Revista Jurídica vol. 04, nº. 49, Curitiba, 2017. pp. 360-392

DOI: 10.6084/m9.figshare.5632153

DADOS PESSOAIS: UMA NOVA *COMMODITY*, LIGADOS AO DIREITO A INTIMIDADE E A DIGNIDADE DA PESSOA HUMANA

PERSONAL DATA: A NEW COMMODITY, LINKED TO THE RIGHT TO THE INTIMIDITY AND DIGNITY OF THE HUMAN PERSON

DAVID AUGUSTO FERNANDES

Pós-doutor em Democracia e Direitos Humanos pela Universidade de Coimbra/Portugal. Doutor e Mestre em Direito. Bacharel em Ciências Jurídicas e Sociais pela Universidade Federal do Rio de Janeiro (1988). Graduado em Engenharia Mecânica pela Fundação Técnico Educacional Souza Marques (1987). Professor Adjunto da Universidade Federal Fluminense, lotado no Departamento de Direito do Instituto de Ciências da Sociedade de Macaé, com exercício docente nas disciplinas de Processo Penal e Criminologia. Cadastrado no CNPQ como líder de pesquisa, sendo que a mesma é direcionada ao Direito Internacional Penal e aos Direitos Humanos. Docente dos Cursos de Especialização em Gestão Pública, Gestão Pública Municipal e Gestão em Saúde Pública, na modalidade de Ensino à Distância, ofertados pela Universidade Federal Fluminense através de Consórcio CEDERJ e da Universidade Aberta do BRASIL (UAB).

RESUMO

O acesso as redes sociais deixam um rastro, que reunidos formam o perfil desse usuário, sendo este utilizado como *commodity* por empresas que objetivam vender os seus produtos ou serviços. O presente artigo aborda uma situação reinante em nossa sociedade: a violação do nosso direito a intimidade, onde somos assediados, nas redes sociais, por propagandas de produtos, que não solicitamos, que possuem o nosso perfil, recebidos, quando acessamos a internet. Fato que afeta a dignidade da pessoa humana. Para atender a este tema foi feita uma pesquisa doutrinaria, assim como nas legislações internacionais e nacionais desenvolvidas, no decorrer dos anos,

DOI: 10.6084/m9.figshare.5632153

para proteger o cidadão, inibindo a violação de nosso direito fundamental de não sermos assediados por propagandas indesejáveis a nós direcionadas.

PALAVRAS-CHAVE: *Commodity*; Direito a intimidade; dignidade da pessoa humana; dados pessoais.

ABSTRACT

Access to social networks leaves a trail, which together form the profile of this user, being used as a commodity by companies that aim to sell their products or services. This article addresses a situation prevailing in our society: the violation of our right to privacy, where we are harassed, on social networks, by advertisements of products that we do not solicit, that have our profile, received, when we access the Internet. A fact that affects the dignity of the human person. To meet this theme, a doctrinal research was done, as well as in the international and national legislations developed, over the years, to protect the citizen, inhibiting the violation of our fundamental right not to be harassed by undesirable advertisements directed to us.

KEYWORDS: Commodity; Right to intimacy; Dignity of Human Person; Personal Data.

INTRODUÇÃO

No mundo globalizado em que vivemos o fluxo de informações, via internet, é muito alto, havendo tecnologia de ponta que separa dados de determinado nicho de pessoas, produtos e serviços, sendo estes utilizados para determinada finalidade, por determinada camada, para fim específicos, qual seja: propaganda, oferecimento de produtos, serviços, entre outros.

Atualmente o tratamento dado a estas informações pessoais podem servir de *commodity*, já que é um ativo de grande valor agregado, permitindo ter um acesso mais preciso aos dados pessoais de uma pessoa em particular, pois quando acessa

vol. 04, nº. 49, Curitiba, 2017. pp. 360-392

DOI: 10.6084/m9.figshare.5632153

as redes sociais, deixa seu “rastro”, revelando seus dados, seus interesses nas redes sociais. Tais informações podem ser usadas para vários objetivos, entre eles o lucro.

Pode ser observada, na mídia, a reclamação de pessoas, geralmente idosas, que são assediadas por financeiras, que sabedoras dos dados pessoais dos aposentados oferecem empréstimos, sendo que quando destes contatos informam ter conhecimento da vida financeira do aposentado, ou simplesmente o oferecimento de um determinado cartão de crédito, onde o interlocutor dando a entender que sabe de sua atividade profissional ou financeira, sem que o “beneficiário do oferecimento do cartão” tenha mantido em algum momento contato anterior com a pessoa que o procura, sendo tal procedimento uma flagrante violação ao sigilo de seus dados pessoais.

