâmetros assentes visam auxiliar as agências de proteção de dados e até mesmo o poder judiciário para viabilizar um juízo de ponderação de valores tendo em vista os interesses envolvidos que deverão ser sopesados: liberdade de expressão, o direito de informar contrapondo-se ao direito à privacidade e intimidade em prol da dignidade da pessoa humana.

Assim sendo, o direito ao esquecimento adquiriu reconhecimento jurisprudencial em âmbito internacional, e as solicitações devem ser apresentadas pelo interessado diretamente ao buscador, que deverá examinar o pedido e atender ou não o solicitado²⁹¹.

A Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas, prevê no artigo 6º-1 o direito ao esquecimento está previsto quando os dados deixarem de ser necessários para efeitos da transmissão da comunicação estes devem ser eliminados ou tornados anónimos²⁹².

Em seguida, com vistas a uniformização de normas entre os Estados-membros, foi editado Regulamento (UE) 2016/679, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, revogando a Diretiva 95/46/CE.

Analisando-se o Direito do esquecimento contemplado Regulamento Geral de Dados Pessoais, temos o artigo 5º-1-e, verifica-se o limite da conservação dos dados, ou seja, instrumentalizando o titular dos dados pessoais para pleitear o apagamento ou exclusão dos

²⁸⁹ EUROPA. Tribunal de Justiça da União Européia. Acórdão do Tribunal de Justiça (Grande Secção) de 13 de maio de 2014. **Google Spain SL e Google Inc. contra Agência Española de Protección de Datos (AEPD) e Mario Costeja González**. [s.d.].

²⁹⁰ VIDIGAL, Leonardo Bruno Marinho- **O Direito ao Esquecimento e a Incipiente Experiência Brasileira: Incompreensões sobre o Tema, limites para sua Aplicação e a Desafiadora Efetivação no Ambiente Virtual**. Rio de Janeiro: Pontifícia Universidade Católica do Rio de Janeiro, 2017. Dissertação de Mestrado, p. 22.

²⁹¹ *Idem* – **Op. Cit.** p. 203.

²⁹² UNIÃO EUROPEIA. Directiva 2002/58/CE do Parlamento Europeu e do Conselho. **Relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas 12 de Julho de 2002**. [Em linha]. [Consult. 18 mar. 2019]. Disponível em WWW:<URL:<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=EN>>.

dados uma vez cumpridas sua finalidade. O artigo 17 do Regulamento Geral de Proteção de Dados, consagra de forma explícita o direito a ser esquecido (direito ao apagamento dos dados), onde o titular dos dados pessoais tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem obrigação de apagar os dados pessoais sem tardar²⁹³.

O direito ao esquecimento pode ser caracterizado como uma esfera de proteção, uma redoma, que permitiria que uma pessoa não autorizasse a divulgação de um fato que lhe diga respeito, ainda que verídico, por causar-lhe sofrimento ou algum transtorno, levando-se em consideração a utilidade e a data da ocorrência em que a informação, objeto de proteção, foi realizada.²⁹⁴

Dessa forma, é incontestável que a pessoa tem o dever legal de gerir a recolha e a proficuidade dos dados das pessoas envolvidas, tendo, de toda sorte, o livre arbítrio para que os fatos ocorridos no passado não sejam ressuscitados de forma descontextualizada o que fatalmente causará sofrimento.

Atualmente as pessoas são instigadas à constante exposição e ao permanente resgate de fatos e atos pretéritos, dando a impressão de que é pecaminoso esquecer o que quer que seja. Outro elemento importante desse fenômeno é o de que igual realidade se averigua por todo o globo, ao que parece ser uma epidemia mundial: a da necessidade de ser celebridade e de ser constantemente visto, notado e “curtido”: as selfies criadas para a replicação por milhares de pessoas, as atividades corporativas, as páginas de relacionamento e outros fenômenos hoje em evidência forçam até aquele ser humano mais discreto a de, alguma forma, exhibir/divulgar alguma faceta de sua existência. E a cibernética veio para acentuar tudo o que há de bom e de ruim nisso.²⁹⁵

As ferramentas de busca na internet, aplicativos que identificam e reconhecem pessoas pela fisionomia gravada em um enorme banco de imagens, as câmeras de vigilância em locais públicos e privados, entre outros, todos formam e formatam uma realidade em que é quase impossível esquecer²⁹⁶.

²⁹³ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Em linha]. [Consult. 15 mai. 2018]. Disponível em WWW:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679.

²⁹⁴ MARTINEZ, Pablo Dominguez - **Direito ao Esquecimento - A proteção da memória individual na sociedade da informação**. Rio de Janeiro: Lumen Juris, 2014. ISBN 978-8584401055, p. 58.

²⁹⁵ CONSALTER, Zilda Mara – **Direito ao Esquecimento**. 2017. p. 171.

²⁹⁶ *Idem* – **Op. Cit.** p. 172.

As mudanças tecnológicas mudam esse paradigma. Com computadores e aparelhos eletrônicos, lembrar, ao invés de esquecer aumenta o padrão. Ferramentas de busca gravam toda a pesquisa para aumentar sua performance, e tem somente recentemente iniciado o ato de apagar as antigas gravações dos seus servidores. As atualizações de status dos usuários em páginas sociais, os transitórios tweets são transformados em registros permanentes. Os sistemas de pesquisa buscam todos os registros na internet. Os telefones celulares e serviços de e-mail geram logs das conversas, por mais mundanas e “esquecíveis” que possam ser. E não é preciso ser uma celebridade para ser constantemente lembrado²⁹⁷.

O direito a ser esquecido é reservado para o direito de ter os dados pessoais on line retirados, ou conseguir restrição ou impedimento no acesso a esses dados restritos, especialmente no contexto de aplicações geradas pelo próprio usuário ou outrem, incorporando direitos relativos à indexação de dados dos motores de busca²⁹⁸.

A direito ao esquecimento despontou no século XX, onde emergia a proteção da intimidade das pessoas, dado isso alguns casos chegaram as raias do Tribunal sendo certo que não com a utilização dessa expressão, mas de fácil percepção a natureza dos julgados que dizia respeito ao direito ao esquecimento.

Foi a partir dessa construção jurisprudencial em países como Alemanha, França, Estados Unidos que se chegou ao conceito do direito ao esquecimento referenciado de forma como veremos a seguir de forma implacável no Regulamento Geral de Dados da União Europeia. Todavia, embora o novo rótulo, em termos gerais, a ideia subjacente ao assim chamado direito ao esquecimento é bem mais antiga e guarda relação com o já clássico conflito que tantas vezes se estabelece entre a proteção da personalidade e outros bens jurídicos, como a segurança e o interesse público etc. e a liberdade de expressão e informação²⁹⁹.

A França em 1983 deu o primeiro passo aclamando na jurisprudência Francesa, o Tribunal de Grande Instance de Paris, legitimou o direito ao esquecimento de forma perceptível: “considerando que qualquer pessoa que se tenha envolvido em acontecimentos públicos pode, com o passar do tempo, reivindicar o direito ao esquecimento; a lembrança destes acontecimentos é ilegítima se não for fundada nas necessidades da história ou se for de natureza a ferir sua sensibilidade; visto que o direito ao esquecimento, que se impõe a todos, inclusive

²⁹⁷ CONLEY, Chris *apud* CONSALTER, Zilda Mara – **Direito ao Esquecimento**. 2017. p. 174.

²⁹⁸ CONSALTER, Zilda Mara – **Direito ao Esquecimento**. 2017. p. 183.

²⁹⁹ SARLET, Ingo Wolfgang - **Tema da moda, direito ao esquecimento é anterior à internet**. [Em linha]. [Consult. 13 maio 2019]. Disponível em WWW:<URL:<https://www.conjur.com.br/2015-mai-22/direitos-fundamentais-tema-moda-direito-esquecimento-anterior-internet>>.

aos jornalistas, deve igualmente beneficiar a todos, inclusive aos condenados que pagaram sua dívida para com a sociedade e tentam reinserir-se nela”³⁰⁰.

Na Alemanha, o famoso caso emblemático: caso Lebach – Uma Reclamação Constitucional, contra decisão judicial, em 05/06/1973, cidade Lebach, distrito de Sarre, em 1969 ocorreu um latrocínio de quatro soldados Alemães, tendo sido condenados à prisão perpétua dois acusados, e um terceiro partícipe a seis anos de reclusão, tendo ampla cobertura pela imprensa e televisão locais. O latrocínio passou a ser conhecido como o “assassinato de soldados de Lebach” . Quatro soldados, que guardavam um depósito de munição, foram, durante a noite, brutalmente assassinados, um quinto foi gravemente ferido³⁰¹. Armas e munições foram roubadas. Os dois principais acusados foram condenados, em agosto de 1970, à prisão perpétua. O reclamante foi condenado, por tê-los auxiliado na preparação da ação criminosa, a seis anos de reclusão. A ZDF (*Zweites Deutsches Fernsehen* – Segundo Canal Alemão), atenta ao grande interesse da opinião pública no caso, produziu um documentário sobre todo o ocorrido. No documentário, além dos dois condenados à prisão perpétua, também o reclamante era apresentado com foto e nome, para depois serem representados por atores com detalhes da relação dos condenados entre si, incluindo suas ligações homossexuais, dos acontecimentos da noite do crime e, finalmente, da sua perseguição e prisão pela polícia. O documentário deveria ser transmitido em uma sexta-feira à noite, pouco antes da soltura do reclamante. As tentativas do reclamante de conseguir em juízo uma medida liminar que pudesse impedir a transmissão do programa resultaram infrutíferas: tanto o Tribunal Estadual de Mainz quanto o Superior Tribunal Estadual de Koblenz julgaram improcedente o pedido do reclamante³⁰².

O TCF (Tribunal Constitucional Federal) julgou procedente a Reclamação Constitucional por vislumbrar uma violação perpetrada pelos tribunais do direito de desenvolvimento da personalidade (Art. 2 I GG) e, por consequência, por considerar que uma intervenção na liberdade de radiodifusão, que se consubstanciaria na proibição de transmissão determinada pelos tribunais competentes (no caso de deferimento do pedido do reclamante) restaria, neste caso, justificada. O TCF, portanto, revogou as decisões dos tribunais civis e

³⁰⁰ OST, Francis *apud* CONSALTER, Zilda Mara – **Direito ao Esquecimento**. 2017. p. 197-8.

³⁰¹ SCHWABE, Jürgen - **Cinqüenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Montevideo: Konrad – Denauer Stiftung, 2005. ISBN: 9974794218, p. 487.

³⁰² *Idem* – **Op. Cit.** p. 487.

proibiu a ZDF de transmitir o documentário até a decisão final da ação principal pelos tribunais ordinários competentes³⁰³.

A fundamentação da decisão merece relevância já que se faz necessário sopesar a colisão de bens jurídicos envolvidos: a necessidade de informar a população e o direito da personalidade do transgressor, concluindo com ressalvas já que a informação a população é imprescindível e deve se sobrepor sobre o direito de personalidade do criminoso, mas ao mesmo tempo, há de se respeitar a esfera íntima da vida do criminoso, baseado no princípio da proporcionalidade. Segundo este, a informação do nome, foto ou outra identificação do criminoso nem sempre é permitida. A proteção constitucional da personalidade, porém, não admite que a televisão se ocupe com a pessoa do criminoso e sua vida privada por tempo ilimitado e além da notícia atual, p.ex. na forma de um documentário³⁰⁴. Um noticiário posterior será, de qualquer forma, inadmissível se ele tiver o condão, em face da informação atual, de provocar um prejuízo considerável novo ou adicional à pessoa do criminoso, especialmente se ameaçar sua reintegração à sociedade (ressocialização). A ameaça à ressocialização deve ser em regra tolerada quando um programa sobre um crime grave, que identificar o autor do crime, for transmitido [logo] após sua soltura ou em momento anterior próximo à soltura³⁰⁵.

A solução do conflito deve partir do pressuposto de que, segundo a vontade da Constituição, ambos os valores constitucionais configuram componentes essenciais da ordem democrática livre da Grundgesetz, de forma que nenhum deles pode pretender a prevalência absoluta. Os valores constitucionais devem ser, por isso, em caso de conflito, se possível, harmonizados; se isso não for atingido, deve ser decidido, considerando-se a configuração típica e as circunstâncias especiais do caso particular, qual dos dois interesses deve ser preterido. Ambos os valores constitucionais devem ser vistos, em sua relação com a dignidade humana, como o centro do sistema axiológico da Constituição. Resumindo, tem-se que um noticiário sobre um crime com os nomes [verdadeiros], fotos ou representação dos acusados, principalmente na forma de documentário, significará em regra uma intervenção grave na sua esfera [privada] da personalidade.³⁰⁶

Em 1931, o Tribunal de Apelação da Califórnia, no importante caso *Melvin versus Reid*, reconheceu a existência de um direito ao esquecimento em favor de Gabrielle Darley, uma ex-prostituta que no passado fora acusada de homicídio, porém absolvida em 1918. Posteriormente

³⁰³ SCHWABE, Jürgen - **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. 2005. p. 487.

³⁰⁴ *Idem* – ***Ibidem***.

³⁰⁵ *Idem* – ***Op. Cit.*** p. 488.

³⁰⁶ *Idem* – ***Op. Cit.*** p. 491-2.

ela se casou com Bernard Melvin, levando uma vida digna e honrada e merecendo a admiração e o bom conceito das pessoas conhecidas. Em 1925, um produtor de cinema de nome Reid fez um filme baseado na biografia daquela mulher, com destaques para as suas características sensuais e o processo criminal a que respondera. Aquele tipo de publicidade causou enorme dor moral à apelante Gabrielle, com reflexos em sua saúde, levando-a a postular na Justiça uma reparação pela grave ofensa ao seu direito à intimidade da vida passada. E o tribunal condenou o autor do agravo a uma indenização como forma material de reparação, apesar de não se referir, literalmente, à existência de um direito ao esquecimento³⁰⁷.

A história, registra inúmeros casos onde o direito ao esquecimento foi o protagonista em diversas demandas, retrocedendo ao famoso leading case “Right to be let alone” de Samuel D. Warren e Louis D. Brandeis, onde foi criando-se farta jurisprudência em diversos países, elevando-o a categoria de direitos fundamentais.

No Brasil, também tem-se notícia de casos de pessoas conhecidas que buscaram o isolamento, exercendo o seu direito de “let to be alone”, não admitindo dar entrevistas e sequer participar de programas nos diversos meios de comunicação de massa. Em especial sobre o direito ao esquecimento, de forma mais particular o leading case Chacina da Candelária, que foi julgado no Superior Tribunal de Justiça (STJ) pela lavra do Acórdão do Ministro Luis Felipe Salomão.

O objeto da demanda foi a reconstituição do crime denominado “Chacina da Candelária” ocorrido em 23 de julho de 1993 de grande repercussão internacional, em um programa da Rede Globo intitulado “Linha Direta”, treze anos após o fato, sem autorização expressa de uma das partes envolvidas. O autor da demanda foi indiciado como coautor dos homicídios ocorridos em 23 de julho de 1993, respondeu processo criminal, tendo sido absolvido por negativa de autoria, por unanimidade pelo conselho de sentença do Tribunal do Júri. O processo teve como partes a Globo Comunicações e Participações S/A, na qualidade de Ré e Jurandir Gomes de França como autor.

O Autor reivindicou uma ação de dano moral por entender que a exposição de sua imagem e nome no mencionado programa foi ilícita e causou-lhe intenso abalo moral, essa situação o prejudicou sobremaneira em sua vida profissional, não tendo mais conseguido emprego, além de ter sido obrigado a desfazer-se de todos os seus bens e abandonar a

³⁰⁷ DOTTI, René Ariel. **Proteção da vida privada e liberdade de informação: possibilidades e limites**. São Paulo: Revista dos Tribunais, 1980. ISBN: 978-8520300367, p. 90-1.

comunidade para não ser morto por "justiceiros" e traficantes e também para proteger a segurança de seus familiares, assim consignou o Ministro relator³⁰⁸.

O Juízo *a quo* julgou improcedente o pedido autoral em relação ao direito ao anonimato e ao esquecimento e quanto ao reconhecimento do dano moral, fundamentado no direito de informação da população por um caso com requinte de crueldade afetando a imagem da cidade do Rio de Janeiro, não só a nível nacional, mas resvalando a nível internacional. Inconformado, o autor recorreu aos Tribunais superiores, que reconheceu o dano moral sofrido pelo autor embasado no princípio da dignidade humana sustentando “ 2ª instância que reformou a sentença por maioria reconhecendo o dano moral, lastreado no princípio constitucional da dignidade da pessoa humana, fundamento da República brasileira, sustentando que constituiu abuso do direito de informar e violação da imagem do cidadão a edição de programa jornalístico contra a vontade expressamente manifestada de quem desejava prosseguir no esquecimento”³⁰⁹.

Inconformada, a Ré, Globo Comunicações e Participações S.A., recorreu ao Superior Tribunal de Justiça (STJ) visando a reforma da sentença sob o argumento de que não houve invasão da privacidade/intimidade do autor porque os fatos eram públicos e foram amplamente debatidos pela sociedade, tendo se limitado a expor os fatos como aconteceram. Sintetizou o recorrente-Rede Globo, que "o simples fato da pessoa se relacionar com a notícia ou fato histórico de interesse coletivo já é suficiente para mitigar seu direito à intimidade, tornando lícita a divulgação de seu nome e de sua imagem independentemente de autorização"³¹⁰.

O voto do Ministro Luís Felipe Salomão foi emblemático, por referenciar o direito ao esquecimento no ordenamento jurídico brasileiro, assevera o Ministro:

“Com efeito, o reconhecimento do direito ao esquecimento dos condenados que cumpriram integralmente a pena e, sobretudo, dos que foram absolvidos em processo criminal, além de sinalizar uma evolução cultural da sociedade, confere concretude a um ordenamento jurídico que, entre a memória – que é a conexão do presente com o passado – e a esperança – que é o vínculo do futuro com o presente –, fez clara opção pela segunda. E é por essa ótica que o direito ao esquecimento revela sua maior nobreza, pois afirma-se, na verdade, como um direito à esperança, em absoluta sintonia com a presunção legal e constitucional de regenerabilidade da pessoa humana”³¹¹.

Concluindo, a despeito da Chacina da Candelária ter se tornado – com muita razão – um fato histórico, que expôs as chagas do País ao mundo, tornando-se símbolo da precária proteção

³⁰⁸ BRASIL. Superior Tribunal de Justiça. **REsp. nº 1.334.097 RJ** [Em linha]. [Consult. 13 maio 2019]. Disponível em

WWW:<URL:https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=29381336&num_registro=201201449107&data=20130910&tipo=91&formato=PDF>.

³⁰⁹ *Idem* – **Op. Cit.**

³¹⁰ *Idem* – **Op. Cit.**

³¹¹ *Idem* – **Op. Cit.** p. 9.

estatal conferida aos direitos humanos da criança e do adolescente em situação de risco, o certo é que a fatídica história seria bem contada e de forma fidedigna sem que para isso a imagem e o nome do autor precisassem ser expostos em rede nacional³¹². Nem a liberdade de imprensa seria tolhida, nem a honra do autor seria maculada, caso se ocultassem o nome e a fisionomia do recorrido, ponderação de valores que, no caso, seria a melhor solução ao conflito³¹³.

O direito ao esquecimento no Brasil, não tem uma regulação própria, nem mesmo na legislação de proteção de dados pessoais, mas foi reconhecido no Enunciado 531³¹⁴ da VI Jornada de Direito Civil promovida pelo Conselho da Justiça Federal (CJF) em março de 2013, sendo considerado uma orientação doutrinária: “*A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento*”, motivado sob o argumento de que “os danos provocados pelas novas tecnologias de informação vêm-se acumulando nos dias atuais”. O direito ao esquecimento nasceu na área penal, a partir das sentenças criminosas, onde buscava-se a ressocialização do preso, após o cumprimento de sua pena. Muitos condenados, mesmo após cumprirem sua pena foram discriminados e tiveram dificuldades de ingressar no mercado de trabalho em função de ficarem marcados, principalmente quando os crimes tiveram repercussão nacional nas diferentes mídias. O direito ao esquecimento nesse contexto é uma forma de apagar da memória um fato que marcou um indivíduo e que mesmo após ter cumprido sua pena ainda o assombra.

Sendo assim, o direito ao esquecimento não atribui a ninguém o direito de apagar fatos ou reescrever a própria história, mas apenas assegura a possibilidade de discutir o uso que é dado aos fatos pretéritos, mais especificamente o modo e a finalidade com que são lembrados³¹⁵.

A VI jornada de Direito Civil realizada em novembro de 2011³¹⁶, através do enunciado 404 assim garante que “A tutela da privacidade da pessoa humana compreende os controles espacial, contextual e temporal dos próprios dados, sendo necessário seu expresso consentimento para tratamento de informações que versem especialmente o estado de saúde, a condição sexual, a origem racial ou étnica, as convicções religiosas, filosóficas e políticas.

³¹² BRASIL. Superior Tribunal de Justiça. **REsp. nº 1.334.097 RJ** [Em linha]. [Consult. 13 maio 2019]. Disponível em

WWW:<URL:<https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=29381336&num_registro=201201449107&data=20130910&tipo=91&formato=PDF>.

³¹³ *Idem* – **Op. Cit.**

³¹⁴ CONSELHO DA JUSTIÇA FEDERAL. **VI Jornada de Direito Civil** [Em linha]. [Consult. 14 maio 2019]. Disponível em WWW:<URL:<<https://www.cjf.jus.br/enunciados/enunciado/142>>.

³¹⁵ *Idem* – **Op. Cit.**

³¹⁶ CONSELHO DA JUSTIÇA FEDERAL. **VI Jornada de Direito Civil**. [Em linha]. [Consult. 14 Maio 2019]. Disponível em WWW:<URL:<<https://www.cjf.jus.br/enunciados/enunciado/362>>.

O Artigo 17 do Regulamento Geral de Proteção de Dados³¹⁷ como já mencionado anteriormente institui o Direito ao apagamento dos dados («direito a ser esquecido»), onde o titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada. O direito ao apagamento dos dados pessoais, pode ser entendido como relativo, por estar adstrito as condições previstas no diploma legal.

O direito ao esquecimento incorpora uma expressão de controle temporal de dados e preenche com o fator cronológico o requisito de ferramenta protetiva da privacidade. Está incluído na proteção à privacidade, que tem como fundamento a Constituição Federal de 1988, mais especificamente no artigo 5º, incisos X, XI e XII, como também o ordenamento infraconstitucional, no artigo 21 do Código Civil³¹⁸.

A ideia central que norteia a noção de um direito ao esquecimento diz com a pretensão das pessoas, físicas e mesmo jurídicas, no sentido de que determinadas informações (aqui compreendidas em sentido amplo) que lhes dizem respeito, especialmente àquelas ligadas aos seus direitos de personalidade, ou, no caso das pessoas jurídicas, à sua imagem e bom nome, não sejam mais divulgadas de modo a impedir sejam objeto de acesso por parte de terceiros ou pelo menos que o acesso a tais informações seja dificultado, tudo de modo a propiciar uma espécie de esquecimento no corpo social³¹⁹.

O impacto da decisão proferida pelo Tribunal de Justiça da União Europeia tem reflexos até os dias atuais. Compulsando o relatório de transparência do motor de busca da internet, Google³²⁰, tem-se a informação de 803.957 solicitações de remoção e 3.135.663 URLs (*Uniform Resource Locator*), com solicitações de remoção até 01 janeiro de 2019. Sendo o número de URLs removidos após a revisão o percentual de 44,6% que corresponde a 1.203.639 e 55,4% corresponde a 1.496.807 não removidos no período de 29/05/2014 a

³¹⁷ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Em linha]. [Consult. 15 nov. 2018]. Disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679>.

³¹⁸ MORAES, Melina Ferracini – **Direito ao Esquecimento na Internet**. Curitiba: Juruá, 2018. ISBN 978-85-362-8204-6, p.57.

³¹⁹ SARLET, Ingo Wolfgang - **Tema da moda, direito ao esquecimento é anterior à internet** [Em linha]. [Consult. 13 maio 2019]. Disponível em WWW:<URL:<https://www.conjur.com.br/2015-mai-22/direitos-fundamentais-tema-moda-direito-esquecimento-anterior-internet>>.

³²⁰ “Em uma decisão de maio de 2014, o Tribunal de Justiça da União Europeia considerou que os indivíduos têm o direito de solicitar que mecanismos de pesquisa, como o Google, removam determinados resultados sobre eles. O relatório apresenta dados sobre o volume de solicitações, os URLs removidos, os solicitantes, o conteúdo dos sites e os URLs identificados nas solicitações”. TRANSPARENCY REPORT. **Remoções da pesquisa em cumprimento da legislação europeia sobre privacidade**. [Em linha]. [Consult. 17 maio 2019]. Disponível em WWW:<URL:https://transparencyreport.google.com/eu-privacy/overview?requests_over_time=country:PT&lu=delisted_urls&delisted_urls=start:1401321600000;end:1558051200000;country>.

17/05/2019. Não são incluídas solicitações de remoção de URLs que estão com a revisão pendente ou precisam de informações adicionais para serem processadas. O domínio facebook foi o que teve o maior número de URLs removidos da pesquisa Google, com o total de URLs solicitadas 51.298 e URLs removidas 21.295, seguidas do annuaire.118712.fr, twitter.com, www.youtube.com e profileengine.com.

A título ilustrativo e exemplificativo registraremos algumas solicitações relevantes do ano de 2016, contidas no site de Transparência do gigante tecnológico Google³²¹, a cerca de remoção de conteúdo por parte de pessoas que identificaram suas informações nos sites de pesquisa. A solicitação de remoção do conteúdo é equacionada pelo provedor sopesando o direito da pessoa interessada na remoção com o interesse público do conteúdo em questão.

Na Alemanha, foi solicitado a remoção de quatro artigos de notícias sobre uma pesquisa acadêmica que continha a foto de um indivíduo porque ele passou por uma mudança de gênero e se identificava com um novo nome. Os artigos não foram removidos porque foram considerados relevantes para a vida profissional e pesquisa do estudante.

Na Espanha a solicitação foi de um indivíduo para remover uma notícia de 1994 e uma postagem em um fórum de 2007 sobre a participação do solicitante em atividades com chefe do braço político de uma organização terrorista identificada pelo Estado. O artigo não foi removido por razões de interesse público.

Na Itália, a solicitação foi de remoção de dezenas de notícia recentes de fontes confiáveis sobre a condenação de um indivíduo por estupro, incluindo imagens de vídeo da vítima. Inicialmente, a solicitação foi recusada e a Autoridade Italiana de Proteção de Dados interviu requerendo uma explicação ao Google sobre a decisão. O Google prosseguiu com a recusa por se tratar de crime grave, o que foi acatado pela Autoridade Italiana de Proteção de Dados.

Na Bélgica, o pedido foi de uma Autoridade Belga de Proteção de dados para remover cinco URLs da pesquisa Google que descrevem um incidente em que o agressor atacou violentamente uma vítima. O autor do crime foi condenado. Foi removido três URLs que não continham o nome do autor do crime, mas foi recusado a remover dois URLs que o mencionavam.

Em breve análise, deduz-se que a preservação e proteção da identidade das pessoas afetadas está diretamente relacionada com a gravidade dos fatos e/ou o interesse público onde o provedor, detentor da informação é que dita as normas se remove ou não o conteúdo ainda

³²¹ TRANSPARENCY REPORT. **Remoções da pesquisa em cumprimento da legislação europeia sobre privacidade.** [s.d].

que com as justificativas apresentadas em respeito com os critérios exigidos pelo Grupo de Trabalho do artigo 29.º na análise do exercício do direito ao esquecimento, não bastando a simples decisão do titular dos dados pessoais.

Estamos diante do empoderamento dos provedores do mundo virtual que não só armazenam como têm acesso irrestrito aos dados que circulam na internet, através das redes sociais, motores de busca etc., o que leva a espionagem massiva de dados pessoais por diversas agências de segurança ao redor do mundo, como já foi anunciado anteriormente.

3.2.1 Limitações ao exercício do direito ao esquecimento digital

Antes de adentrarmos nas limitações ao exercício do direito ao esquecimento, mister se faz consignar que internet vem sendo um instrumento eficaz na fabricação e disseminação da informação. Estamos no terceiro milênio da chamada Sociedade Informacional devido a velocidade e a quantidade numerosa de informações que circulam na internet e que são compartilhadas em frações de segundo por milhares de pessoas ao redor do mundo.

De fato, nas sociedades de informação em que vivemos, pode-se dizer que “nós somos as nossas informações”, pois que elas nos definem, nos classificam, nos etiquetam; portanto, ter como controlar a circulação das informações e saber quem usa significa adquirir, concretamente, um poder sobre si mesmo³²². A sociedade da informação, portanto, muda e dita comportamentos, regendo as formas de comunicação, os relacionamentos interpessoais, o consumo e a própria vida em sociedade³²³.

Estamos inseridos numa sociedade democrática que tem como princípios assegurar o exercício dos direitos sociais e individuais, a liberdade, a segurança, o bem-estar, o desenvolvimento, a igualdade e a justiça como valores supremos de uma sociedade fraterna, pluralista e sem preconceitos, fundada na harmonia social e comprometida, na ordem interna e internacional³²⁴.

O direito do esquecimento manifestou-se para garantir a pessoa humana o direito à autodeterminação informacional, de forma a empoderar o titular dos dados pessoais no total controle do fluxo de suas informações, podendo solicitar seu apagamento, restrição ou

³²² RODOTÀ, Stefano - **A Vida na Sociedade de Vigilância – A privacidade hoje**. Rio de Janeiro: Renovar, 2008. ISBN 978857147-688-2, p. 7.

³²³ Martins, Guilherme Magalhães - O direito ao esquecimento na internet e a proteção dos consumidores. **Revista Luso-Brasileira de Direito do Consumo**. Curitiba. 7:25 (2017), 61-99.

³²⁴ BRASIL. **Constituição da República Federativa do Brasil**, de 05 de outubro de 1988. [Em linha]. [Consult. 05 de jan. de 2018]. Disponível em WWW: <URL: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.html>.

retificação desde que não fira interesses públicos e de segurança nacional. Podendo ser definido como o direito da pessoa de apagar informações pretéritas suas e que não têm nenhum interesse público, ou seja, algo que não fere o direito à informação ou à liberdade de expressão e que, também, respeita os princípios constitucionalmente protegidos da intimidade, da vida privada, da honra e da imagem das pessoas³²⁵.

Nessa rota conclui-se que o direito ao esquecimento não será ilimitado e isolado, ao contrário, este direito deve ser contextualizado para que seja reconhecido quando não estiver em conflito com outros direitos igualmente tutelados, tais como, direito de acesso à informação, direito de liberdade de expressão, livre manifestação do pensamento artístico, literário, científico, dentre outros³²⁶. Negar a existência do direito ao esquecimento é admitir pena de caráter perpetuo. O direito ao esquecimento guarda relação direta com a privacidade que permite ao cidadão de se manter na solidão, no anonimato, na reserva ou na intimidade³²⁷.

A aplicação do direito ao esquecimento, como um desdobramento do direito da personalidade, tido como um direito fundamental do indivíduo, que como se sabe, não tem o condão de ser absoluto, requerendo a utilização da técnica de ponderação de valores com vistas a conciliar interesses, analisando a circunstância de cada caso de per si, tendo sempre como valor supremo a dignidade da pessoa humana, sendo que nem sempre o direito ao esquecimento prevalecerá sobre os demais direitos em foco.

Desta feita, as restrições a um direito fundamental, dar-se-ão em obediência a alguns requisitos como muito bem elencou Nelson Nery³²⁸ Junior, relacionando uma série de requisitos para que possa haver restrição a um direito fundamental: a) a restrição deve estar constitucionalmente prevista, ou seja, autorizada por algum dispositivo constitucional b) a restrição deverá ser proporcional de modo que não se aniquile o direito constitucional objeto da restrição c) a restrição deve atender ao interesse social, privilegiando outros interesses previstos na Constituição d) o ato do Poder Público que restringe um direito fundamental deve ser exaustivamente fundamentado de forma a demonstrar que a escolha pela restrição do direito é a melhor possível e) os atos do Poder Público que restringir direitos fundamentais podem ser analisados pelo Poder Judiciário, em razão de não haver discricionariedade administrativa que autorize a violação de direitos fundamentais.

³²⁵ FRANCEZ, André. **Direito do entretenimento na Internet**. São Paulo: Saraiva, 2013. ISBN: 9788502208391, p. 201.

³²⁶ LIMA, Cíntia Rosa Pereira de – **Direito ao esquecimento e internet: o fundamento legal no direito comunitário europeu, no direito italiano e no brasileiro**. Revista dos Tribunais. São Paulo. p. 97.

³²⁷ CHEHAB, Gustavo - O direito na sociedade da informação. **Revista dos Tribunais**. 104:952 (2015), p. 90.

³²⁸ NERY JUNIOR; Nelson. NERY; Rosa Maria de Andrade. **Constituição Federal Comentada e Legislação Constitucional**. 4. ed. São Paulo: Revista dos Tribunais, 2013. ISBN: 9788520347416, p. 216.

O Regulamento Geral de Proteção de Dados da União Europeia, no artigo 17º destaca de forma objetiva o direito ao esquecimento, com a ressalva no item 3.º dos limites ao direito do apagamento nos casos em que o tratamento dos dados se revele necessário ao exercício da liberdade de expressão e informação; ao cumprimento de uma obrigação legal; para o exercício da Autoridade Pública ou funções de Interesse Público; para fins de investigação científica ou histórica ou para fins estatísticos; para exercício ou defesa de um direito num processo judicial³²⁹.

3.2.1.1 Liberdade de expressão e liberdade de informação

A primeira limitação em relação ao direito do esquecimento, está relacionada a liberdade de expressão e a liberdade de informação, (direito de informar e ser informado), devendo para tanto se ter o cuidado de não desaguar na alegação de censura ou afronta a livre manifestação do pensamento. Deve-se ponderar muito bem o direito (ou dever) de divulgar fatos relevantes no ambiente informacional e o resguardo ao direito à intimidade e proteção à dignidade da pessoa e à inviolabilidade pessoal³³⁰. O direito de expressão é livre, diga-se, mas seu exercício tem limitações³³¹.

O respeito a liberdade de expressão tem sua previsão na Carta de Direitos Fundamentais da União Europeia (artigo 11.º-1 e 2)³³² e na Constituição dos diversos países de regime democrático, e na Declaração Universal dos Direitos do Homem, artigo 19³³³ “toda pessoa tem direito à liberdade de, sem interferências, ter opiniões e procurar, receber e transmitir informações por quaisquer meios, independentemente de fronteiras”.

A doutrina é pacífica no entendimento de que liberdade de expressão e liberdade de informação são distintos, não podendo ser concebidos como direitos absolutos, os limites

³²⁹ UNIÃO EUROPEIA - Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Em linha]. [Consult. 15 nov. 2018]. Disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679>.

³³⁰ CONSALTER, Zilda Mara – **Direito ao Esquecimento**. 2017. p. 303.

³³¹ NETO, Antonio Rulli; JUNIOR, Antonio Rulli - Direito ao Esquecimento e o Superinformacionismo: Apontamentos no Direito Brasileiro dentro do Contexto de Sociedade da Informação. **Revista do Instituto do Direito Brasileiro**, 1:1 (2012), 419-34. [Em linha]. [Consult. 13 maio 2019]. Disponível em WWW:<URL:<https://blook.pt/publications/publication/296c62416268/>>.

³³² UNIÃO EUROPEIA - **Carta dos Direitos Fundamentais da União Europeia**. [Em linha]. [Consult. 01 fev. 2018]. Disponível em WWW: <URL:<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN>>.

³³³ UNIÃO EUROPEIA - **Declaração Universal dos Direitos do Homem**. [Em linha]. [Consult. 01 fev. 2018]. Disponível em WWW: <URL:http://pfdc.pgr.mpf.mp.br/atuacao-e-conteudos-de-apoio/legislacao/direitos-humanos/declar_dir_homem.pdf>.

encontram-se na própria Constituição. A liberdade de expressão está diretamente ligada liberdade de pensamento, de expor suas ideias sem qualquer censura nos mais variados meios de propagar suas opiniões. Já a liberdade de informação diz respeito ao direito individual de comunicar livremente fatos e ao direito difuso de ser deles informado³³⁴. Uma distinção importante entre os dois institutos tem-se a veracidade e a imparcialidade da informação. E é justamente, em razão dessa distinção fundamental que se deve pensar em um direito de informação que seja distinto em sua natureza da liberdade de expressão³³⁵.

Na ponderação de valores tensionados no caso em concreto seria a presença de elementos tais como ausência de contemporaneidade/atualidade e exatidão da informação, a sua veracidade, a manutenção presente do interesse público na divulgação da mesma, a pertinência na divulgação e a completa ausência de abuso no seu uso³³⁶.

No Brasil, tem-se um caso emblemático do Superior Tribunal de Justiça, se contrapondo ao famoso caso da Chacina da Candelária, onde se discutiu a liberdade de informação/expressão e o direito do esquecimento, no julgamento do REsp 1.335.153³³⁷ caso Aída Curi, que entrou para a história, vítima de um homicídio em 1958, de grande repercussão na imprensa, nas redes televisivas, tendo o processo criminal se estendido para discussões nos meios acadêmicos.

Entretanto, 50 anos depois o programa chamado “Linha direta Justiça” transmitido pela Rede Globo de Televisão, veiculou o caso Aída Curi empregando o nome e a imagem da Aída. Os irmãos da vítima, ajuizaram ação de reparação de danos morais contra a Rede globo, pelo fato da emissora “ter reaberto antigas feridas dos autores, veiculando novamente a vida, a morte e a pós-morte de Aída Curi, explorando sua imagem”³³⁸. Consideraram a exploração do caso visando auferir lucros com audiência e publicidade se valendo da tragédia da família, sem ter tido o consentimento.

O juízo de primeira instância julgou improcedente, a sentença foi mantida em grau de apelação pelo Tribunal de Justiça do Estado do Rio de Janeiro, desaguando no Superior Tribunal de Justiça e no Supremo Tribunal Federal. Os irmãos da Aída embasaram o recurso focando no direito ao esquecimento onde vivenciaram uma tragédia na família a cinquenta anos

³³⁴ ASENJO, Porfirio Barroso e TALAVERA, Maria del Mar - La libertad de expresión y sus limitaciones constitucionales. **Revista de Ciencias Sociales y Humanas**, 15 (2011).

³³⁵ CARVALHO, Luis Gustavo Grandinetti Castanho - **Direito de informação e liberdade de expressão**. Rio de Janeiro: Renovar, 1999. ISBN 8571471495, p. 24.

³³⁶ CONSALTER, Zilda Mara – **Direito ao Esquecimento**. 2017. p. 303.

³³⁷ BRASIL. Superior Tribunal de Justiça. **REsp. nº 1.335.153 RJ**. [Em linha]. [Consult. 13 maio 2019]. Disponível em WWW:<URL:https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=29381336&num_registro=201201449107&data=20130910&tipo=91&formato=PDF>.

³³⁸ *Idem* – **Op. Cit.**

atrás, onde a Rede Globo, recorrida, de forma ilícita trouxe à tona toda a dor, sofrimento experimentado pelos familiares da vítima, direito esse que foi violentado pela emissora ré, por ocasião da veiculação da reportagem não autorizada da morte da irmã dos autores.