Outro dado que pode ser observado pelo “ internauta” é que são direcionados a ele propagandas de determinados produtos ou serviços, isto através de um tratamento dado pela Google Inc., ou outra empresa do gênero ao perfil do usuário na rede, violando seu direito a intimidade e ao desejo de receber informações que não pediu.

Tal rotina em nosso cotidiano conduziu a elaboração do presente artigo, onde utilizando-se de pesquisa doutrinaria e aos ordenamentos jurídicos internos e externos procuramos materializar o desenvolvimento da consciência internacional para preservação do direito a intimidade dos dados pessoais de cada indivíduo, sendo tal direito levado ao nível de preceito fundamental, já reconhecido na sociedade internacional.

No primeiro tópico é apresentada a proteção de dados pessoais, sendo que este, desde a metade do século passado tem assegurado a condição de direitos fundamentais, alicerçado na própria Declaração Universal dos Direitos Humanos e em outros ordenamentos que o sucederam, permitindo a sedimentação do direito a intimidade na comunidade internacional.

Seguindo, abordamos a proteção de dados de caráter pessoal, onde foram apresentados vários dispositivos legais que dão lastro a este preceito fundamental. Promovendo a criação de regras de garantias para o cidadão e a princípios reguladores para a garantia da proteção desses dados de caráter pessoal para que não seja infringido o direito a intimidade de cada pessoa.

DOI: 10.6084/m9.figshare.5632153

Prosseguindo, ancorado nos ordenamentos jurídicos existentes na sociedade internacional temos a definição de dados pessoais e quem são seus titulares, havendo, inclusive, em nosso País um Projeto de Lei tratando do tema em estudo.

O tratamento de dados é outro ponto que foi considerado no presente trabalho para melhor desenvolvimento do tema em estudo, sendo que para tal serviram de base as legislações internacionais e seu desenvolvimento no decorrer das décadas no século findo.

No tópico seguinte foi abordado o direito ao esquecimento, pois o mesmo é um derivativo do direito a intimidade e merecedor de preocupação na atualidade.

Ato continuo são focados o direito dos titulares dos dados e os deveres dos responsáveis pelos tratamentos de dados, pontos nodais para materialização desse direito fundamental, assim como a formatação de regramentos para sua sustentação.

A proteção de dados no ordenamento brasileiro se apresenta de forma singela, mas com o advento do Projeto de Lei, em tramitação no Congresso nacional, existe a possibilidade de uma aproximação da legislação nacional com o ordenamento externo já sedimentado.

Passando, em última *ratio,* as considerações finais.

2 PROTEÇÃO DE DADOS PESSOAIS

2.1 DIREITOS FUNDAMENTAIS

O direito à informação é preceito fundamental, já sedimentado na sociedade internacional, sendo que foi sacramentado no artigo XIX, da Declaração Universal dos Direitos Humanos (DUDH): “Toda pessoa tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras”.

Este direito à informação é um preceito delineador que representa a importância do alcance da liberdade contemporânea ao acesso a informação, que se apresenta em grande volume, facilitado pelo processamento automatizado de dados,

DOI: 10.6084/m9.figshare.5632153

que com os computadores transformou a informação dispersa em informação organizada, organizada em bancos de dados, que contêm dados pessoais, proporcionando uma nova definição dos poderes e direitos sobre as informações pessoais e, por via de consequência sobre a própria pessoa (WIENER, 2010, p.20).

Levando a haver, com o passar dos anos, uma preocupação com a manipulação dos dados pessoais e sua afetação ao direito fundamental de proteção dos dados de caráter pessoal. Conduzindo a criação de legislações, em diversos Estados, para proteção dos dados pessoais[1].

Observa-se em alguns países, que a tutela autônoma dos dados pessoais foi um primeiro passo rumo à sua consideração como um direito fundamental. Este posicionamento surge em países cujo ordenamento reflete o sistema jurídico europeu continental. Aliado a isto temos os países que sofreram uma mudança de regime político, sendo exemplo a Espanha[2] e Portugal[3], que lhes proporcionou reescrever

[1] Listamos aqui os países que possuem codificação de Proteção de Dados Pessoais, sendo que somente os países marcados com asterisco não possuem Entidade Supervisora de Dados, os demais possuem: Albânia, Argentina, Austrália, Áustria, Azerbaijão*, Alemanha, Bélgica, Bósnia, Bulgária, Canadá, Chile, Chipre, Coréia do Sul, Croácia, Dinamarca, Eslováquia, Eslovênia, Espanha, Estônia, Finlândia, França, Grécia, Hong Kong, Holanda, Hungria, Irlanda, Islândia, Israel, Itália, Japão, Letônia, Liechtenstein, Lituânia, Luxemburgo, Malta, Mônaco, Nova Zelândia, Holanda, Noruega, Polônia, Portugal, Romênia, San Marino, Sérvia*, Tailândia, Taiwan* e Ucrânia*.