O Ministro Luís Felipe Salomão, não acolheu a pretensão dos autores por ter entendido que o “cerne do programa foi o crime em si, e não a vítima ou sua imagem. No caso, a imagem da vítima não constituiu um chamariz de audiência, mostrando-se improvável que uma única fotografia ocasionaria um decréscimo ou acréscimo na receptividade da reconstituição pelo público expectador e que durante toda a matéria, o caso Aída Curi foi retratado mediante dramatizações realizadas por atores contratados, tendo havido uma única exposição da imagem real da falecida”, o que por esses motivos foi negado provimento ao recurso.

Contrastando com o famoso caso da Chacina da Candelária, que também teve o caso veiculado no famoso programa “Linha Direta – Justiça, o recurso foi provido acolhendo a tese do direito ao esquecimento, sob o teor argumentativo de que:

“permitir nova veiculação do fato, com a indicação precisa do nome e imagem do autor, significaria a permissão de uma segunda ofensa à sua dignidade, só porque a primeira já ocorrera no passado, uma vez que, como bem reconheceu o acórdão recorrido, além do crime em si, o inquérito policial consubstanciou uma reconhecida "vergonha" nacional à parte. Deveras, os valores sociais ora cultuados conduzem a sociedade a uma percepção invertida dos fatos, o que gera também uma conclusão às avessas: antes de enxergar um inocente injustamente acusado, visualiza um culpado acidentalmente absolvido”³³⁹.

De onde se conclui que não raro o exercício de direito ao esquecimento impõe ponderação com o exercício de outros direitos, como a liberdade de informação, sendo certo que a ponderação nem sempre se resolverá em favor do direito ao esquecimento. O caso concreto deve ser analisado em suas peculiaridades, sopesando-se a utilidade informativa na continuada divulgação da notícia com riscos trazidos pela recordação do fato à pessoa envolvida. Como em outros conflitos já analisados, não há aqui solução simples. Impõe-se, ao contrário, delicado balanceamento entre interesses em jogo³⁴⁰.

Rememorando as reflexões do Desembargador Federal Rogério de Meneses Fialho Moreira, do Tribunal Regional Federal da 5ª Região, em Recife (PE), tendo coordenado a 6ª Jornada de Direito Civil do Conselho da Justiça Federal em março de 2013 em entrevista dada

³³⁹ BRASIL. Superior Tribunal de Justiça. **REsp. nº 1.334.097 RJ**. [Em linha]. [Consult. 13 maio 2019]. Disponível em WWW:<URL:<https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=29381336&num_registro=201201449107&data=20130910&tipo=91&formato=PDF>>.

³⁴⁰ SCHREIBER, Anderson - **Direito da personalidade**. 2013. p. 171-2.

a Agência Brasil³⁴¹, comunga do entendimento doutrinário majoritário da dificuldade em definir em que circunstâncias caberá a aplicação do direito ao esquecimento em detrimento de outros direitos fundamentais. Não obstante, sustenta que uma pessoa possa reivindicar que fatos de sua vida privada não sejam revelados lastreado no princípio constitucional da dignidade da pessoa humana, fundamento vital de uma sociedade democrática de direito, consolidada na Carta de Direitos Fundamentais da União Europeia.

Segue o seu raciocínio asseverando que vivemos em uma sociedade informacional, com nossa privacidade permanentemente exposta, e porque o potencial de danos dos atuais meios de informação é muito maior, hoje é muito mais difícil assegurar a alguém o direito ao esquecimento. Décadas atrás, alguém dava uma declaração a um jornal e aquilo era esquecido com maior facilidade. Não se trata de revisar o passado, reescrever a história ou apagar fatos de interesse jornalístico. O direito ao esquecimento visa a assegurar a vida privada e não a vida pública ou fatos criminosos, por exemplo. Enquanto houver um resíduo de informação de interesse ou relevante para o debate público será possível trazer isso à tona.

O julgamento da relevância de uma informação terá que ser analisado caso a caso e com bom senso. Para ser aplicado, o direito ao esquecimento precisa ser confrontado com outros direitos constitucionais, como o direito à informação e a proibição à censura. Não há como estabelecer previamente por quanto tempo uma informação tem valor público ou as hipóteses em que o direito ao esquecimento se aplica. Vai ser preciso analisar caso a caso, levando em conta também o nível de exposição a que cada pessoa esteve ou está exposta, mas também que há certos aspectos da vida, mesmo que da maior das celebridades, que são estritamente íntimos³⁴².

3.2.1.2 Interesse Público

Em seguida o limite que se impõe é o que diz respeito ao interesse público que por si só é de grande monta porque atinge a sociedade. Caso haja qualquer interesse da população em geral nas informações/fatos/atos nos quais está envolvido o titular deste direito, este não poderá ser concebido como argumento para a proteção de sua intimidade³⁴³. A solução deve residir na constatação da existência ou não de um interesse público atual na divulgação da informação³⁴⁴.

³⁴¹ MOREIRA, Rogério de Meneses Fialho - **Direito ao esquecimento não se confunde com censura**. [Em linha]. [Consult. 17 maio 2019]. Disponível em WWW:<URL:http://agenciabrasil.ebc.com.br/geral/noticia/2014-06/para-sabado-ii-direito-ao-esquecimento-divide-opinioes-de-especialistas>.

³⁴² MOREIRA, Rogério de Meneses Fialho - **Direito ao esquecimento não se confunde com censura**. [s.d.].

³⁴³ CONSALTER, Zilda Mara – **Direito ao Esquecimento**. 2017. p. 296.

³⁴⁴ *Idem* – **Op. Cit.** p. 296.

A internet e as novas tecnologias inverteram os termos da lógica e da regra geral, o esquecimento é agora exceção em um entorno onde o passado se converteu em um presente onipresente³⁴⁵.

Para tecer a ponderação entre o direito ao esquecimento e o interesse público, primeiramente, deverá ser avaliado a atualidade do tema resgatado ao presente, mas acima de tudo, verificar se se trata, efetivamente de assunto de interesse público ou meramente curiosidade do público³⁴⁶.

Por outro lado, dizer que sempre e sempre o interesse público na divulgação de casos judiciais deve prevalecer sobre a privacidade ou intimidade dos envolvidos, pode confrontar a própria letra da Constituição, que prevê solução exatamente contrária, ou seja, de sacrifício da publicidade (art. 5º, inciso LX)³⁴⁷: A lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem³⁴⁸. A restrição ao direito à privacidade ocorre diante da maior relevância de outro direito em detrimento deste, ou em defesa do interesse público³⁴⁹.

3.2.1.3 Memória histórica

O terceiro fator limitante ao direito ao esquecimento é de igual forma o direito à memória, a história de um povo, ou de uma pessoa singular. O direito à memória, ou à verdade histórica não tem um indivíduo como titular, mas si, de modo difuso, tem inúmeros legitimados para reclamá-lo. O direito à memória é mais amplo: cuida do referencial de um povo, de uma nação ou de um indivíduo³⁵⁰.

Não há como negar que certos episódios são insuscetíveis de serem esquecidos. São fatos que se prendem à própria essência de um povo ou de um indivíduo, que marcaram de

³⁴⁵ LOPEZ, Angel Cobacho *apud* CONSALTER, Zilda Mara – **Direito ao Esquecimento**. 2017.

³⁴⁶ CONSALTER, Zilda Mara – **Direito ao Esquecimento**. 2017. p. 300.

³⁴⁷ BRASIL. Constituição da República Federativa do Brasil, de 05 de outubro de 1988. [Em linha]. [Consult. 27 de abr. de 2019]. Disponível em WWW: <URL:http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.html>.

³⁴⁸ BRASIL. Superior Tribunal de Justiça. **REsp. nº 1.335.153 RJ**. [Em linha]. [Consult. 13 maio 2019]. Disponível em WWW:<URL:https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=29381336&num_registro=201201449107&data=20130910&tipo=91&formato=PDF>.

³⁴⁹ DANTAS, Fernanda Lage Alves – **O Paradoxo do Direito à Privacidade e sua Operacionalização**. Rio de Janeiro: Lumen Juris, 2016. ISBN 978-85-8440-852-8, p. 198.

³⁵⁰ *Idem* – **Op. Cit.** p. 310.

forma indelével sua história, que deve ser recontada para formação da identidade cultural do país³⁵¹.

Partindo do Enunciado 531³⁵² relativo ao direito do esquecimento: “A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento.” “Não atribui a ninguém o direito de apagar fatos ou reescrever a própria história, mas apenas assegura a possibilidade de discutir o uso que é dado aos fatos pretéritos, mais especificamente o modo e a finalidade com que são lembrados”³⁵³. Assim, não é qualquer informação que seria eliminada do mundo virtual ou de veículos de informação e busca. Há que se ponderar primeiro se não há naquele fato de que se busca o esquecimento pelo particular interessado, o direito à memória de todo um povo³⁵⁴.

3.2.1.4 Atuação do próprio titular

Como já contextualizado anteriormente vive-se uma cultura do informacionismo, da hiperexposição, do exibicionismo gratuito e inconsequente, da ânsia por eternizar toda e qualquer experiência através das redes sociais, LinkedIn, Twitter, Facebook, Flickr, (um site de hospedagem e compartilhamento de fotos, imagens, ilustrações e etc.), Trumblr (plataforma de blogs), *Whatsapp*, *Instagram*, *Telegram*, *Hangouts* (plataforma de comunicação, desenvolvida pela Google, que inclui mensagens instantâneas, chat de vídeo, SMS e VOIP)³⁵⁵.

Ou seja, hoje, a sociedade em que vivemos disponibiliza os mais diversos meios tecnológicos, através da internet, onde as pessoas passaram a expor sua vida diária nas redes sociais sem qualquer restrição. Estamos de frente do problema do “impulso à auto exposição”, não apenas porque a pessoa participa de uma vida comum com os demais, compartilhando experiência tecnológica e informações próprias a seu tempo, mas, fundamentalmente, porque

³⁵¹ COSTA, Andre Brandão Nery – Direito ao esquecimento na Internet: a Scarlet letter digital in: SCHREIBER, Anderson - **Direito da personalidade**. 2013. p. 206.

³⁵² CONSELHO DA JUSTIÇA FEDERAL. **VI Jornada de Direito Civil** [Em linha]. [Consult. 14 maio 2019]. Disponível em WWW:<URL:<https://www.cjf.jus.br/enunciados/enunciado/142>>.

³⁵³ RODEGHERI, Leticia Bodanese; RAMINELLI, Francieli Puntel; OLIVEIRA, Rafael Santos de – Dignidade da pessoa humana e intimidade na sociedade informacional: o direito ao esquecimento de dados pessoais. In **Congresso Internacional de Direito e Contemporaneidade**, 2 UFSM, 2013, Santa Maria – RS. p. 879-890.

³⁵⁴ CONSALTER, Zilda Mara – **Direito ao Esquecimento**. 2017. p. 313.

³⁵⁵ *Idem* – **Op. Cit.** p. 325-6.

também o indivíduo deseja aparecer e, em determinada medida, fazer-se visto, “por feitos e palavras”, pelos demais³⁵⁶.

Trata-se da limitação do direito ao esquecimento pela renúncia tácita do indivíduo à autodeterminação individual, no campo do direito privado, em que também se requer a análise da colisão do direito à privacidade do indivíduo e o armazenamento de informações por ele mesmo disponibilizadas anteriormente³⁵⁷.

O questionamento que se deve fazer é até que ponto o indivíduo que se expõe nas redes sociais fornecendo informações sobre sua vida privada, que circulam em frações de segundo no ciberespaço, pode valer-se do direito ao apagamento (direito a ser esquecido) sob a alegação da violação aos seus direitos da personalidade e de seus dados pessoais? A exposição, de forma voluntária, sem precedentes, por parte da pessoa, é uma renúncia a esfera mais reservada do indivíduo.

Os usuários da internet não se apercebem que ao acessar um site aceitam os termos e condições impostos pelos provedores, sem ler, e ao consentir, estamos dando carta branca para que possam aceder a todos os dados inseridos nas plataformas. Esses dados são coletados e depois vendidos para empresas e agências de publicidade. Todos os usuários das redes de computadores, smartphones deixam rastros digitais a cada momento em todo o lugar.

No ciberespaço, reiteradamente os indivíduos tendem a acessar uma nova plataforma da internet, a um novo aplicativo ou rede social sem atender as advertências dos riscos de exposição de dados pessoais, privados e íntimos, de maneira que sem perceber, coloca a si mesmo em situação de vulnerabilidade, enquanto os conteúdos privados que publica podem chegar a ser, contra a sua vontade, conhecidos de forma massiva pelo resto dos usuários da rede³⁵⁸. Quanto mais informação é alimentada na rede, através de conversas, compras, fotos, vídeos entre outros, mais munção os usuários abastecem os provedores para comercializarem para terceiros interessados em fornecer produtos e serviços na rede.

No mundo virtual, os fatos ocorridos numa determinada fase da vida do indivíduo, jamais serão esquecidos, apagados, uma vez disparado na internet se propaga em questões de

³⁵⁶ CARELLO, Clarissa; CACHAPUZ, Maria Cláudia - **A Doutrina do “Right to be Forgotten” Pela Perspectiva das Relações Entre Privados**. [Em linha]. [Consult. 17 maio 2019]. Disponível em WWW:<URL:www.ajuris.org.br/OJS2/index.php/REVAJURIS/article/download/.../Ajuris_140_DT3>.

³⁵⁷ CACHAPUZ Apud LIMONG, Cristina de Souza – Limites ao Exercício do Direito ao Esquecimento. **Revista de Direito Brasileira**. 14:6 (2016). [Em linha]. [Consult. 17 maio 2019]. Disponível em WWW:<URL:https://www.indexlaw.org/index.php/rdb/article/view/2982>.

³⁵⁸ TOURIÑO, Alejandro – **El Derecho al olvido y a la intimidad em internet**. Madrid: Catarata, 2014. ISBN 978-84-8319-880-3, p. 21.

segundo, permanecendo armazenado nos motores de busca em todo o ciberespaço de forma permanente.

O uso de imagens, arquivos de texto ou outra forma que possa violar a intimidade da pessoa, em descompasso com a atualidade, pode causar-lhe inúmeros dissabores. Mesmo que tenham sido efetuadas pelo próprio ofendido ou com seu consentimento inicial, seria possível pensar na sua extração da rede, desde que por motivos relevantes e justificados, se aqueles já não mais corresponderem à realidade do indivíduo ou se tornaram de algum modo um inconveniente para aquele ³⁵⁹.

A finalidade do direito ao esquecimento é a garantia da dignidade da pessoa humana, que encontra sérias dificuldades quando o indivíduo convive com a dor e o constrangimento causados pelo passado³⁶⁰. Nessa seara, o direito ao esquecimento deverá prevalecer uma vez que está diretamente relacionado ao direito à privacidade, a honra e o direito à imagem de um indivíduo e que só interessa a ele. A memória coletiva de uma sociedade necessita de proteção, a memória individual carece de ser tutelada. Ninguém está obrigado a conviver com resquícios passados, sem qualquer relevância para os dias atuais, e causadores de sofrimentos³⁶¹.

A tutela do esquecimento deve ser adotada se a exposição se deu sem o consentimento do ofendido, por meio de medidas escusas e condenáveis, como captação de imagens sem permissão, a violação de máquinas por intermédio de programas espões e outras que a tecnologia e a vida moderna permitem³⁶². Internet e redes sociais são o paradigma da exposição pública de vidas privadas³⁶³. O marco das redes sociais facebook, Twiter e Tuenti, faz com que milhares de ciberusuários compartilhem informação livremente, sem dar importância ao fato de que, às vezes, o compartilhado é parte ou está diretamente relacionado à privacidade dos cidadãos. Imagens, vídeos e comentários correm o risco de serem descontextualizados na rede, e o que é mais grave, gozando de uma perenidade que faz com que observados após a data de sua publicação, estes podem comprometer ou condicionar o futuro dos cidadãos³⁶⁴.

³⁵⁹ CONSALTER, Zilda Mara – **Direito ao Esquecimento**. 2017. p. 332.

³⁶⁰ REGO, Giancarlos Coutinho do - **Direito ao Esquecimento: proteção à memória individual** [Em linha]. [Consult. 19 maio 2019]. Disponível em WWW:<URL:<<https://giancarlosregojusbrasil.com.br/artigos/327294577/direito-ao-esquecimento-protecao-a-memoria-individual>>>.

³⁶¹ *Idem* – **Op. Cit.**

³⁶² CONSALTER, Zilda Mara – **Direito ao Esquecimento**. 2017. p. 341.

³⁶³ CASTELLANO, Pere Simon - **O regime constitucional do direito de ser esquecido na internet**. [Em linha]. [Consult. 19 maio 2019]. Disponível em WWW:URL:<https://www.academia.edu/898086/El_r%C3%A9gimen_constitucional_del_derecho_al_olvido_en_Internet>.

³⁶⁴ CASTELLANO, Pere Simon - **Neutralidad de la red y otros retos para el futuro de Internet - Actas del VII Congreso Internacional Internet**. [Em linha]. [Consult. 19 maio 2019]. Disponível em WWW:<URL:<http://www.huygens.es/ebooks/Neutralidad_de_la_red.pdf>>.

CAPÍTULO IV

4 RESPONSABILIDADE CIVIL POR VIOLAÇÃO DE DADOS PESSOAIS A LUZ DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS.

Após discorrermos sobre a proteção de dados pessoais, sobre a privacidade e intimidade, um dos direitos fundamentais do indivíduo, que está diretamente relacionada com os dados pessoais, exploraremos os desdobramentos da violação dos dados pessoais. Ou seja, o indivíduo que teve seus dados violados tem direito a uma indenização? Quem deverá ser responsabilizado por essa violação? Que tipo de relação existe entre o titular de dados pessoais e o responsável pelo tratamento e/ou subcontratante e/ou autoridade de controle? Todas essas questões serão tratadas nesse capítulo com vistas a buscar uma forma de garantir ao titular de dados pessoais, dados esses que pressupõe-se que detém o total controle, (auto determinação informativa), que será compensado, não como uma forma de reparar totalmente o dano, já que no mundo virtual, lamentavelmente a informação se dissipa em questões de segundo através de diversos motores de busca, e muitas vezes fica difícil apagar as informações em todo esse caminho através da desindexação das informações, dos links dos mecanismos de busca da internet.

Consoante os grandes teóricos no assunto, a tônica da responsabilidade civil só se impõe em decorrência de uma norma, de um preceito e um dano, o que gera a obrigação de indenizar a vítima por violação de bens jurídicos. O Código Civil Português no artigo 483.º estabelece como regra a responsabilidade civil subjetiva, como aquele que, com dolo ou mera culpa, violar ilicitamente o direito de outrem ou qualquer disposição legal destinada a proteger interesses alheios fica obrigado a indenizar o lesado pelos danos resultantes da violação. Admitindo mitigar a responsabilidade através da previsão legal da presunção de culpa contida no artigo 487.º do código civil. A indenização independente de culpa só nos casos especificados na lei, está se falando da responsabilidade objetiva, artigo 483.º-2 do Código Civil português.

O princípio basilar da responsabilidade civil é *neminem laedere*, ou seja, não lesar a outrem. O mestre da Responsabilidade Civil no Brasil, o Ilustre Desembargador Sérgio Cavalieri Filho ³⁶⁵ com muita propriedade e atualidade nos ensina, « Tem-se dito, com absoluto acerto, que para trilhar os caminhos da Responsabilidade Civil, o estudioso necessita, além de não perder de vista a constante evolução social, utilizar com frequência a lógica do razoável ». Ou melhor, mesmo com toda a carga de evolução tecnológica, com diferentes recursos que

³⁶⁵ FILHO CAVALIERI, Sergio – **Programa de Responsabilidade Civil**. 7.ª ed. São Paulo: Atlas, 2007. ISBN 978-85-224-4688-9.

possibilita o homem interagir com pessoas e coisas nos quatro cantos do mundo em frações de segundo, o Direito é um complexo dinâmico, onde sofre influências das condições externas, e o aplicador do Direito não pode deixar de considerar as características sociais, econômicas e legais da polêmica em questão. A lógica formal não esgotaria a razão, na medida em que existem outros setores que pertencem à lógica jurídica, mas fogem da racionalidade, como a lógica dos problemas humanos de conduta prática³⁶⁶. O princípio da responsabilidade civil far-se-á presente sempre quando houver a violação de um dos direitos fundamentais do indivíduo.

A fim de analisarmos quem é o verdadeiro responsável pela violação de dados pessoais para que a vítima venha a ser ressarcida na devida proporção de seu dano, cabe, inicialmente aqui distinguir o conceito de obrigação e responsabilidade, para que possamos estabelecer quem será responsabilizado no caso da violação de dados. Então, partiremos sobre o conceito de obrigação que é tida como um dever jurídico originário, enquanto a responsabilidade é um dever jurídico sucessivo em decorrência da violação do primeiro. A responsabilidade só aponta a partir da violação de um dever jurídico prévio.

Portanto, no caso do Regulamento Geral de Proteção de Dados, o conteúdo é determinado, qual seja a proteção de dados pessoais. A fonte da obrigação é a própria lei, que impõe como responsável pelo tratamento, uma empresa ou organismo, podendo a empresa ou organismo delegar uma pessoa específica ou nomear um subcontratante com a obrigação de agir em conformidade com os princípios estabelecidos no RGPD onde o subcontratante está diretamente vinculado ao responsável pelo tratamento por força de contrato firmado. Quem vai responder pela violação de dados pessoais? aquele que tinha o dever de protegê-los em função da finalidade e através dos meios adequados: o responsável pelo tratamento ou subcontratante ou outros envolvidos na cadeia de tratamento. Logo, no caso de violação de dados, o lesado poderá pleitear uma indenização aquele que tinha o dever de agir em conformidade com o regulamento, lastreado no princípio da *restitutio in integrum*.

O artigo 24º estabelece que o responsável pelo tratamento de dados tem o dever legal de aplicar as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o regulamento. Quer dizer, o responsável pelo tratamento tem a obrigação legal de dar o tratamento dos dados pessoais em conformidade, com total obediência ao regulamento de forma a não causar danos aos seus titulares.

³⁶⁶ SICHES, Luis Recaséns - **Experiência Jurídica, Naturaleza de la Cosa e Lógica Razonable**. México: Fondo de Cultura Económica, 1971, p. 151.

A fonte desse dever decorre de um encargo estabelecido pela própria lei, o que caracteriza a responsabilidade extracontratual, onde uma vez seja violado esse dever, surge o direito de indenizar com vistas a efetividade de uma verdadeira justiça, onde o causador do dano tem a obrigação de reparar. Sem danos não há que se falar em reparação.

Em sede de responsabilidade civil extracontratual, tem-se a responsabilidade subjetiva, aquela em que a culpa tem que ser provada para efeitos de indenização. O fundamento da responsabilidade subjetiva é a culpa do agente. A parte prejudicada terá que provar a culpa do responsável. Tem-se como pressupostos da responsabilidade subjetiva primeiramente a violação de um dever jurídico, a conduta culposa (culpa), o dano e nexo causal. O artigo 927 do Código Civil Brasileiro assim dispõe: “Aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo”, reconhecendo como ato ilícito quando alguém de forma culposa (negligência ou imprudência) viola direito e causa dano comete um ato ilícito (artigo 186 e 187 do Código Civil Brasileiro).

O código Civil Português como já dito anteriormente trata da responsabilidade subjetiva no artigo 483.º -1, e o artigo 487-1.º positiva a presunção legal de culpa. Ocorre que com a revolução industrial, mudou consideravelmente a sociedade nos mais variados campos, transportes, indústria, nas empresas, etc., acidentes começaram a aparecer em larga escala, a tecnologia cresceu de forma vertiginosa, onde constatou-se que a ideia de culpa como critério para a responsabilidade civil para a reparação era frágil, já que provar a culpa do agente em diversas circunstâncias era uma prova diabólica, ou seja, a vítima ficaria sempre sem ressarcimento devido a inúmeras barreiras para se provar a culpa do causador do dano. Em função disso invoca-se a presunção da culpa, a causalidade em favor da vítima, através do mecanismo inversão do ônus da prova, o que pode ser considerado um degrau até se chegar à responsabilidade objetiva.

Na presunção de culpa, tem-se a culpa ainda como fundamento da responsabilidade civil, mas, alterada no que tange a distribuição do ônus da prova, que nesse caso a inversão do *onus probandi* recai sobre o acionado, que deverá provar que não agiu com culpa.

Mister se faz estabelecer o nexo causal entre a conduta do agente, por sua culpa e o dano sofrido pela vítima. Nesse contexto, também devemos ressaltar que a questão da teoria da causalidade adequada, o nexo causal, deve ser considerado, onde uma diz respeito a complexidade da prova e a outra a atribuir a causa efetiva que ocasionou o dano, o que nem sempre pode se apontar. Muitas vezes tem-se várias causas, sendo que nem todas contribuíram para aquele resultado, há de se averiguar e considerar somente aquela que efetivamente causou o dano para gerar o direito de indenizar.

Em função da dificuldade em proteger a vítima de ser ver ressarcida por possíveis danos em função da conduta do agente, conduta essa difícil de ser provada, por ser a vítima hipossuficiente, e não dispor de condições econômicas para tanto, e também relacionada a sociedade tecnológica em franco desenvolvimento, a responsabilidade subjetiva já não mais contemplava os anseios dos cidadãos. O mundo tecnológico, virtual demandava providências concretas e ágeis para garantir a reparação por violação de direitos pessoais envolvidos, surgindo novas exigências de caráter pragmático onde despontou a responsabilidade objetiva com base na teoria do risco. Risco é perigo, conseqüentemente uma perspectiva e danos, onde deve-se ter a preocupação de que o causador do dano não fique indene. A responsabilidade objetiva surge como um garante mínimo indispensável à sociedade³⁶⁷.

A teoria do risco se resume no simples fato de que o prejuízo causado pelo agente deverá ser suportado por ele que causou independentemente de culpa. Nesse caso a solução é simples bastando para tanto provar o fato. Provado o fato, provado o dano está, o que denomina-se *in re ipsa*, não mais tendo o lesado a obrigação de provar a culpa do agente. Podemos relacionar as peculiaridades do risco mais comuns, partindo da teoria do risco proveito, como muito bem diz o nome, está diretamente relacionado com a atividade que tira o seu lucro, onde se aplica o ditado jurídico de que quem tem o bônus tem o ônus, estando adstrita aos comerciantes e industriais que exercem atividade lucrativa e devem agir com cautela a fim de não lesar os consumidores, diferente da teoria do risco criado adotada por Caio Mario onde não se tem similitude com o proveito econômico da atividade, esta se resume no fato de que aquele que, em razão de sua atividade ou profissão, cria um perigo, está sujeito à reparação do dano que causar, salvo prova de haver adotado todas as medidas idôneas a evitá-lo³⁶⁸, ou seja aquele que exercer uma atividade vai responder pelos danos causados em razão de sua atividade independente de apurar-se a culpa do agente, se este agiu com negligência, imprudência ou imperícia.

Adentrando nos pressupostos da responsabilidade civil temos conduta do lesante, dano e o nexo de causalidade entre a conduta e o dano. Na responsabilidade objetiva é imprescindível o nexo causal, sendo excepcionada no caso onde se aplica a teoria do risco integral. Para caracterizar-se a responsabilidade tem que haver uma causa e um resultado. Eliminando-se o nexo causal desaparece a obrigação de reparar.

³⁶⁷ VARIZ, Maria Afonso Manuel – **Da responsabilidade Civil decorrente de produtos defeituosos**. Coimbra: Coimbra, 1991. ISBN972-32-0466-5, p. 15.

³⁶⁸ MARIO, Caio - **Responsabilidade Civil**. 12. ed. São Paulo: Saraiva, 2018, p. 24.

Já na seara da violação de dados pessoais que gera danos materiais e/ou imateriais nos titulares dos dados, por infração as normas contidas no regulamento, é pacífico o entendimento e está positivado no regulamento o direito de indenização, artigo 82º. Cabe apenas analisarmos o âmbito da responsabilidade daquele que detiver o encargo do tratamento de dados, e que muitas vezes percebe-se a existência de terceiros que também poderão ser responsabilizados.

O Regulamento Geral de Proteção de dados avança quando de forma pragmática e objetiva estabelece e impõe os deveres e obrigações que deverão ser seguidos pelos seus agentes impondo-lhes o princípio da responsabilidade em caso de violação aos princípios e deveres estatuídos no RGPD, ressaltando a importância da segurança do tratamento dos dados, (artigo 32º). A figura *data controller* (responsável pelo tratamento de dados) e *data processor* (subcontratante), assim denominado por Mafalda Miranda Barbosa³⁶⁹, assumem como peças centrais da regulamentação relativa aos dados pessoais e nos dotam de critérios de determinação do responsável em caso de violação do direito à proteção de dados pessoais. Todavia, haveremos de analisar em que medida a lesão que ocorre se liga funcionalmente ao dever preterido, para o que teremos de confrontar a esfera de responsabilidade do *controller* com outras esferas de responsabilidade³⁷⁰.

Cotejando o RGPD com a Lei n.º 67/98 - Lei da Protecção de Dados Pessoais, que transpôs para a ordem jurídica portuguesa a Diretiva 95/46/CE, anteriormente em vigor, tem-se alguns direitos robustecidos, e mecanismos mais austeros. Mafalda Miranda Barbosa³⁷¹, traçou um paralelo entre as duas legislações realçando alguns pontos de maior relevância, que serão aqui destacados: o conceito de dados pessoais foi mais alargado no Regulamento, já que passou a referendar dados de localização ou identificadores por via eletrônica, identidade genética, entre outros meios possíveis de identificação; O tratamento de dados pessoais deve ser feito de forma lícita, transparente e de acordo com o princípio da boa-fé, na Lei 67/98, não havia de forma explícita, no corpo da lei, o exercício da transparência. Já o princípio da minimização de dados, o princípio da exatidão e o princípio da limitação, princípio da integridade já eram aclamados na Lei 67/98 e preservado no RGPD. O princípio da confidencialidade como requisito que deve se render a proteção de dados não estava abrangido na Lei 67/98, não significando dizer com isso que não se detectasse o princípio em tela. O

³⁶⁹ BARBOSA, Mafalda Miranda - **Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil**. [Em linha]. [Consult. 6 jun.2019]. Disponível em WWW:<URL:<<https://www.revistadedireitocomercial.com/data-controllers-e-data-processors>>>.

³⁷⁰ *Idem* – **Op. Cit.**

³⁷¹ *Idem* – **Op. Cit.**

RGPD disciplinou o tratamento com vistas a garantir a segurança adequada, valendo-se de medidas técnicas organizativas adequadas.

O regulamento geral de proteção de dados está sob o manto das duas espécies de responsabilidade civil, a contratual e extracontratual no que diz respeito a toda a cadeia de pessoas responsáveis pelo cumprimento dos princípios estatuídos no Regulamento em casos de violação de dados dos seus titulares.

A responsabilidade contratual está positivada no artigo 28º-3, onde o subcontratante estabelece um negócio jurídico com o responsável pelo tratamento, exclusivamente, por contrato ou outro ato normativo, onde o responsável pelo tratamento avalia e delega ao subcontratante desde que este reúna condições de garantidor da execução do tratamento em total obediência aos requisitos do regulamento. O subcontratante não tem autonomia total devendo estar adstrito as orientações e instruções do responsável pelo tratamento que prima pelo fiel cumprimento dos princípios contidos no regulamento.

Percebe-se nitidamente que em que pese o responsável pelo tratamento delegar ao subcontratante este continua com o vínculo, onde é responsável solidário em caso de violação de dados de terceiros. Os deveres jurídicos, no caso em tela, têm a fonte no contrato firmado entre as partes. A transgressão de um dever concebido num negócio jurídico, caracteriza um ilícito contratual, em caso de danos todas as pessoas envolvidas poderão responder solidariamente em função de cada caso concreto, já que as diversas pessoas compreendidas podem assumir pra si a função de ser as responsáveis pelo tratamento de dados. Devendo ser exonerada a responsabilidade se o responsável pelo tratamento ou o subcontratante comprovar que não é o responsável pelo fato que desencadeou os danos.

O subcontratante que agirá por força de um contrato para prestação de tratamento de dados de terceiros, deve ter a percepção de que sua atuação pode afetar os interesses desses terceiros, deve incorporar o âmbito dos interesses dos terceiros, pelo que estes se devem integrar na esfera de proteção do contrato³⁷².

Na responsabilidade contratual, basta para tanto que a violação dos dados ocorra pela preterição de determinados deveres que oneram o responsável pelo tratamento, numa relação contratual firmada entre ele e o titular daqueles. Ainda que o contrato não tenha como objeto

³⁷² BARBOSA, Mafalda Miranda - **Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil**. [s.d.].

essa proteção dos dados, a boa-fé pode impor determinados deveres de cuidado que, quando violados, geram responsabilidade contratual³⁷³.

Já a responsabilidade extracontratual está contida no artigo 82 do regulamento que estabelece de forma expressa o direito a indenização do responsável pelo tratamento ou do subcontratante em casos de violação do presente regulamento. Vivemos num mundo altamente tecnológico, numa sociedade informacional onde diariamente as pessoas difundem seus dados pessoais e esses circulam livremente perpassando por diversas empresas que muitas vezes partilham esses dados com terceiros sem que os donos das informações tenham conhecimento. Os dados que eram considerados privados passam a ser públicos.

Nessa linha surgiu o regulamento para dar segurança jurídica aos titulares dos dados salvaguardando não só a privacidade, mas vários direitos da personalidade do titular dos dados, já que as empresas devem obediência aos princípios estatuídos no regulamento visando a proteção dos dados pessoais, onde o responsável pelo tratamento de dados deve sempre primar determinando a finalidade e os meios de tratamento dos dados, a fim de que os dados não sejam violados.

O regulamento elenca uma série de atores com o dever de diligenciar o tratamento dos dados em total obediência aos princípios estatuídos no regulamento, figurando como protagonista o designado como responsável pelo tratamento que detém o poder de aplicar as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o regulamento. Por assim ser, os responsáveis pelo tratamento têm uma obrigação legal, em que no caso de violação dos dados, (artigo 82º 1-3) onde estes poderão ilidir sua culpa se provarem que de modo algum são responsáveis pelo evento que deu origem aos danos. Estamos diante do instituto da responsabilidade extracontratual subjetiva com culpa presumida (artigo 483.º-1 e 487.º-1). A presunção de culpa no caso é *juris tantum*, é relativa, onde o responsável pelo tratamento presume-se culpado até prova em contrário. A inversão do ônus da prova passa ao demandado devendo provar que não é o responsável pelos danos causados pela violação de dados.

Nesse contexto, o próprio regulamento no artigo 4º-7³⁷⁴, define o Responsável pelo tratamento como a pessoa singular ou coletiva, autoridade pública, agência ou outro organismo.

³⁷³ BARBOSA, Mafalda Miranda - **Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil**. [s.d.].

³⁷⁴ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Em linha]. [Consult. 15 nov. 2018]. Disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679>.

No caso da empresa ou organismo, o comitente ou patrão responderá por ato culposos do empregado no exercício de suas funções, por estar caracterizada a relação de vínculo em relação a atividade propriamente dita da empresa, que pode ser considerada de risco, já que no mundo virtual que vivemos praticamente todas as atividades implicam em algum risco. Seguramente a empresa ou organismo é que será a responsável pelo tratamento de dados, tendo o dever de arcar com as obrigações contidas no regulamento da proteção de dados e pela reparação no caso de violação de dados do seu titular, aquele que, de boa-fé confiou em fornecer suas informações pessoais.

Importante se faz traçar o desenho do atuar do responsável e subcontratante, para entendermos a responsabilidade de cada um de forma a garantir ao lesado o direito de se ver indenizado. O responsável pelo tratamento é a pessoa que exerce o controlo sobre os dados, razão pela qual lhe são impostos especiais deveres e lhe é imputada a responsabilidade, em caso de violação de algum deles, controle esse que não deve ser meramente formal, mas refletir a realidade, devendo aquele que é indicado como controller exercer um controle efetivo sobre os dados³⁷⁵. O Subcontratante, no RGPD, está diretamente vinculado ao responsável pelo tratamento por um contrato. Há previsão legal caso o subcontratante necessite contratar outro subcontratante, mas para isso o responsável pelo tratamento deverá dar autorização por escrito.

O responsável pelo tratamento tem o dever positivado na norma de proceder um tratamento lícito. A licitude do tratamento está diretamente vinculada a ocorrência de uma das seguintes situações: se o titular dos dados tiver dado o seu consentimento pra tratamento de seus dados com uma finalidade específica, se esse tratamento for necessário para a execução de um contrato no qual o titular de dados é parte, se o tratamento for necessário para a defesa de interesses vitais do titular dos dados, se for necessário para atingir interesses prosseguidos pelo responsável pelo tratamento ou terceiros, conforme dispõe o artigo 6º do RGPD³⁷⁶.

Está previsto no RGPD a possibilidade do responsável pelo tratamento (controllers) recorrer a subcontratantes (processor), desde que este último ofereça garantias suficientes de execução de medidas técnicas e organizativas adequadas, em cumprimento as regras estabelecidas no RGPD (artigo 28 º). No caso de um conjunto de operações de tratamento

³⁷⁵ BARBOSA, Mafalda Miranda - **Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil**. [s.d.].

³⁷⁶ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Em linha]. [Consult. 15 nov. 2018]. Disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679>.

apresentar riscos elevados, é de total responsabilidade do responsável efetuar uma avaliação de impacto sobre a proteção de dados, solicitando um parecer do encarregado da proteção de dados, caso tenha sido designado.

A figura do encarregado da proteção de dados, artigo 38º e 39º, também poderá ser responsabilizado junto ao titular dos dados se não cumprir com os deveres constantes no RGPD. Ao assumir as suas funções, assume concomitantemente uma esfera de risco, de tal modo que, se violar algum desses deveres a primitiva esfera de responsabilidade pelo outro convola-se numa esfera de responsabilidade perante o outro³⁷⁷.

A autoridade de controle tem como uma de suas atribuições elaborar e dar publicidade a lista dos tipos de operação de tratamento sujeitos ao requisito de avaliação de impacto sobre a proteção de dados. (artigo 35º - 4) .

Como muito bem pontuou, Mafalda Miranda Barbosa³⁷⁸, no diagnóstico da responsabilidade civil em sede do RGPD, o fato de haver pluralidade de controllers , necessariamente não significa dizer que teremos diversidade de responsáveis, até porque o controle conjunto não está diretamente relacionado a várias pessoas na execução de tratamento de dados, onde se impõe a responsabilidade solidária somente em casos de reconhecimento das mesmas finalidades e meios que porventura tenham sido definidas em conjunto, como uma simbiose para um só tratamento dos dados, por parte dos envolvidos, que serão tratados como responsáveis pelo tratamento de dados em suas diferentes esferas .

Ao mesmo tempo quando a empresa ou organismo determina uma pessoa singular específica de dentro da empresa como responsável para trabalhar os dados, tendo o dever de obedecer rigorosamente os princípios estabelecidos na legislação, de igual forma esta pessoa assumirá o papel de responsável pelo tratamento, mas, não se pode esquecer a existência de uma relação de subordinação e dependência que está presente, dado que a pessoa singular age em nome da empresa e esta sim será sempre a responsável pelo tratamento de dados de forma direta e responderá em casos de violação dos princípios contidos no RGPD.

Considerar a empresa como responsável em caso de violação de dados e não a pessoa que foi designada para tratar os dados dentro da empresa, é uma forma de garantir ao lesado sua integral reparação, o que não exclui da empresa o direito de regresso contra a pessoa que foi atribuído a obrigação de obedecer aos princípios na RGPD, e que assim não procedeu, desde que haja prova irrefutável do não incumprimento. A pessoa que teve seus dados violados não

³⁷⁷ BARBOSA, Mafalda Miranda - **Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil**. [s.d.].