[2] A Constituição espanhola de 1978 contém os seguintes dispositivos:
Art. 18. – (...) 4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos (...);
Art. 105. – (...) b) La Ley regulará el acceso de los ciudadanos a los archivios y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas".

[3] A constituição portuguesa de 1976 dispõe sobre a utilização da informática nos sete incisos de seu artigo 35:
"Artigo 35.º (Utilização da informática) 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.
2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.
3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.
4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos.
6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.
7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei".

DOI: 10.6084/m9.figshare.5632153

suas cartas fundamentais, sendo estes países onde foi possível observar uma tendência à consideração da problemática relacionada à informática e à informação pessoal em nível constitucional, sendo que no caso da Constituição portuguesa, há uma referência explícita à proteção de dados pessoais (DONEDA, 2010, p. 39).

Temos na Convenção 108, do Conselho da Europa, de 28 de janeiro de 1981, uma abordagem dos direitos fundamentais, onde em seu preâmbulo, testifica que a proteção de dados pessoais está diretamente ligada à proteção dos direitos humanos e das liberdades fundamentais, entendendo-a como pressuposto do estado democrático e trazendo para este campo a disciplina, evidenciando sua alusão ao artigo 8º da Convenção Europeia para os Direitos do Homem[4].

Compartilhando a mesma visão, verifica-se na Carta dos Direitos Fundamentais da União Europeia, de 7 de dezembro de 2000, em cujo artigo 8º, que trata da "proteção de dados pessoais", inspirou-se no artigo 8º da Convenção de Strasbourg, na Diretiva 95/46/CE e no artigo 286 do tratado instituidor da União Europeia [5], consolidando a técnica que já era legitimada pelo legislador e pela doutrina de vários países europeus de considerar a tutela dos dados pessoais como um direito autônomo em relação à tutela da privacidade (DONEDA, 2010, p. 49).

2.2 A PROTEÇÃO DE DADOS DE CARÁTER PESSOAL

O caminho trilhado para o tratamento autônomo da proteção de dados pessoais tem seu marco inicial há aproximadamente quatro décadas quando foram editadas leis objetivando regular um cenário no qual centros de processamento de dados, de grande porte, concentrariam a coleta e gestão dos dados pessoais. Estando

[4] Seu artigo 1º, que trata do "objetivo da diretiva", afirma que "Os Estados-membros assegurarão, em conformidade com a presente diretiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais".

[5] "Artigo 286. 1. A partir de 1 de janeiro de 1999, os actos comunitários relativos à protecção das pessoas singulares em matéria de tratamento de dados de carácter pessoal e de livre circulação desses dados serão aplicáveis às instituições e órgãos instituídos pelo presente Tratado, ou com base nele.
2. Antes da data prevista no nº 1, o Conselho, deliberando nos termos do artigo 251, criará um órgão independente de supervisão, incumbido de fiscalizar a aplicação dos citados "actos comunitários às instituições e órgãos da Comunidade e adaptará as demais disposições que se afigurem adequadas".

DOI: 10.6084/m9.figshare.5632153

o núcleo destas leis, na concessão de autorizações para a criação destes bancos de dados e do seu controle por órgãos públicos materializados posteriormente.

Estas leis abordavam, também, o controle do uso de informações pessoais pelo Estado e pelas suas estruturas administrativas, que eram o destinatário principal destas normas. O desconhecimento, à época, sobre a matéria levou a que se optasse por princípios de proteção, amplos e abstratos, direcionados basicamente na atividade de processamento de dados (DONEDA, 2010, p. 41)[6].

No final da década de 1970, com a ocorrência da disseminação dos bancos de dados informatizados, temos na França, a Lei nº 78-17, de 6 de janeiro de 1978, versando sobre a proteção de dados pessoais, denominada *Informatique et Libertées*[7], cuja característica básica era estar ancorada na consideração da privacidade e na proteção dos dados pessoais como uma liberdade negativa, a ser exercida pelo próprio cidadão, diversa das leis anteriores que estavam fixadas no fenômeno computacional em si (DONEDA, 2010, p. 42).