³⁷⁸ *Idem* – **Op. Cit.**

pode estar à mercê de todo um processo para se apurar a culpa do responsável pelo descumprimento, por esse motivo a empresa deverá responder objetivamente. A responsabilidade objetiva consiste na reparação do dano, independentemente de culpa, nos casos especificados em lei ou quando o negócio desenvolvido pelo causador do dano resultar, na sua espécie, risco para o direito de outros conforme artigo 927 parágrafo único da Lei 10.406/2001³⁷⁹.

Em apertada síntese, verifica-se que o artigo 82º - 1 e 3 do RGPD, trata da responsabilidade civil extracontratual por culpa presumida, em conformidade com o artigo 483.º-1 e artigo 487.º-1 do Código Civil Português, onde determina que qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos, salvo se este provar que não é o responsável pelos evento que desencadeou os danos, caracterizado está nesse item 3, a inversão do *onus probandi*, em favor do lesado³⁸⁰.

Estamos na seara da responsabilidade civil pela violação de dados pessoais, que são considerados direitos fundamentais do indivíduo, onde a previsão de apurar a responsabilidade não pode ser fechada em obediência integral à lei, devendo permear a busca da realização da verdadeira justiça, através da análise de cada caso concreto, ponderando sempre os bens jurídicos que devem ser tutelados. Desenhar a responsabilidade subjetiva com base na culpa presumida é ainda discutir extensivamente a culpa do causador do dano, o que, pode ser um obstáculo a dar a segurança jurídica a pessoa que teve seus dados pessoais violados pelo simples fato do causador do dano dispor de meios e técnicas de ilidir sua culpabilidade, já que estamos vivendo num mundo altamente tecnológico.

Contudo, não é razoável somente uma análise tecnicista de se limitar a averiguar se o responsável pelo tratamento ou o subcontratante não cumpriu com as obrigações decorrentes do regulamento para assegurar a efetiva indenização ao titular dos dados violados. Entretanto, há de se considerar, também, para se apurar a responsabilidade e a possibilidade de uma indenização, a questão dos direitos da personalidade envolvidos, já que não necessariamente a suposta violação de um direito pleiteado estará na base do direito à proteção de dados, bem

³⁷⁹ BRASIL. Lei n.º 10.406, de 10 de janeiro de 2001. **Institui o Código Civil**. [Em linha]. [Consult. 01 de jan. 2018]. Disponível em WWW: <URL: http://www.planalto.gov.br/ccivil_03/leis/2002/110406.html>.

³⁸⁰ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Em linha]. [Consult. 15 nov. 2018]. disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679>.

como proceder a uma análise da conduta do controller ou processor para mensurar até que ponto sua ação ou omissão ensejará o dever de indenizar a pessoa que teve seus dados violados. A responsabilidade do controller não afasta a responsabilidade própria do processor.

Ou seja, não basta apurar o somente o agir do responsável pelo tratamento ou dos demais responsáveis, devendo-se ponderar também os direitos envolvidos e se estão sob a égide da proteção de dados. A essência da legislação para proteção de dados é não só a privacidade, mas os demais direitos da personalidade, que devem ser tutelados em prol da dignidade da pessoa humana, que é o cerne de todos os direitos personalíssimos, e é nessa linha que deve ser apurado a possível violação.

Adentrando no instituto da responsabilidade civil objetiva, que preconiza que todo aquele que exerce uma atividade de risco, que por sua natureza pode implicar em risco para os direitos de outrem, deve assumir os riscos e reparar o dano dela decorrente, independente de culpa – art. 927 parágrafo único da Lei 10.406/2001³⁸¹. Tendo como pressupostos a conduta humana, o dano e o nexo de causalidade. O elemento culpa é escusável. Como conduta humana, traz-se o conceito “vem a ser o ato humano, comissivo ou omissivo, ilícito ou lícito, voluntário e objetivamente imputável, do próprio agente ou de terceiros, ou o fato de animal ou coisa inanimada, que cause danos a outrem, gerando o dever de satisfazer os direitos do lesado”³⁸². Dano a sim definido como “o grande vilão da responsabilidade civil. Não haveria que se falar em indenização, nem em ressarcimento, se não houvesse dano. Pode haver responsabilidade sem culpa, mas não pode responsabilidade sem danos. Na responsabilidade objetiva, qualquer que seja a modalidade do risco que lhe sirva de fundamento – risco profissional, risco proveito, risco criado etc. -, o dano constitui o seu elemento preponderante. Tanto é assim que, sem danos, não haverá o que reparar, ainda que a conduta tenha sido culposa ou até dolosa”³⁸³.

E por fim o nexo causal, que é considerado tão somente a relação de causalidade entre a conduta do agente e o dano. O dano pode até existir, mas, para caracterizar a responsabilidade é fundamental que a causa do dano esteja relacionada de forma direta com a conduta do agente.

Cimentado nesses pressupostos e esmiuçando o Regulamento Geral de Proteção de dados, em relação a definição e a especificação da responsabilidade do responsável pelo tratamento de dados (artigos 4º-7/8/ e artigo 24º), os responsáveis conjuntos pelo tratamento

³⁸¹ BRASIL. Lei n.º 10.406, de 10 de janeiro de 2001. **Institui o Código Civil**. [Em linha]. [Consult. 01 de jan. 2018]. Disponível em WWW: <URL: http://www.planalto.gov.br/ccivil_03/leis/2002/110406.html>.

³⁸² DINIZ, Maria Helena. Curso de Direito Civil Brasileiro – **Teoria Geral do Direito Civil**. Saraiva: Rio de Janeiro. 2015. ISBN 9788502143326, p. 37.

³⁸³ GAGLIANO, Pablo Stolze. PAMPLONA FILHO, Rodolfo - **Novo Curso de Direito Civil, Volume 3: Responsabilidade Civil**. São Paulo: Saraiva, 2003. ISBN 978-85-472-1647-4, p. 40.

(artigo 26º), o subcontratante (artigo 28º), o encarregado da proteção de dados (artigo 38º), conclui-se que a atribuição desempenhada pelas pessoas elencadas é uma atividade de alto risco, inerente a natureza do tratamento e que afeta diretamente os direitos e liberdades das pessoas envolvidas, onde se impõe a aplicação de medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco (artigo 32º). O próprio regulamento considera a atividade desenvolvida no tratamento de dados pessoais uma atividade de risco na medida em que expõe direitos fundamentais dos indivíduos que devem ser preservados e garantidos constitucionalmente em prol da dignidade humana.

Nessa linha de construção de pensamento, chega-se à conclusão de que a empresa que exerce atividade de risco, como no caso dos responsáveis pelo tratamento, assim considerados, pessoa coletiva, agência ou outro organismo, que gerencia os dados pessoais de todos os cidadãos em diversos lugares, tem o dever de fazê-lo com segurança, de modo a não ocasionar danos as pessoas envolvidas, onde deveria responder independente de culpa. Entretanto, o regulamento postula a responsabilidade com base na culpa presumida (artigo 82º - 3) em consonância com o artigo 483.º -1 e 487.º-1 do Código Civil, isentando o responsável pelo tratamento ou subcontratante, se este provar que não é o responsável pelo evento que ocasionou os danos, o que poderá dificultar a vítima de se ver reparada nos danos sofridos. O responsável pelo tratamento ou subcontratante só poderá se eximir de sua culpa se alegar que embora tenha cumprido com as normas do regulamento, a violação de dados ocorrera, por caso fortuito ou força maior e ainda que não existe o nexo causal entre o dano e seu agir em conformidade com o regulamento, podendo alegar diversas hipóteses de excludente de culpabilidade, o que afastará o dever de indenizar a vítima.

Podemos trazer a lume, como uma forma de garantir ao titular dos dados violados uma forma efetiva e eficiente de reparação a noção da culpa contra a legalidade, onde essa se materializa quando o dever violado resulta de texto expresso de lei ou regulamento. Bastando para tanto ocorrer a violação de norma legal, uma vez ocorrido o dano, no caso, a violação de dados, o responsável pelo tratamento deverá responder civilmente por sua culpa pelo simples fato de ter transgredido uma norma jurídica.

Para melhor entendimento tem-se a culpa contra a legalidade “quando a simples infração da norma regulamentar é fator determinante da responsabilidade, isto é, desde que entre a sua transgressão e o evento danoso se estabelece indispensável nexo causal, pois, nesta hipótese, o ofensor que executa um ato proibido, ou não cumpre com o que determina a lei ou o

regulamento, incorre, só por este fato, em culpa, sem que seja mister ulteriores investigações”³⁸⁴.

A responsabilidade conjunta pelo tratamento só será efetivada se houver identidade de finalidade e meios, configurando a responsabilidade solidária, onde ambos serão os responsáveis conjuntos pelo tratamento, onde terão que provar que sua atuação não ocasionou os danos ao titular dos dados, por ter agido no regular exercício de direito em total submissão as obrigações contidas no regulamento. E em não sendo possível a identificação de quem efetivamente deu causa a violação de dados, todos na cadeia responderão de forma solidária cabendo o direito de regresso.

A partir do momento em que um determinado sujeito lida com dados alheios, assume uma esfera de risco/responsabilidade, devendo adotar as medidas de cuidado – consagradas pelo legislador – no sentido de garantir a sua incolumidade. Não o fazendo, a primitiva esfera de responsabilidade (responsabilidade pelo outro, ou pelos dados do outro) convola-se numa outra esfera, mais ampla, de responsabilidade, no sentido da *liability* (responsabilidade perante o outro)³⁸⁵.

Dessa forma, a responsabilidade civil tem um grande desafio a ser enfrentado no que tange a apurar a responsabilidade pela violação de dados pessoais que causarem danos materiais ou imateriais ao titular dos dados, garantindo-lhe uma indenização. A figura central e de vital importância no regulamento é o responsável pelo tratamento e subcontratante onde se revestem da função de dar tratamento lícito, leal e transparente em relação ao titular dos dados, limitando a recolha para finalidades determinadas, explícitas e legítimas como positivado no RGPD³⁸⁶. Nesse contexto, a problemática maior é relacionar a violação de dados a falta do cumprimento dos deveres por parte do controller, ou seja, o nexos causal, da conduta ilícita do agente, a culpa e o dano perpetrado no titular dos dados, o que para tanto há de se analisar as diferentes variantes da que incide a responsabilidade do controller ou do processor, além de se confrontar a ilicitude, a culpa e o dano.

O artigo 82º do regulamento consolidou o direito do titular de dados de se ver ressarcido através de uma indenização em casos de violação de seus dados, por parte daqueles que ao

³⁸⁴ GARCEZ *apud* FILHO, Sergio Cavaleri – **Programa de Responsabilidade Civil**. 2007. p. 41.

³⁸⁵ BARBOSA, Mafalda Miranda - **Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil**. [s.d.].

³⁸⁶ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Em linha]. [Consult. 15 nov. 2018]. Disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679>.

avocarem a função de responsável pelo tratamento dos dados das pessoas, assumiram o risco de agir com cuidado em proceder o tratamento dos dados em conformidade com o regulamento e assegurar que seja efetuado com equidade, transparência e confidencialidade para com as pessoas singulares, a fim de não propiciar a ocorrência de danos. O regulamento prevê ainda o controle conjunto de responsáveis pelo tratamento de dados, o que não significa dizer com isso que havendo pluralidade de responsáveis haverá pluralidade de executores. O controle conjunto implica em inevitavelmente em compartilhamento de finalidades e meios.

Aliado a essa busca do derradeiro responsável em caso de violação de dados, deve-se perquirir, de igual forma, o critério qualitativo dos danos sofridos pela vítima e quais os bens jurídicos lesionados e se estão cobertos pelo manto do regulamento. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade, como sustenta o considerando 4³⁸⁷ do RGPD.

Um outro ponto a ser considerado no regulamento, no artigo 82º é a exclusão da responsabilidade por fato exclusivo do titular dos dados (concorrências de causas). O regulamento não contempla a possibilidade de o titular concorrer de alguma forma para a violação de seus dados pessoais. O fato exclusivo da vítima, no caso o titular dos dados, rompe com o nexo causal, acarretando a exoneração do responsável pelo tratamento ou o subcontratante. Nesse aspecto, mister se faz a repartição proporcional dos prejuízos, ponderando o grau de causalidade de cada parte envolvida.

Contrastando com a legislação brasileira de proteção de dados, a Lei 13.709/2018 disciplina no inciso III do artigo 43 a exclusão da responsabilidade quando ficar devidamente provado que o dano decorreu de culpa exclusiva do titular dos dados. De igual forma, contempla a responsabilidade e o ressarcimento de danos por parte do controlador ou o operador em razão da atividade de tratamento de dados pessoais causar danos de ordem patrimonial, moral, individual ou coletivo, a outrem, admitindo a solidariedade entre operador e controlador inserta na letra da lei nos incisos I e II do referido artigo 42³⁸⁸.

³⁸⁷ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Em linha]. [Consult. 15 nov. 2018]. Disponível em WWW: <URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679>>.

³⁸⁸ BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)** [Em linha]. [Consult. 10 abr. 2019]. Disponível em WWW: <URL:http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>.

A garantia do direito à indenização ao titular por violação de seus dados, perpassa pelo compartilhamento do ônus da prova àquele que reúne melhor condição técnica para elaborá-lo. Nesse sentido, a legislação brasileira de proteção de dados de forma concreta prevê a inversão do *onus probandi*, no parágrafo 2º do artigo 42, a ser utilizada pelo Juiz, numa demanda judicial, em favor do titular dos dados quando for verossímil suas alegações, e a produção de prova resultar-lhe excessivamente onerosa, ou caso seja considerado hipossuficiente na produção de provas.

Enfim, o crescimento da tecnologia, em larga escala, onde a internet não conhece fronteiras, e em função disso tem-se noticiado frequentemente inúmeros problemas decorrentes desse acesso ilimitado ao mundo virtual, atingindo bens personalíssimos que até então pode-se dizer eram comedidos, e, hoje, em função da facilidade de acesso à tecnologia da informação, ao dados das pessoas são recolhidos e processados de forma vertiginosa e em grandes proporções fugindo ao controle do titular dos dados, podendo resultar numa violação de dados sem precedentes, uma vez que é quase impossível ter o controle sobre a abrangência de uma informação exposta no ciberespaço. Nessa trajetória a responsabilidade civil, no mundo globalizado, tem uma missão de mudar alguns paradigmas para recepcionar os anseios de uma população no surgimento de uma nova sociedade de risco com vistas a tutelar os direitos fundamentais.

O regulamento geral de proteção de dados, tem sem dúvida o compromisso de garantir que o titular dos dados, objeto de violação, não fique subjugado a ver a inversão do ônus probatório em favor do responsável pelo tratamento ou subcontratante, já que estes terão os meios e instrumentos para ilidir sua responsabilidade, deixando a vítima totalmente desprotegida, e sem a proteção de seus dados pessoais interferindo de forma direta na sua vida privada, numa afronta ao princípio constitucional da dignidade da pessoa humana.

4.1 A responsabilidade pelos operadores dos motores de busca na qualidade de responsáveis pelo tratamento de dados

Os motores de busca nada mais são do que as ferramentas usadas pelos usuários para pesquisar qualquer informação na internet, no world wide web criada na década de 1990, o famoso WWW. Qualquer pessoa que tenha um computador pode navegar na web acedendo a toda e qualquer informação em qualquer lugar do planeta. Importante aqui consignar como funciona o motor de busca para que possamos analisar a responsabilidade civil dos referidos operadores do motor de busca e equipará-los como responsáveis pelo tratamento.

As informações brotam porque logo após o aparecimento da internet, uma realidade transnacional na sua essência, surgiram vários motores de busca que tinham como objetivo organizar as informações que apareciam na internet, colacionando-as, para disponibilizá-las para o internauta de forma rápida e eficiente. Tanto assim, que hoje, não existe uma pessoa no ciberespaço que se valha do gigante Google que armazena e disponibiliza toda e qualquer informação, e tem como concorrente o Bing e Yahoo de menor expressão.

Os motores de busca recorrem a spiders(aranhas) ou robôs que devastam os sites, blogs, em busca de novos conteúdos nos sites já indexados, o conteúdo passa a estar interligado em um número incontáveis de sites, através desses links possibilitam a conexão com diversas páginas existentes na rede. A partir daí o operador do motor de busca examina e recolhe todo o conteúdo.

Nesse contexto, tem ocorrido relato de várias denúncias de pessoas que foram vítimas de violação do direito à privacidade operado nos motores de busca. O caso emblemático e já abordado no capítulo três quando tratamos do direito ao esquecimento, foi o do M.Costeja González, envolvendo o Google Spain SL, a Google Inc. e à Agencia Española de Protección de Datos, quando à agência determinou que à Google retirasse dos motores de busca os dados pessoais do Sr. González e inviabilizasse o acesso no futuro de forma definitiva, já que ao postar o nome M.Costeja González no site do Google imediatamente era transferido para o site do jornal La Vanguardia, onde o referido jornal mencionava o anuncio de um imóvel de propriedade do Sr. González que estava sendo levado a hasta pública por uma dívida com a Segurança Social. O problema havia sido resolvido a tempos atrás, mas a informação continuava nos motores de busca.

O acórdão proferido enfrentou a questão de apurar quais obrigações dos operadores de motores de busca em relação a proteção de dados pessoais das pessoas que não desejem ver suas informações pessoais devassadas na web, possibilitando terceiros a invadir sua privacidade, e até mesmo localizá-las.

O grupo de trabalho instituído pelo artigo 29 da Diretiva 95/46/CE³⁸⁹, concebeu os motores de busca como uma ferramenta de localização de informação. Considera os motores de busca como de serviços que ajudam os seus utilizadores encontrar informação na web. Reconhece duas atribuições aos operadores dos motores de busca em relação aos dados pessoais: Em primeiro lugar, na qualidade de prestadores de serviços aos utilizadores, onde os motores de busca, recolhem e tratam vastas quantidades de dados dos seus utilizadores,

³⁸⁹ Grupo de Trabalho Do Artigo 29 Sobre Proteção de Dados. Parecer 1/2008 Sobre Questões de Protecção dos Dados Ligadas aos Motores de Pesquisa. 2008. Artigo recebido via correio digital.

incluindo dados obtidos por meios técnicos, como os testemunhos de conexão, sendo assim considerados responsáveis pelo tratamento de dados dos utilizadores, sendo plenamente responsáveis ao abrigo da Diretiva .

Em segundo lugar, na qualidade de fornecedores de conteúdo, os motores de pesquisa contribuem para tornar as publicações mais facilmente acessíveis a um público mundial, onde nesse caso, amparado pela legislação não são considerados os principais responsáveis pelos dados que tratam, a exceção em relação a disponibilidade de um "cache" a longo prazo e operações de valor acrescentado em dados pessoais (como motores de pesquisa destinados à elaboração de perfis de pessoas singulares). Nesse sentido, os motores de busca devem ser consagrados como responsáveis pelo tratamento dos dados e tem o dever de seguir as normas emanadas pelo regulamento.

A Carta Europeia de Direitos Fundamentais publicada em 18 de dezembro de 2000, em seu artigo 8.^o³⁹⁰ ressaltava a proteção de dados pessoais, tendo assegurado o direito à liberdade de opinião e a liberdade de receber e transmitir informações ou ideias sem qualquer ingerência de poderes públicos e sem consideração de fronteiras. (artigo 11.^o), o que nos remete a todo o processo de recolha e armazenamento de informações do histórico de pesquisas do usuário da internet que possibilita a construção de um perfil do usuário. Os dados coletados podem ser repassados a terceiros com fins comerciais, ou até mesmo por questões de segurança nacional.

O grupo de trabalho definiu dados pessoais como: endereços IP e testemunhos de conexão (cookies), adotou o histórico de pesquisa de uma pessoa, como dados pessoais se esta for identificável. Quanto aos IP, que possibilita a identificação do endereço de seus utilizadores, estes só são identificáveis pelos fornecedores de acesso a internet, que dispõe dos dados sobre os seus endereços. Se um testemunho contiver um identificador único do utilizador, esse identificador constitui claramente um dado pessoal.

Atribuiu de igual forma, responsável pelo tratamento, o fornecedor de um motor de busca por tratar dos dados dos usuários da internet, como o endereço do IP e /ou testemunhos persistentes como um identificador único, por determinar as finalidades e meios do tratamento.

O papel que os operadores dos motores de busca exercem na sociedade informacional é de grande relevância, já que a informação, nos dias de hoje, é vital, entretanto, não se pode descuidar de direitos fundamentais do cidadão em detrimento de se levantar a bandeira do livre fluxo de informação aliado ao direito fundamental à liberdade de expressão a qualquer preço.

³⁹⁰ UNIÃO EUROPEIA - **Carta dos Direitos Fundamentais da União Europeia**. [Em linha]. [Consult. 01 fev. 2018]. Disponível em WWW: <URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN>.

Há de se equilibrar juntamente com a tutela de proteção do direito à vida privada correlacionada a proteção de dados pessoais em respeito à legislação vigente.

A luz da Diretiva 95/46/EC, o fornecedor de motor de busca, nem sempre figura como um intermediário, e a diretiva é omissa em relação aqueles que atuam na forma de intermediários da informação difundida na internet. Mas, ao mesmo tempo, com base nas definições do responsável pelo tratamento, pode-se concluir que a aplicação das regras de proteção de dados pessoais é perfeitamente oportuna.

Após extensos estudos confrontados com as análises apresentadas pelos fornecedores de motores de busca em relação as finalidades relacionadas ao tratamento dos dados pessoais, o grupo de trabalho³⁹¹ concluiu e dirimiu dúvidas acerca da responsabilidade dos fornecedores de motores de busca, clarificando as obrigações que deverão ser seguidas em consonância com a legislação em vigor : que os fornecedores de motores de busca podem tratar os dados pessoais para finalidade legítimas e em relação a quantidade de dados, estes devem ser compatíveis com as finalidades que deseja alcançar; os motores de busca excluir ou anonimizar os dados de forma irreversível e profícuo; quanto ao período de conservação não deverá ser superior a seis meses, e se for o caso de dilatação desse prazo deverá vir acompanhado de uma justificativa relevante e diretamente relacionada com a finalidade a que se destina;

Em caso de utilização de testemunhos de conexão, a duração também deverá ser proporcional a sua necessidade; considerando que os fornecedores de motores de busca recolhem dados pessoais dos utilizadores do serviço, em especial o IP, entende o grupo não haver necessidade de recolha de mais dados quando estiver relacionado com a apresentação de resultados de pesquisa e de anúncios; quanto as informações, estas devem ser claras, explícitas em relação a identidade e localização dos dados que pretende recolher, conservar e até mesmo difundir, além de esclarecer a finalidade da recolha; o consentimento dos utilizadores também deverá ser requerido quando os dados não forem fornecidos por seus titulares, ainda que com o objetivo de engrandecer o perfil do utilizador e de igual forma com vistas a conservar o histórico de pesquisa individual; os fornecedores de motores de busca devem respeitar as opções de exclusão dos editores de sítio Web que indiquem que o sítio Web não deve ser varrido e indexado, nem incluído nos "caches" dos motores de pesquisa; no caso específico de um "cache" em que dados pessoais sejam disponibilizados durante mais tempo do que a publicação original, devem respeitar o direito das pessoas em causa de remoção do "cache" de dados excessivos e inexactos e por fim os motores de busca de pessoas que utilizam software de

³⁹¹ GRUPO DE TRABALHO DO ARTIGO 29 SOBRE PROTEÇÃO DE DADOS. PARECER 1/2008 SOBRE QUESTÕES DE PROTECÇÃO DOS DADOS LIGADAS AOS MOTORES DE PESQUISA. 2008.

reconhecimento facial em imagens, deverão ter fundamento fidedigno para o tratamento, incluindo o consentimento, em total obediência aos pressupostos em relação ao tratamento contidos na Diretiva 95/46/CE.

Por mais que rebusquemos, não resta dúvida de que os fornecedores de motores de busca são equiparados aos responsáveis pelo tratamento dos dados e deverão ser responsabilizados na forma da legislação em vigor no caso de violação dos dados pessoais, como assim entendeu o Tribunal de Justiça (Grande Seção), no caso *González* declarando no sentido de que a operação de um motor de busca está relacionado em localizar informações publicadas através do mecanismo spider, ou colocadas na internet por terceiros, indexá-las, armazená-las e em seguida disponibilizá-las aos internautas, portanto sua execução deverá ser identificada como tratamento de dados pessoais, onde o conteúdo dessas informações integram os dados pessoais.

Sedimentada essa questão, na seara da responsabilidade civil verificamos que a dignidade da pessoa humana é o alicerce de todos os princípios morais universais. O direito à privacidade, a intimidade, está no seio da integridade da pessoa. Sem embargo, o cenário atual é bem diferente do que havia nos séculos passados. Estamos na era digital, onde a tecnologia desponta de forma veloz, possibilitando o acesso ilimitado das pessoas as mais diferentes plataformas digitais que movimentam todo um cenário econômico e social.

Nesse contexto temos o direito à privacidade de certa forma ameaçado na sociedade informacional, em virtude do fenômeno social tido como a superexposição das pessoas, que sem qualquer cerimônia alimentam os mais variados sites com seus dados pessoais sem ter a consciência e uma autorresponsabilização de que seus atos podem vir a violar seus direitos personalíssimos na medida em que os motores de busca coletam, indexam e armazenam as informações e disseminam nas redes sem qualquer responsabilidade no tratamento desses dados.

A pedra angular da sociedade informacional a que estamos inseridos é exatamente conciliar direitos personalíssimos, de caráter irrenunciáveis tais como a privacidade no sentido da proteção de dados e assegurar a liberdade no fluxo de informações aliada ao direito da liberdade de expressão, garantias fundamentais do cidadão digital.

A questão da privacidade é a tônica da violação de dados no mundo virtual, e uma vez violada o causador do dano deverá ressarcir a vítima restituindo-a a seu estado anterior. No entanto, há de se considerar que nenhum direito fundamental é absoluto quando estão inseridos no contexto social. Por diversas vezes nos deparamos com valores em conflito, onde caberá a responsabilidade civil invocar o princípio da proporcionalidade, essencial ao Estado de Direito,

para materializar-se a vontade concreta da lei, com equilíbrio, quando os direitos e as liberdades fundamentais das pessoas forem lesados os se apresentarem em rota de colisão³⁹².

O regulamento geral de proteção de dados é uma norma que garante a pessoa que teve seus dados violados por infração das normas contidas no regulamento o direito de obter uma indenização por parte do responsável pelo tratamento dos dados. O direito à privacidade está implícito no tratamento dos dados pessoais, onde o consentimento é o sustentáculo de todo o sistema de proteção de dados, o que deve ser um ato positivo, claro e explícito, não sendo considerado o silêncio como uma forma de anuência. A não observância dos princípios contidos no regulamento, licitude, lealdade, transparência, limitação das finalidades, minimização dos dados, exatidão, limite de conservação, integridade e confidencialidade e finalmente responsabilidade³⁹³, poderá contribuir para a violação de dados, cabendo ao titular dos dados requerer indenização ao responsável pelo tratamento, na forma do artigo 82º do RGPD.

As lesões que a informática pode causar a intimidade e a privacidade das pessoas ainda não estão traçadas pelo simples fato de não termos o domínio da dimensão de uma informação projetada no mundo virtual.

³⁹² SILVA, Roberto de Abreu – **A falta contra a legalidade constitucional**. Rio de Janeiro: Lumen Juris, 2002. ISBN 85-7387-221-7, p. 88-9.

³⁹³ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Em linha]. [Consult. 15 nov. 2018]. disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679>.

CONCLUSÃO

You have already zero privacy anyway. get over it.”

McNealy Scott

A violação de dados pessoais no mundo virtual vem sendo uma constante em função da velocidade com que os dados circulam no ciberespaço. Dados esses que são alimentados pelos próprios usuários da rede, que de forma voluntária e talvez até inocentes os ejetam na grande Web. Esse cenário, nos fez construir uma vasta pesquisa sobre uma das facetas do direito da personalidade, o direito à privacidade e o direito à proteção dos dados pessoais, elevados à categoria de direito fundamental.

O episódio do 11 de setembro foi um marco não só nos Estados Unidos, diretamente afetado, mas em todo o mundo, em especial a Europa. A partir daí iniciou-se um processo de vigilância sem precedentes. Diversas formas, as mais sofisticadas com alta tecnologia foram lançadas para monitorar vinte e quatro horas por dia em diversos cantos do mundo conversas, rostos, formas de agir, acessos a diversos sites, entre outros. Em função disso, o universo mudou e a privacidade das pessoas também foi colocada em xeque, já que se passou a valorizar a segurança nacional em detrimento de preservar a privacidade, os dados pessoais dos indivíduos. Estamos inseridos numa sociedade de informação, e não se pode negar que os cidadãos têm o direito à autodeterminação informativa, exercendo o seu direito de controle de suas informações dando o seu consentimento de forma clara e transparente, podendo retificá-las e até apagá-las quando lhe convier.

Na era digital, esse talvez seja um aspecto difícil de assimilar, pois os indivíduos vêm, por desconhecimento ou temeridade, colocando em perigo sua intimidade e integridade a cada dia de maneira mais marcante. As pessoas agem muitas vezes na internet sem contar com os riscos decorrentes da possibilidade da perda de controle de qualquer dado, informação, imagem sua que saia do âmbito de intimidade e que possa passar a ser de domínio público (com as danosas consequências que dessa ação/omissão derivam)³⁹⁴.

Iniciamos o primeiro capítulo fazendo alusão a privacidade no ciberespaço, onde considera-se um dos maiores desafios tendo em vista a velocidade com que as informações circulam no mundo virtual e o fato dos internautas transmitirem suas informações na rede em larga escala. Partimos de um estudo sobre o conceito de privacidade e intimidade, e até a sua

³⁹⁴ CONSALTER, Zilda Mara – **Direito ao Esquecimento**, p. 359.

dificuldade em estabelecer suas diferenças. Trouxemos à tona o caso emblemático, conhecido mundialmente por todos os grandes doutrinadores, o caso artigo intitulado “O direito de estar só”, de Samuel D. Warren e Louis D. Brandeis e o reconhecimento do respeito a vida privada através da Convenção Europeia dos Direitos do Homem e a Carta dos Direitos Fundamentais que defendeu e reiterou que a dignidade da pessoa humana é a base inviolável de todos os direitos fundamentais. Desde a antiguidade, a privacidade sempre foi alvo de preocupação pois está intimamente ligada na determinação da pessoa publicar algo particular, mas, que não se afaste de sua esfera privada.

A era digital através da internet faz parte do nosso dia a dia. Estamos cada vez mais dependentes dela. A vida se transformou em função das novas tecnologias sendo que também trouxeram desdobramentos que alcançam direitos fundamentais dos indivíduos, como a privacidade, o controle de seus dados pessoais entre outros de igual relevância. Estes na ânsia de surfar nas redes sociais, nos aplicativos que assolam os smartphones não se dão conta de que estão fornecendo e autorizando de forma tácita que suas informações sejam dispersadas na rede.

A gigante Google da Web, é uma potência no mercado virtual, onde milhares de pessoas acessam nos lugares mais distantes. Chegamos ao ponto de armazenarmos os nossos arquivos de texto, imagens ou outros na nuvem, “armazenamento cloud”, que também só poderão ser acessados se tiver acesso à internet, o que pode ser uma barreira, já que em alguns lugares a internet é falha. Os arquivos salvos na nuvem ficam armazenados em diversos servidores ao redor do mundo, isto é, estamos delegando nosso patrimônio pessoal, toda a nossa vida, a nossa história a servidores que sequer sabemos aonde ficam, e o que é feito com nossos dados.

O direito de privacidade na internet, necessariamente compreende quatro direitos-base: o direito de navegar com privacidade na internet, o direito de monitorar quem monitora, o direito de deletar os dados pessoais e o direito de proteger a identidade on line³⁹⁵.

No capítulo dois abordamos o direito à proteção de dados pessoais traçando a evolução da legislação em diferentes países da Europa, que contemplou a proteção de dados pessoais até a Regulamentação Geral de Proteção de Dados na União Europeia que impôs uma disciplina uniforme entre os vários Estados que compõem a União Europeia e a mais nova legislação do Brasil, a Lei 13.709/18 sobre a proteção de dados pessoais, que entrará em vigor em 2020. Sendo certo que o Marco Civil da Internet aprovado pelas Leis Brasileira em abril de 2014 estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil,

³⁹⁵ FORTES, Vinicius Borges - **Os Direitos de Privacidade e a Proteção de Dados Pessoais na Internet**. p. 6

considerando o acesso à internet uma condição para a cidadania³⁹⁶. Aponta de igual forma a responsabilidade dos provedores de internet. Registre-se ainda que o Marco Civil influenciou países como a França e Itália

Vivemos numa sociedade informacional onde não podemos ignorar a internet, lugar onde tudo acontece, onde expressamos nossa personalidade sem nos preocuparmos com os dados que inserimos. Entretanto, esses dados, se não protegidos podem causar danos irreparáveis aos titulares dos dados pessoais. Nesse sentido trabalhamos os pilares das normas de proteção de dados pessoais, os dados pessoais, a anonimização e pseudonimização e em especial o consentimento, assim considerado como baluarte da proteção de dados como forma de empoderar o titular dos dados. Esse controle de dados pessoais está implícito no conceito de autodeterminação informativa onde o indivíduo tem o poder de determinar as informações a seu respeito que podem circular nas redes sociais.

No capítulo três intitulado Data Breach- Violação de dados no mundo virtual. Os dados têm, hoje, um grande valor comercial porquanto é alimentado pelos cidadãos digitais que diariamente num simples click introduzem suas informações pessoais na rede de computadores, nos smartphones, sem se preocuparem com o destino das mesmas e quem manobra essas informações. Acreditam de forma ingênua, que sua privacidade jamais será violada, uma vez que o compartilhamento está restrito aos amigos, no caso das redes sociais. A violação de dados está positivada no Regulamento Geral de Proteção de Dados encontra sua definição no artigo 4º/12, que considera como uma violação de segurança que provoque de modo accidental ou ilícito, a destruição, a perda a alteração, a divulgação ou o acesso, não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento³⁹⁷. E, mesmo com uma norma protetiva em vigor, ainda assim tem-se notícias em diferentes países acerca de violação de dados por parte do titânico Google.

O direito ao esquecimento foi tratado no capítulo três, entendido como uma forma de proteção da vida privada, da honra e da imagem para preservar a dignidade da pessoa humana. A pessoa tem o direito de apagar, excluir dados relativos à sua vida privada, em que pese a dificuldade de se “esquecer” na internet. Uma vez propagada a informação esta circula através

³⁹⁶ BRASIL. Lei n.º 12.965, de 24 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.**[Em linha]. [Consult. 15 abr. 2019]. Disponível em WWW: <URL: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

³⁹⁷ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).** Em linha]. [Consult. 15 nov. 2018]. disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679>>.

de diversos motores de busca permanecendo infinitamente em diversos servidores. O Brasil não dispunha de uma legislação específica que retratasse o direito ao esquecimento, mas por extensão a Constituição da República Federativa do Brasil de 1988 resguardava a vida privada e a honra. Partindo dessa construção, os Tribunais Superiores de Justiça vêm enfrentando casos que buscava-se o direito ao esquecimento, casos emblemáticos verdadeiros divisores de água, já que ao envolver direito ao esquecimento de igual forma se acendem outros direitos fundamentais como a liberdade de expressão, a memória, o interesse público, valores esses que devem ser sopesados em cada caso concreto. O direito ao esquecimento não é absoluto e sofre limitações assim como os demais direitos fundamentais, eles necessitam estar sempre inseridos num contexto social onde a técnica de ponderação deverá sempre prevalecer. A internet, ao contrário das pessoas, não esquece. Deixa rasto, “pegadas digitais” e faz de memórias, acontecimentos³⁹⁸.

E por fim o capítulo reservado a responsabilidade civil pela violação de dados pessoais com previsão expressa no Regulamento Europeu no artigo 82º. Onde tem-se o responsável pelo tratamento ou subcontratante que deverá responder pelos danos causados ficando isento se provar que não é de modo algum responsável pelo evento que deu origem aos danos (artigo 82º-3). Tem-se aqui a responsabilidade subjetiva pela presunção de culpa, onde o dever de reparar é objetivo embora com mitigação, na medida em que o responsável pelo tratamento poderá se eximir da reparação provando algumas das escusas legais. Pode-se dizer que o regulamento adotou a responsabilidade semi-objetiva, com a presunção de culpa (artigo 487.º-1), deslocando o ônus da prova para o responsável pelo tratamento.

É de se estranhar que uma legislação de ponta como o Regulamento que teve o cuidado de individualizar a conduta do responsável pelo tratamento, os princípios que deve obedecer os meios que deve utilizar, para impedir a violação de dados tenha adotado a teoria subjetiva com base na presunção de culpa. A indenização às vítimas pode ficar comprometida na medida em que o responsável pelo tratamento ou subcontratante pode facilmente ilidir sua responsabilidade, pois tem acesso aos mais modernos meios tecnológicos para justificar que não foi o responsável pela violação dos dados.

A nosso sentir, não podemos ignorar o fato de que estamos na era digital, onde a tecnologia desponta a largos passos, a informação e a velocidade com que ela se espalha é algo até mesmo assustador, nessa rota, não há como se acolher a tese de responsabilidade subjetiva,

³⁹⁸ PINHEIRO, Alexandre Sousa – **Privacy e protecção de dados pessoais: A construção dogmática do direito à identidade informacional**. p.225.

ainda que com presunção de culpa nos casos de violação de dados uma vez que pode estar em perigo o direito do titular dos dados em se ver indenizado.

No contexto atual, a tese da responsabilidade objetiva, a responsabilidade sem culpa, vem ganhando notoriedade por ser a forma adequada de proteger os direitos personalíssimos por possíveis violações, garantido a vítima o direito de se ver indenizada independente de culpa do agente lesante. Essa teoria poderia ser plenamente aplicável e adotada no regulamento por preencher os pressupostos que caracterizam a responsabilidade objetiva, como veremos a seguir.

O primeiro pressuposto a destacar é no que tange a atividade de risco. Quando a atividade desenvolvida pelo autor do dano (no caso o responsável pelo tratamento ou subcontratante) é por sua natureza de risco para o direito alheio. Nesse ponto, não paira qualquer dúvida de que a atividade do responsável pelo tratamento ou subcontratante é de grande risco por envolver informações de caráter pessoal de pessoa identificada ou identificável, são informações de caráter eminentemente privado, onde uma falha no meio de tratamento, ou uma finalidade diferente da autorizada na norma, poderá resultar em danos de grande repercussão atingindo bens personalíssimos além da privacidade. A atuação do responsável pelo tratamento ou subcontratante deverá ser prestada com toda a técnica a fim de não frustrar a expectativa legítima de segurança, não causando danos ao titular dos dados.

Não basta a atividade ser de risco, porque inúmeras outras atividades são de risco e necessárias a sociedade, o risco implica no atuar com segurança para não causar danos, em o fazendo responderá independentemente de culpa. Nesse sentido, a própria definição de violação de dados contida no regulamento prediz uma violação de segurança de modo accidental ou ilícito (artigo 4º-12). A violação do dever de segurança, ocorre quando o serviço é realizado com defeito, o que impõe o dever de indenizar na responsabilidade objetiva.

O pressuposto do nexo causal, também indispensável, não o sendo no caso da responsabilidade fundada no risco integral, o que não é o caso. Se inexistiu defeito na atuação do responsável pelo tratamento ou subcontratante, não havendo relação de causa entre o dano e a atividade desempenhada não se fala em indenizar.