Não tardando para ocorrer uma mudança de foco: percebeu-se que o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para a sua efetiva participação na vida social e, o que era exceção, tornou-se regra. Tanto o Estado como os entes privados utilizavam intensamente o fluxo de informações pessoais para seu funcionamento, e a interrupção ou mesmo o questionamento deste fluxo pelo cidadão implica muito frequentemente na sua exclusão de algum aspecto da vida social.

Já na década de 1980 as leis passaram a sofisticar a tutela dos dados pessoais, continuando centrada no cidadão, contudo, passou a abranger mais que a liberdade de fornecer ou não os próprios dados pessoais, focando também em garantir

[6] Este enfoque era natural, visto que a motivação destas leis ter sido a "ameaça" representada pela tecnologia e, especificamente, pelos computadores. A estrutura e a gramática destas leis eram algo tecnocrática e condicionada pela informática – nelas, tratavam-se dos "bancos de dados", e não propriamente da "privacidade", desde seus princípios genéricos até os regimes de autorização e de modalidades de tratamento de dados, a serem determinados *ex ante*, sem prever a participação do cidadão neste processo. Estas leis de proteção de dados não demoraram muito a se tornarem ultrapassadas, diante da multiplicação dos centros de processamento de dados, que inviabilizou o controle baseado em um regime de autorizações.

[7] É do mesmo período a lei austríaca [Datenschutzgesetz (DSG), Lei nº 565/1978, de 18 de outubro de 1978]; aliado a este fato deve ser lembrado que a constituição portuguesa e a espanhola apontam neste sentido, mesmo que as leis de proteção de dados destes países tenham surgido somente um pouco mais tarde.

DOI: 10.6084/m9.figshare.5632153

a efetividade desta liberdade. Nestas leis a proteção de dados é vista, como um processo mais complexo, que envolve a própria participação do indivíduo na sociedade e leva em consideração o contexto no qual lhe for solicitado que revele seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada por eventuais condicionantes, conduzindo ao efetivo exercício da autodeterminação informativa[8].

Utilizando como paradigma a Carta de Direitos Fundamentais da União Europeia (CDFUE), onde expressamente, apresenta em seu artigo 8º, a afirmação de que "as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito" (EUROPARL, 2000)[9], sendo que tal procedimento é um afluxo dos direitos fundamentais, tentando inibir a exposição de cada pessoa no ambiente social em que reside[10].

As normas europeias que visam a proteção de dados surgiram como resposta à necessidade de fazer circular informações pessoais, consequência do funcionamento do mercado interno e do aumento do fluxo transfronteiriço de dados que acompanha a circulação de mercadorias, de pessoas, de serviços e de capitais. Devendo o fluxo de dados pessoais realizar-se no respeito dos direitos fundamentais, só um nível de proteção equivalente em todos os Estados-Membros, garantindo por uma legislação harmonizada, asseguraria a livre circulação de dados no mercado interno (DONEDA, 2010, p. 49; MACARIO, 1997, p.9)[11].

---

[8] A autodeterminação informativa surgiu basicamente como uma extensão das liberdades presentes nas leis de segunda geração, e são várias as mudanças específicas neste sentido que podem ser identificadas na estrutura destas novas leis.

[9] Artigo 8º - Proteção de dados pessoais
1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente

[10] Interessante observar que em 1950 tinha-se na Convenção Europeia dos Direitos do Homem (CEDH), de 4 de novembro de 1950, testificado no artigo 8º, o direito ao respeito pela vida privada e familiar, onde afirma: "Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pela sua correspondência".

[11] Também, nota-se uma dupla nuança: se a Diretiva, por um lado, procura proteger a pessoa física em relação ao tratamento de seus dados pessoais, por outro se destaca sua missão de induzir o comércio através do estabelecimento de regras comuns para proteção de dados na região, o que não surpreende se considerarmos as exigências de um mercado unificado como o europeu em diminuir de forma ampla os custos de transações, o que inclui harmonizar as regras relativas a dados pessoais.
Conforme Macario este caráter levou alguns autores a desencorajarem a leitura da diretiva em chave de direitos fundamentais do homem em relação à informação pessoal, apesar de reconhecerem que,

DOI: 10.6084/m9.figshare.5632153

A Diretiva 95/46/CE**,** do Parlamento Europeu e do Conselho da Europa, de 24 de outubro de 1995, veio a responder a esta necessidade, ao obrigar os Estados à adoção de legislação oferecendo garantias semelhantes em todo o espaço europeu, e ao regrar os procedimentos quanto aos fluxos de dados pessoais para países que não os da União Europeia, tendo este passado a ser classificado de modo diferenciado, consoante ofereçam, ou não, um nível de proteção adequado (SARMENTO E CASTRO, 2013, p. 121)[12].