Um outro ponto que deverá ser analisado é a responsabilidade pelo fato de outrem no que se refere ao responsável pelo tratamento dos dados ou subcontratante, assim definido no artigo 4º /7-8, que os define como uma pessoa singular ou coletiva, autoridade pública, a agência ou outro organismo³⁹⁹. Ou seja, os responsáveis ou subcontratantes podem ser pessoas

³⁹⁹ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre**

jurídicas, ou ainda que se admita que a empresa nomeie uma pessoa específica como responsável pelo tratamento ou subcontratante, a relação de subordinação entre a pessoa singular e a empresa que delegou a função se faz presente, onde o comitente é considerado o afiançador dos efeitos ofensivos praticados pelos seus agentes, respondendo de forma objetiva, independente de culpa. Podendo exercer o direito de regresso contra aquele que agiu com a falta de dever de cuidado, no caso o empregado.

Nessa linha, o artigo 500.º do código civil adota a responsabilidade objetiva, deduzindo que aquele que encarrega outrem de qualquer comissão responde independentemente de culpa, pelos danos que o comissário causar, desde que sobre este recaia também a obrigação de indenizar. Donde se conclui que o dano tenha ocorrido no exercício da função. A relação funcional entre o dano e a atividade da pessoa singular se faz necessário para que a empresa na qualidade de empregador responda pelos atos de seus empregados.

Pelo que foi exposto, conclui-se que a teoria da responsabilidade objetiva é a que mais se coaduna com a realidade atual, uma sociedade informacional onde o direito à privacidade e o direito à proteção de dados pessoais são direitos que estão diuturnamente em conflito com outros direitos fundamentais como o direito à liberdade de expressão e a liberdade de informação no ciberespaço. A responsabilidade semi-objetiva adotada pelo regulamento, ao nosso sentir, possibilita um entrave para o titular dos danos se ver ressarcido, em função de que o responsável pelo tratamento ou subcontratante têm fácil acesso as mais sofisticadas tecnologias para justificar uma possível falha na violação de dados, eximindo-os do direito a indenizar como preceitua o artigo 82º -3. A aplicabilidade da responsabilidade objetiva em sede do regulamento possibilitaria uma maior amplitude e segurança jurídica para aquele que tiveram seus dados violados garantindo-lhes o direito a uma indenização em respeito a dignidade da pessoa humana.

As vítimas que tiveram seus dados violados jamais poderão ficar indenidos sob uma escusa de que não é possível identificar o causador do dano. A legislação em vigor é clara no sentido de que qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do regulamento tem direito a receber uma indenização do responsável pelo tratamento de dados ou do subcontratante, prevendo de igual forma a solidariedade quando tem se mais de

circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Em linha]. [Consult. 15 nov. 2018]. disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679>>.

um envolvido⁴⁰⁰. Não se cogita responsabilidade, independente da modalidade, se não está caracterizado um dever jurídico preexistente. Não sendo possível evitar o dano as pessoas devem se primar por uma reparação justa com vista a se fazer a verdadeira, justa e perfeita justiça.

Diante da exposição do presente trabalho, cuja temática girou em torno da violação de dados pessoais como um desafio da sociedade informacional, verificamos a dificuldade de proteger de forma eficiente e eficaz os dados pessoais dos indivíduos, considerando a estrutura e funcionamento da internet, dos diversos servidores que estão ao redor do mundo com os nossos dados pessoais. Primeiramente porque os internautas não têm noção real dos riscos resultantes do desvio do controle de seus dados, passando-os a ser públicos. O seja, o que é considerado privado na internet torna-se público ao compartilhar as informações ou ao expor suas ideias, seu perfil. A exposição pessoal virou febre na internet. As pessoas dão a saber ao mundo virtual todas as suas ações e sua forma de viver.

Entendemos que o controle dessa violação de dados só será contido na medida em que as autoridades investirem num processo em massa de conscientização dos internautas não só da necessidade de se sopesar o que é colocado na web, mas também do entendimento dos riscos latentes em compartilhar seus dados, imagens de sua vida privada nas redes sociais. O mito do anonimato na internet deverá ser desmistificado, mesmo se camuflando atrás de um pseudônimo pode ser perseguido e identificado.

O titular dos dados pessoais não pode dispor do exercício da autodeterminação informativa e nem permitir que seja usurpados esses direitos sob a bandeira da ameaça à segurança pública.

Enfim, é fato que a nossa privacidade vem correndo riscos sérios em nome de uma segurança pública numa sociedade de insegurança. Não podemos evitar a vigilância sem fronteiras e nem tampouco prever os riscos e seus desdobramentos, mas temos o dever de lutar alicerçados no princípio basilar da dignidade da pessoa humana.

⁴⁰⁰ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Em linha]. [Consult. 15 nov. 2018]. disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679>>.

REFERÊNCIAS

ALERTA SECURITY. **Os Pilares da Segurança da Informação**. [Em linha]. [Consult. 28 maio 2019]. Disponível em WWW:<URL:<https://alertasecurity.com.br/blog/31-base-capitulo-1-os-pilares-da-seguranca-da-informacao>>.

ALONSO, Felix Ruiz – Pessoa, intimidade e o direito à privacidade. *in*: MARTINS FILHO, Ives Gandra; MONTEIRO JUNIOR, Antônio Jorge (Coord.). **Direito à privacidade**. São Paulo: Centro de Extensão Universitária, 2005. ISBN 85-98239-36-4.

ARGENTINA. Lei 25.326 – **Proteção de Dados Pessoais**. [Em linha]. [Consult. 11 maio 2019]. Disponível em WWW:<URL:<http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm>>.

ARGENTINA. Lei 25.326. **Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales**. [Em linha]. [Consult. 11 maio 2019]. Disponível em WWW:<URL:<http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm>>.

ARGENTINA. Ley 27275. **Artigo 1º. Derecho de Acceso a La Información Pública**. [Em linha]. [Consult. 11 maio 2019]. Disponível em WWW:<URL:<http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/norma.htm>>.

ASENJO, Porfirio Barroso e TALAVERA, Maria del Mar - La libertad de expresión y sus limitaciones constitucionales. **Revista de Ciencias Sociales y Humanas**, 15 (2011).

BARBOSA, Mafalda Miranda - Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil. **Revista de Direito Comercial**. [Em linha]. [Consult. 6 jun.2019]. Disponível em WWW:<URL:<https://www.revistadedireitocomercial.com/data-controllers-e-data-processors>>.

BILBAO, Maria Nieves de La Serna - **El Derecho a La Protección de Datos de Carácter Personal En Europa**. [Em linha]. [Consult. 30 out. 2018] . Disponível em WWW:<URL:http://ocw.uc3m.es/derecho-administrativo/derecho-de-las-tecnologias-de-la-informacion/material-de-clase-1/leccion_2.pdf>.

BIONI, Bruno RICARDO - **Xequemate o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPOPAI, 2015.

BLOG DE PROTECCIÓN DE DATOS PARA EMPRESAS Y AUTÓNOMOS - **Cuál fue el importe de la multa a las primeras empresas que incumplieron el RGPD?** [Em linha]. [Consult. 04 maio 2019]. Disponível em WWW:<URL:https://protecciondatos-lopdp.com/empresas/multa-empresas-incumplieron-rgpd/#Nuevos_importes_para_2019>.

BRASIL, Superior Tribunal de Justiça. **REsp. nº 1.501.603 RJ**. [Em linha]. [Consult. 22 Abr. 2019]. Disponível em WWW:<URL:<https://ww2.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=1668833&tipo=0&nreg=>

201402900716&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20171218&formato=PDF&salvar=false>.

BRASIL. **Constituição da República Federativa do Brasil**, de 05 de outubro de 1988. [Em linha]. [Consult. 27 de abr. de 2019]. Disponível em WWW: <URL:http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.html>.

BRASIL. **Lei n.º 10.406**, de 10 de janeiro de 2001. Institui o Código Civil. [Em linha]. [Consult. 01 de jan. 2018]. Disponível em WWW: <URL: http://www.planalto.gov.br/ccivil_03/leis/2002/110406.html>.

BRASIL. **Lei n.º 12.527**, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências [Em linha]. [Consult. 19 abr. 2019]. Disponível em WWW: <URL: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm>.

BRASIL. **Lei n.º 12.965**, de 24 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil [Em linha]. [Consult. 15 abr. 2019]. Disponível em WWW: <URL: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>.

BRASIL. **Lei n.º 13.709**, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet) [Em linha]. [Consult. 10 abr. 2019]. Disponível em WWW: <URL:http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>.

BRASIL. Superior Tribunal de Justiça. **REsp. nº 1.316.921 RJ**. [Em linha]. [Consult. 22 abr. 2019]. Disponível em WWW:<URL:<https://stj.jusbrasil.com.br/jurisprudencia/22026857/recurso-especial-resp-1316921-rj-2011-0307909-6-stj/relatorio-e-voto-22026860?ref=juris-tabs>>.

BRASIL. Superior Tribunal de Justiça. **REsp. nº 1.334.097 RJ**. [Em linha]. p. 4-5. [Consult. 13 maio 2019]. Disponível em WWW:<URL:https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=29381336&num_registro=201201449107&data=20130910&tipo=91&formato=PDF>.

BRASIL. Superior Tribunal de Justiça. **REsp. nº 1.335.153 RJ**. [Em linha]. [Consult. 13 maio 2019]. Disponível em WWW:<URL:https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=29381336&num_registro=201201449107&data=20130910&tipo=91&formato=PDF>.

CACHAPUZ, Maria Cláudia Mércio - **Privacidade, proteção de dados e autodeterminação informativa** [Em linha]. [Consult. 19 Maio 2019]. Disponível em WWW:<URL:<https://revistajuridica.presidencia.gov.br/index.php/saj/article/view/126/118>>.

CÁDIMA, Francisco Ruy – **O Facebook, as redes sociais e o direito ao esquecimento**. [Em linha]. [Consult. 03 out. 2015]. Disponível em WWW: <URL:http://www.researchgate.net/publication/277556597_O_Facebook_as_redes_sociais_e_o_direito_ao_esquecimento>.

CARELLO, Clarissa; CACHAPUZ, Maria Cláudia - **A Doutrina do “Right to be Forgotten” Pela Perspectiva das Relações Entre Privados**. [Em linha]. [Consult. 17 maio 2019]. Disponível em WWW:<URL:www.ajuris.org.br/OJS2/index.php/REVAJURIS/article/download/.../Ajuris_140_DT3>.

CARVALHO, Luis Gustavo Grandinetti Castanho – **Direito à Privacidade**. [Em linha] [Consult. 31 maio 2018] Disponível em WWW:<URL:http://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista02/revista02_51.pdf>.

_____. - **Direito de informação e liberdade de expressão**. Rio de Janeiro: Renovar, 1999. ISBN 8571471495.

CASTELLANO, Pere Simon - **Neutralidad de la red y otros retos para el futuro de Internet - Actas del VII Congreso Internacional Internet**. [Em linha]. [Consult. 19 maio 2019]. Disponível em WWW:<URL:http://www.huygens.es/ebooks/Neutralidad_de_la_red.pdf>.

_____. - **O regime constitucional do direito de ser esquecido na internet**. [Em linha]. [Consult. 19 maio 2019]. Disponível em WWW:URL:https://www.academia.edu/898086/El_r%C3%A9gimen_constitucional_del_der echo_al_olvido_en_Internet>.

CHEHAB, Gustavo - O direito na sociedade da informação. **Revista dos Tribunais**. 104:952 (2015).

CNIL. **Présentation du Rapport d’activité 2018 et des enjeux 2019 de la CNIL** [Em linha]. [Consult. 7 maio 2019]. Disponível em WWW:<URL:https://www.cnil.fr/fr/presentation-du-rapport-dactivite-2018-et-des-enjeux-2019-de-la-cnil>.

CONSALTER, Zilda Mara – **Direito ao Esquecimento**. Curitiba: Juruá, 2017. ISBN 978-85-362-6485-11.

CONSELHO DA JUSTIÇA FEDERAL. **VI Jornada de Direito Civil** [Em linha]. [Consult. 14 maio 2019]. Disponível em WWW:<URL:https://www.cjf.jus.br/enunciados/enunciado/142>.

COSTA JUNIOR, Paulo José da - **O direito de estar só: tutela penal da intimidade**. 2ª ed. São Paulo: RT, 1995. ISBN: 9780786162635.

COSTA, Andre Brandão Nery – Direito ao esquecimento na Internet: a Scarlet letter digital in: SCHREIBER, Anderson - **Direito da personalidade**. 2013.

CUEVA, Pablo Lucas Murillo - **Informática y protección de datos personales (estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal)**. España: Centro de Estudios Políticos y Constitucionales (España), 1993. ISBN: 84-259-0940-6.

DANTAS, Fernanda Lage Alves – **O Paradoxo do Direito à Privacidade e sua Operacionalização**. Rio de Janeiro: Lumen Juris, 2016. ISBN 978-85-8440-852-8.

DELGADO, Lucrecio Rebollo – **Protección de Datos en Europea**. Madrid: Dykinson, [sd]. ISBN 978-84-9849-333-7.

_____ – **Vida Privada Y Protección de Datos en la Unión Europea**. Madrid: Dykinson, 2008. ISBN 978-84-9849-333-7.

DELIA FERREIRA *apud* SANTOS, Antonio Jeová – **Dano Moral na Internet**. São Paulo: Metodo, 2001. ISBN 858645625X.

DINIZ, Maria Helena - **Curso de Direito Civil Brasileiro: Teoria Geral do Direito Civil**. Rio de Janeiro: Saraiva, 2015. ISBN 9788502143326.

DONEDA, Danilo – **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006. ISBN 85-7147-562-8.

_____ - **Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade**. [Em linha]. [Consult. 15 fev. 2018]. Disponível em WWW: <URL:<http://www.egov.ufsc.br/portal/sites/default/files/anexos/8196-8195-1-PB.htm>>.

_____ - **Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade**. [Em linha]. [Consult. 15 fev. 2018]. Disponível em WWW:<URL:<http://www.egov.ufsc.br/portal/sites/default/files/anexos/8196-8195-1-PB.htm>>.

DOTTI, René Ariel. **Proteção da vida privada e liberdade de informação: possibilidades e limites**. São Paulo: Revista dos Tribunais, 1980. ISBN: 978-8520300367.

ESPANHA. **Constituição Espanhola**. [Em linha]. [Consult. 28 out. 2018]. Disponível em WWW: <URL:<https://www.tribunalconstitucional.es/es/tribunal/normativa/Normativa/CEportugu%C3%A9s.pdf>>.

ESPANHA. Lei Orgânica 5/1992, de 29 de outubro. De regulación del tratamiento automatizado de los datos de carácter personal [Em linha]. [Consult. 22 out. 2018]. Disponível em WWW: <URL:<https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189>>.

ESTADO TAPA NOMBRES EM CONTRATOS PÚBLICOS. PROTEÇÃO DE DADOS DIZ QUE “NÃO FAZ QUALQUER SENTIDO”. TSF Radio Notícias. [Consult. 04 Maio 2019]. Disponível em WWW:<URL:<https://www.tsf.pt/sociedade/interior/estado-tapa-nomes-em-contratos-publicos-protecao-de-dados-diz-que-nao-faz-qualquer-sentido-10783457.html>>.

EUR-LEX 32003D0490. [Em linha]. [Consult. 11 maio 2019]. Disponível em WWW:<URL:<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32003D0490&from=EN>>.

EUROPA (AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA E CONSELHO DA EUROPA). **Manual da Legislação Europeia sobre Proteção de Dados**. [Em linha]. p.16. [Consult. 01 nov. 2018]. Disponível em <<https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-pt.pdf>>.

EUROPA. **Carta de Los Derechos Fundamentales de la Unión Europea** (2000/C 364/01). Diário Oficial de las Comunidades Europeas [Em Linha]. [Consult. 18 abr. 2019]. Disponível em WWW:<URL:http://www.europarl.europa.eu/charter/pdf/text_es.pdf>.

EUROPA. **Convenção de Aplicação do Acordo de SCHENGEN, de 14 de junho de 1985.** [Em linha]. [Consult. 16 nov. 2018]. Disponível em WWW: <URL:[https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:42000A0922\(02\)&from=ES](https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:42000A0922(02)&from=ES)>.

EUROPA. Tribunal de Justiça da União Europeia. Acórdão do Tribunal de Justiça (Grande Secção) de 13 de maio de 2014. **Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González.** [Em linha]. [Consult. 13 maio 2019]. Disponível em WWW:<URL:<https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0131>>.

EUROPEAN COURT OF HUMAN RIGHTS. **Convenção Europeia de Direitos do Homem.** [Em linha]. [Consult. 01 fev. 2018]. Disponível em WWW: <URL:http://www.echr.coe.int/Documents/Convention_por.pdf>.

FARIA, José Eduardo *apud* MINHOTO, Antonio Celso Baeta – **Globalização e Direito: o Impacto da Ordem Mundial Global sobre o Direito.** São Paulo: Juarez de Oliveira, 2004. ISBN 85-7453-460-9.

FARINHO, Domingos Soares – **Intimidade da Vida Privada e Media no Ciberespaço.** Coimbra: Almedina, 2006, ISBN: 9789724027401.

FAZENDEIRO, Ana – **Regulamento Geral sobre a Proteção de Dados.** 2.^a ed. Coimbra: Almedina, 2018. ISBN 978-972-40-7154-1.

FIGUEIRA, Alexandra - **Todos os dias há uma violação de dados pessoais.** [Em linha]. [Consult. 2 maio 2019]. Disponível em WWW:<URL:<https://www.jn.pt/inovacao/interior/todos-os-dias-ha-uma-violacao-de-dados-pessoais-10146047.html>>.

FILHO CAVALIERI, Sergio – **Programa de Responsabilidade Civil.** 7.^a ed. São Paulo: Atlas, 2007. ISBN 978-85-224-4688-9.

FILHO JOSE, Wagson Lindolfo José - **Teoria dos círculos concêntricos da esfera da vida privada.** [Em linha]. [Consult em 30 Jan. 2018]. Disponível em WWW: <URL:<http://www.magistradotrabalhista.com.br/2016/03/teoria-dos-circulos-concentricos-da.html>>.

FORTES, Vinicius Borges - **Os Direitos de Privacidade e a Proteção de Dados Pessoais na Internet.** Rio de Janeiro: Lumen Juris, 2016. ISBN978-85-8440-563-3.

FRANÇA. **LOI n° 2016-1321, du 7 Octobre 2016.** [Em linha]. [Consult. 25abr.2019]. Disponível em WWW: <URL:<https://www.legifrance.gouv.fr/affichLoiPubliee.do?idDocument=JORFDOLE000031589829&type=general&legislature=14>>.

FRANCEZ. André. **Direito do entretenimento na Internet.** São Paulo: Saraiva, 2013. ISBN: 9788502208391.

FROSINI, Vittorio - Bancos de Datos Y Tutela de La Persona. [Em linha]. [sl]: **Revista de estudos políticos.** 30 (1982). p. 27. [Consult. 07 nov. 2018]. Disponível em WWW: <URL:<https://dialnet.unirioja.es/servlet/articulo?codigo=26724>>.

GAGLIANO, Pablo Stolze. PAMPLONA FILHO, Rodolfo - **Novo Curso de Direito Civil**, Volume 3: Responsabilidade Civil. São Paulo: Saraiva, 2003. ISBN 978-85-472-1647-4

GONZÁLES, José Alberto – **Responsabilidade Civil**. Quid Juris, 2013. ISBN 9789727246410.

GREENWALD, Gleen – **Sem Lugar pra se Esconder**. Rio de Janeiro: 2014. ISBN 978-85-431-0096-8.

GUERRA, Gustavo Rabay. Direito a Inviolabilidade e sigilo de comunicações privadas armazenadas: um grande salto rumo à proteção da privacidade na rede *in*: LEITE, George Salomão; LEMOS, Ronaldo. (Coord.). **Marco civil da internet**. São Paulo: Atlas, 2014.

HENRIQUE, Lygia Maria M.; ANDRADE, Vitor Moraes - **Vazamento de dados: uma preocupação da Lei Geral de Proteção de Dados** [Em linha]. [Consult. 01 nov. 2018]. Disponível em WWW:<URL:<https://www.migalhas.com.br/dePeso/16,MI298452,101048-vazamento+de+dados+uma+preocupacao+da+Lei+Geral+de+Protecao+de+Dados>>.

HIGUERAS, Manuel Heredero - **La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del censo de población**. [Consult. 14 nov. 2018]. Disponível em WWW:<URL:<https://revistasonline.inap.es/index.php?journal=DA&page=article&op=view&path%5B%5D=4687>>.

ITS - **Proposta para a criação da Autoridade Brasileira de Proteção aos Dados Pessoais**. [Em linha]. [Consult. 2 maio 2019]. Disponível em WWW:<URL:<https://itsrio.org/wp-content/uploads/2018/12/autoridade-protecao-de-dados.pdf>>.

JABUR, Gilberto Haddad – A dignidade e o rompimento de privacidade. *in*: MARTINS FILHO, Ives Gandra; MONTEIRO JUNIOR, Antônio Jorge (Coord.). **Direito à privacidade**. 2005.

JESUS, Damasio; MILAGRE, Jose Antonio – **Marco Civil da Internet Comentários à Lei 12.965/14**. São Paulo: Saraiva, 2014. ISBN 978-85-02-23018-7.

JUNIOR REALE, Miguel – **Os Direitos da Personalidade**. [Em linha]. [Consult. 26 jan. 2018]. Disponível em WWW: <URL:<http://www.miguelreale.com.br/artigos/dirpers.htm>>.

KOEPSELL, David R. – **A Ontologia do Ciberespaço**. Madras, 2004. ISBN 8573748907.

KUNDERA, Milan *apud* FERNANDES, Paulo Silva - **Globalização, “Sociedade de Risco” e o Futuro do Direito Penal**. São Paulo: Almedina, 2001. ISBN 978-9724015408.

LAM, Stephen - **Cambridge Analytica pode ter usado dados de 63 mil utilizadores portugueses**. [Em linha]. [Consult. 2 maio 2019]. Disponível em WWW:<URL:<https://www.dn.pt/media/interior/cambridge-analytica-pode-ter-usado-dados-de-63-mil-utilizadores-portugueses-9235928.html>>.

LEMOS, Roberto - O marco civil como símbolo do desejo por inovação no Brasil *in*: LEITE, George Salomão; LEMOS, Ronaldo. (Coord.). **Marco civil da internet**. 2014.

LIMA, Cíntia Rosa Pereira de – **Direito ao esquecimento e internet: o fundamento legal no direito comunitário europeu, no direito italiano e no brasileiro**. Revista dos Tribunais. São Paulo.

LIMONG, Cristina de Souza – Limites ao Exercício do Direito ao Esquecimento. **Revista de Direito Brasileira**. 14:6 (2016). [Em linha]. [Consult. 17 maio 2019]. Disponível em WWW:<URL:<https://www.indexlaw.org/index.php/rdb/article/view/2982>>.

LUCAS, Pablo Murillo de La Cueva - **O direito à autodeterminação informativa**. Madrid: Tecnos, 1990.

MARIO, Caio - **Responsabilidade Civil**. 12. ed. São Paulo: Saraiva, 2018.

MARTINEZ, Pablo Dominguez - **Direito ao Esquecimento - A proteção da memória individual na sociedade da informação**. Rio de Janeiro: Lumen Juris, 2014. ISBN 978-8584401055, p. 58.

MARTINS, Guilherme Magalhães - O direito ao esquecimento na internet e a proteção dos consumidores. **Revista Luso-Brasileira de Direito do Consumo**. Curitiba. 7:25 (2017), 61-99.

MINHOTO, Antonio Celso Baeta – **Globalização e Direito: o Impacto da Ordem Mundial Global sobre o Direito**. 2004.

MONTREAL, Novoa *apud* SANTOS, Antonio Jeová – **Dano Moral na Internet**. São Paulo: Método, 2001. ISBN 858645625X.

MORAES, Melina Ferracini – **Direito ao Esquecimento na Internet**. Curitiba: Juruá, 2018. ISBN 978-85-362-8204-6.

MOREIRA, Rogerio de Meneses Fialho - **Direito ao esquecimento não se confunde com censura**. [Em linha]. [Consult. 17 maio 2019]. Disponível em WWW:<URL:<http://agenciabrasil.ebc.com.br/geral/noticia/2014-06/para-sabado-ii-direito-a-esquecimento-divide-opinioes-de-especialistas>>.

NAVARRI, Veronica - **Internet Bill of Rights: un piccolo passo per l'uomo, un grande passo per l'umanità**. [Em linha]. [Consult. 21 abr. 2019]. Disponível em WWW: <URL: <https://medium.com/argomenti-di-diritto-dei-media-digitali/internet-bill-of-rights-un-piccolo-passo-per-luomo-un-grande-passo-per-l-umanit%C3%A0-5442af2a3750>>.

NERY JUNIOR; Nelson. NERY; Rosa Maria de Andrade. **Constituição Federal Comentada e Legislação Constitucional**. 4. ed. São Paulo: Revista dos Tribunais, 2013. ISBN: 9788520347416.

NETO RULLI, Antonio; JUNIOR, Antonio Rulli - Direito ao Esquecimento e o Superinformacionismo: Apontamentos no Direito Brasileiro dentro do Contexto de Sociedade da Informação. **Revista do Instituto do Direito Brasileiro**, 1:1 (2012), 419-34. [Em linha]. [Consult. 13 maio 2019]. Disponível em WWW:<URL:<https://blook.pt/publications/publication/296c62416268/>>.

NOVELINO, Marcelo. **Direito constitucional**. 2ª edição. São Paulo: Método, 2008.

OECD. **Directrices de La OCDE Sobre Protección de La Privacidad Y Flujos Transfronterizos de Datos Personales** [Em linha]. p. 1. [Consult. 24 out. 2018]. Disponível em WWW: <URL:<https://www.oecd.org/sti/ieconomy/15590267.pdf>>.

OLIVEIRA, Jaqueline Simas de - **Google é multado em 50 milhões de euros na França por violação ao GDPR**. [Em linha]. [Consult. 2 Maio 2019]. Disponível em WWW: <URL:<https://www.jota.info/opiniao-e-analise/artigos/google-e-multado-em-50-milhoes-de-euros-na-franca-por-violacao-ao-gdpr-24012019>>.

PAESANI, Liliana Minardi – **Direito e Internet: Liberdade de Informação, privacidade e Responsabilidade Civil**. São Paulo: Atlas, 2013. ISBN 978-85-224-7891-0, p. 20.

PALMA, Fernando - **CID: Confidencialidade, Integridade e Disponibilidade**. [Em linha]. [Consult. 2 maio 2019]. Disponível em WWW:<URL:<https://www.portalgsti.com.br/2016/11/cid-confidencialidade-integridade-e-disponibilidade.html>>.

PEREIRA, Marcelo Cardoso - **Direito à Intimidade na Internet**. Curitiba: Juruá, 2011. ISBN 85-362-0516-4.

PERÉZ ,Maria Mercedes Serrano - El derecho fundamental a la Protección de Datos. Su contenido esencial. **Nuevas políticas públicas** [Em linha]. (2005). [Consult. 10 abr 2019]. p. 225. Disponível em WWW:<URL:<https://dialnet.unirioja.es/servlet/revista?codigo=7332>>.

PINHEIRO, Patricia Peck – **Proteção de Dados Pessoais Comentários à Lei 13.709/2018 (LGPD)**. São Paulo: Saraiva Educação, 2018. ISBN 978-85-53605-28-6, p. 806.

POMPEU, Ana - **MJ instaura processo contra Google Brasil por violação de privacidade**. [Em linha]. [Consult. 01 nov. 2018]. Disponível em WWW:<URL:<https://www.conjur.com.br/2019-fev-07/ministerio-abre-processo-google-violacao-privacidade#author>>.

Portugal sem Meios de Proteção de Dados Pessoais, CNPD Alerta o Agravamento da Situação. [Em linha]. [Consult. 30 abr. 2018]. Disponível em WWW:<URL:<https://jornaleconomico.sapo.pt/noticias/portugal-sem-meios-de-protecao-de-dados-pessoais-cnpd-alerta-o-agravamento-da-situacao-375383>>.

PORTUGAL. Convenção 108. **Para a Protecção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal**. [Em linha]. [Consult. 24 out. 2018]. Disponível em WWW: <URL:<https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>>.

PORTUGAL. Constituição Portuguesa. [Em linha]. [Consult. 28 out. 2018]. Disponível em WWW: <URL:<https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>>

RBADMIN, RGPD – **Violação de Dados: Cia (Confidencialidade, Integridade e Acessibilidade)**. [Em linha]. [Consult. 2 maio 2019]. Disponível em WWW:<URL:<https://www.rbconsulting.pt/tag/rgpd/>>.

REGO, Giancarlos Coutinho do - **Direito ao Esquecimento: proteção à memória individual** [Em linha]. [Consult. 19 maio 2019]. Disponível em

WWW:<URL:<https://giancarlosrego.jusbrasil.com.br/artigos/327294577/direito-ao-esquecimento-protecao-a-memoria-individual>>.

RENASCENÇA - **Acesso irregular a dados do Hospital do Barreiro “pode não ser caso único” e vai ser investigado.** [Em linha]. [Consult. 2 Maio 2019]. Disponível em WWW:<URL:<https://rr.sapo.pt/noticia/117635/acesso-irregular-a-dados-do-hospital-do-barreiro-pode-nao-ser-caso-unico-e-vai-ser-investigado>>.

RODEGHERI, Leticia Bodanese; RAMINELLI, Francieli Puntel; OLIVEIRA, Rafael Santos de – Dignidade da pessoa humana e intimidade na sociedade informacional: o direito ao esquecimento de dados pessoais. In Congresso Internacional de Direito e Contemporaneidade, 2 UFSM, 2013, Santa Maria – RS. p. 879-890.

RODOTÁ, Stefano - “**La Carta dei Diritti in Internet**” – **Privacy Italia.** [Em linha]. [Consult. 26 abr. 2019]. Disponível em WWW: <URL:<https://www.privacyitalia.eu/rodota-un-profeta-dei-diritti-sulla-rete/3483/>>.

_____ - **A Vida na Sociedade de Vigilância – A privacidade hoje.** Rio de Janeiro: Renovar, 2008. ISBN 978857147-688-2.

RUIVO, Inês de Castro - **Anonimização de dados pessoais: o que deve saber.** Portugal: Coluna Juridica, 2016.

RUVIC, Dado - **Três utilizadores processam Facebook** [Em linha]. [Consult. 2 maio 2019]. Disponível em WWW:<URL:<https://www.dn.pt/media/interior/facebook-tres-utilizadores-processam-rede-social-por-alegada-violacao-de-privacidade-9220044.html>>.

SANTOS, Antonio Jeová – **Dano Moral na Internet.** São Paulo: Metodo, 2001. ISBN 858645625X.

SARLET, Ingo Wolfgang - **Tema da moda, direito ao esquecimento é anterior à internet** [Em linha]. [Consult. 13 maio 2019]. Disponível em WWW:<URL:<https://www.conjur.com.br/2015-mai-22/direitos-fundamentais-tema-moda-direito-esquecimento-anterior-internet>>.

SCHREIBER, Anderson - **Direito da personalidade.** 2. ed. São Paulo: Atlas, 2013. ISBN. 978-85.224-7895-8.

SCHWABE, Jürgen - **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão.** Montevideo: Konrad – Denauer Stiftung, 2005. ISBN: 9974794218.

SEGURADO, Rosemary; LIMA, Carolina Silva Mandú de; AMENI, Cauê S. Regulamentação da internet: perspectiva comparada entre Brasil, Chile, Espanha, EUA e França. **História, Ciências, Saúde – Manguinhos.** Rio de Janeiro. ISSN 0104-5970. 22 (2015).

SÉNECA, Hugo - **CNPd: Hospital do Barreiro multado em 400 mil euros por permitir acessos indevidos a processos clínicos.** [Em linha]. [Consult. 01 Nov. 2018]. Disponível em WWW:<URL:<http://exameinformatica.sapo.pt/noticias/mercados/2018-10-19-CNPd-Hospital-do-Barreiro-multado-em-400-mil-euros-por-permitir-acessos-indevidos-a-processos-clinicos>>.

SENTENCIA DE 15 DE DICIEMBRE DE 1983, DEL TRIBUNAL CONSTITUCIONAL FEDERAL ALEMÁN, LEY DEL CENSO. [Em linha]. [Consult. 14 Nov. 2018]. Disponível em WWW: <URL:<http://www.derecho-chile.cl/sentencia-de-15-de-diciembre-de-1983-del-tribunal-constitucional-federal-aleman-ley-del-censo/>>.

SICHES, Luis Recaséns - **Experiência Jurídica, Naturaleza de la Cosa e Lógica Razonable**. México: Fondo de Cultura Económica, 1971.

SILVA, Carlos Bruno Ferreira da – **Proteção de Dados e Cooperação Transacional: Teoria e Prática na Alemanha, Espanha e Brasil**. Belo Horizonte: Arraes, 2014. ISBN 978-85-8238-056-7.

SILVA, Jose Afonso - **Curso de Direito Constitucional Positivo**. 11. ed. São Paulo: Malheiros, 1996.

SILVA, Roberto de Abreu – **A falta contra a legalidade constitucional**. Rio de Janeiro: Lumen Juris, 2002. ISBN 85-7387-221-7.

SOLOVE, Daniel J. - **The Digital Person Technology and Privacy in the Information Age**. United States of America: General Editors, 2004. ISBN 0-8147-9846-2.

SOPRANA, Paula - **Banco Inter fecha acordo e pagará R\$ 1,5 milhão por vazamento de dados** [Em linha]. [Consult. 23 dez. 2018]. Disponível em WWW:<URL:<https://www1.folha.uol.com.br/tec/2018/12/banco-inter-pagara-multa-de-r-15-milhao-por-vazamento-de-dados.shtml>>.

SOUZA, Carlos Affonso; LEMOS Ronaldo - **Marco civil da internet: construção e aplicação**. Juiz de Fora: Editar, 2016. ISBN: 978-85-7851-156-2.

TERWANGNE, Cécile - **Privacidad en Internet y el derecho a ser olvidado/derecho al olvido**. [Em linha]. [Consult. 13 maio 2019]. Disponível em WWW:<URL:<http://www.redalyc.org/articulo.oa?id=78824460006>>.

TOURIÑO, Alejandro – **El Derecho al olvido y a la intimidad em internet**. Madrid: Catarata, 2014. ISBN 978-84-8319-880-3.

TRACTO - **Number of internet users worldwide from 2005 to 2018 (in millions)**. [Em Linha]. [Consult. 23 maio 2019]. Disponível em WWW: <URL:<https://www.tracto.com.br/quantas-pessoas-tem-acesso-a-internet-no-mundo/>>.

TRANSPARENCY REPORT. **Remoções da pesquisa em cumprimento da legislação europeia sobre privacidade**. [Em linha]. [Consult. 17 Maio 2019]. Disponível em WWW:<URL:https://transparencyreport.google.com/eu-privacy/overview?requests_over_time=country:PT&lu=delisted_urls&delisted_urls=start:1401321600000;end:1558051200000;country>.

UNIÃO EUROPEIA - **Carta dos Direitos Fundamentais da União Europeia**. [Em linha]. [Consult. 01 fev. 2018]. Disponível em WWW: <URL:<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN>>.

UNIÃO EUROPEIA - **Tratado da Constituição Europeia** [Em linha]. Luxemburgo: Europa, 2005. [Consult. 01 fev. 2018]. Disponível em WWW: <URL: https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_establishing_a_constitution_for_europe_pt.pdf>.

UNIÃO EUROPEIA (PARLAMENTO) - **Resolución del Parlamento Europeo de 13 de diciembre de 2016, sobre la situación de los derechos fundamentales en la Unión Europea en 2015**. [Em linha]. [Consult. 01 fev. 2018]. Disponível em WWW: <URL:<http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2016-0485&language=ES&ring=A8-2016-0345>>.

UNIÃO EUROPEIA. **Autoridade Europeia para a Proteção de Dados (AEPD)**. [Em linha]. [Consult. 7 maio 2019]. Disponível em WWW: <URL:https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_pt>.

UNIÃO EUROPEIA. Decisão de Execução da Comissão de 21 de agosto de 2012. **Jornal Oficial da União Europeia**. [Em linha]. [Consult. 11 maio 2019]. Disponível em WWW: <URL:<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32012D0484&from=EN>>.

UNIÃO EUROPEIA. Directiva 2002/58/CE do Parlamento Europeu e do Conselho. **Relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas** 12 de Julho de 2002. [Em linha]. [Consult. 18 mar. 2019]. Disponível em WWW: <URL:<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=EN>>.

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho - **relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. 24 de outubro de 1995. [Em linha]. [Consult. 01 nov. 2018]. Disponível em WWW: <URL:<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>>.

UNIÃO EUROPEIA. Directiva 97/66/CE do Parlamento Europeu e do Conselho - **relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações**. 15 de Dezembro de 1997. [Em linha]. [Consult. 15 nov. 2018]. Disponível em WWW: <URL:<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31997L0066&from=PT>>.

UNIÃO EUROPEIA. Regulamento CE/45/2001 do Parlamento Europeu e Conselho de 18 de dezembro de 2000. Relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados. [Em linha]. [Consult. 18 mar. 2019]. Disponível em WWW: URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32001R0045>>.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE**. [Em linha]. [Consult. 18 mar. 2019]. Disponível em WWW: <URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN>>.

UNITED STATES OF AMERICA. **Privacy Act of 1974, 5 U.S.C. § 552.** [Em linha]. [Consult. 23 out. 2018]. Disponível em WWW: <URL:https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1279>.

VALENTE, Jonas - **França aplica multa máxima ao Google por violação de legislação.** [Em linha]. [Consult. 2 maio 2019]. Disponível em WWW:<URL:http://agenciabrasil.ebc.com.br/internacional/noticia/2019-01/franca-aplica-multa-maxima-ao-google-por-violacao-de-legislacao>.

VARIZ, Maria Afonso Manuel – **Da responsabilidade Civil decorrente de produtos defeituosos.** Coimbra: Coimbra, 1991. ISBN972-32-0466-5.

VASCONCELOS, Pedro Pais – **Direitos da Personalidade.** São Paulo: Almedina, 2006, ISBN: 9789724029948.

VEJA. **Vazamento de dados** [Em linha]. [Consult. 10 abr. 2019]. Disponível em WWW: <URL: https://veja.abril.com.br/noticias-sobre/vazamento-de-dados/>.

VIDIGAL, Leonardo Bruno Marinho - **O Direito ao Esquecimento e a Incipiente Experiência Brasileira: Incompreensões sobre o Tema, limites para sua Aplicação e a Desafiadora Efetivação no Ambiente Virtual.** Rio de Janeiro: Pontifícia Universidade Católica do Rio de Janeiro, 2017. Dissertação de Mestrado.

VIEIRA, Jose Ribas – Trajetórias Teóricas do Direito à Intimidade e à Vida Privada *in*: VIEIRA, Jose Ribas (Coord). **Direitos à Intimidade e à Vida Privada.** Curitiba: Juruá, 2011. ISBN 978-85-362-1999-8.

VIEIRA, Sonia Aguiar do Amaral - **Inviolabilidade da Vida Privada e da Intimidade pelos Meios Eletronicos.** São Paulo: Juarez de Oliveira, 2002. ISBN 85-7453-349-1.

WARREN S D.; BRANDEIS, Louis D. **The Right to Privacy.** Harvard Law Review. Cambrige. ISSN: .4:5 (1890) p. 196. [Em linha]. [Consult. 17 fev. 2018]. Disponível em WWW: <URL:https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>.