O artigo 8º, da CDFUE, é um reconhecimento da autonomia da salvaguarda dos dados de caráter pessoal objeto de tratamento automatizado, face à preocupação genericamente concedida pelo direito previsto no artigo 7º, da mesma Carta, acerca do respeito à vida privada.

Esta autonomia já fora reconhecida por alguns textos constitucionais dos Estados-Membros, entre eles podemos citar a Constituição Portuguesa, que desde 1976 consagra como direito fundamental à proteção dos dados pessoais, na época dados pessoais mecanizados (SARMENTO E CASTRO, 2013, p. 121).

"*dal punto di vista più genuinamente privatistico, non v'è dubbio che la direttiva ... sia destinata a diventare un punto di riferimento fondamentale nella ricostruzione sistematica dei diritti della personalità, almeno nella misura in cui il concetto di personalità si trovi a far i conti con la realtà informatica e telematica".*

[12] Esta Diretiva estabelece diretrizes para uniformização do tratamento de Proteção de Dados pessoais pelos Estados-membros. Esse documento estabelece, em essência, que os sistemas de processamento de dados pessoais são criados para servir ao homem e devem respeitar seus direitos individuais e sua liberdade.
Esse processamento deve ser legal e justo aos indivíduos. Os dados pessoais processados devem ser adequados, relevantes e não excessivos para os propósitos a que se destinam, os quis devem ser explícitos e legítimos, e determinados ao tempo da coleta das informações.
Para que o processamento de dados seja legal, deve, ainda mais, ser feito com o consentimento do indivíduo ou ser necessário para algumas atividades especificadas, como para o desempenho de uma tarefa de interesse público.
Para que seja considerado justo o processamento, o indivíduo deve estar em posição de saber de sua existência e de ter acesso completo e preciso aos seus dados pessoais.
Deve haver, nas legislações dos Estados-membros, exceções que equilibrem a oposição entre os direitos fundamentais dos indivíduos e a legitimidade do processamento de dados pessoais.
A Diretiva excepciona de sua incidência os processamentos de dados relativos a segurança do Estado e a vigilância de vídeo para o propósito de segurança pública, defesa, segurança nacional e atividades ligadas a persecução criminal.
O processamento de dados pessoais, no âmbito da União Europeia, deve ser feito de acordo com a legislação do respectivo Estado-membro, na qual devem ser especificadas as condições em que o processamento de dados é legal. Deve haver, ainda, previsão das obrigações das entidades controladoras de dados e dos direitos dos indivíduos, de acordo com os princípios do processamento de dados pessoais.

DOI: 10.6084/m9.figshare.5632153

Apesar da existência de vários ordenamentos jurídicos editados em vários Estados (MORGADO, 2017)[13], versando sobre o tema em comento, é possível reagrupar seus objetivos e linhas de atuação principais em torno de alguns princípios comuns perceptíveis em vários desses ordenamentos.

O núcleo básico dos princípios de proteção de dados que até hoje são utilizados tem as suas origens em uma série de discussões que, na segunda metade da década de 1960, acompanhou a tentativa do estabelecimento do National Data Center nos Estados Unidos (DONEDA, 2010, p. 44)[14].

Continua o autor a esclarecer que no início da década de 1970 a atuação da Secretary for Health, Education and Welfare (HEW), composta por uma comissão de especialistas, divulgado em 1973, um estudo que concluiu pela relação direta entre a privacidade e os tratamentos de dados pessoais, e pela necessidade de estabelecer a regra do controle sobre as próprias informações:

> A privacidade pessoal de um indivíduo é afetada diretamente pelo tipo de divulgação e utilização que é feita das informações registradas a seu respeito. Um tal registro, contendo informações sobre um indivíduo identificável deve, portanto, ser administrado com procedimentos que permitam a este indivíduo

[13] Na Alemanha, existe o Ato Federal de Proteção de Dados (Bundesdatenschutzgesetz – BDSG), o qual, para implementar a Diretiva nº 95/45/EC, estabelece, dentre várias outras disposições específicas, ser seu propósito proteger o indivíduo contra desrespeito a sua privacidade na utilização de seus dados pessoais. Suas disposições devem-se aplicar a entidades públicas e privadas; no Reino Unido, existe o Ato de Proteção de Dados de 1998, do Parlamento (Act 1998, de 16 de julho de 1998), que estabelece os seguintes princípios para o processamento de dados pessoais: o processamento deve justo e legal; os dados pessoais devem ser obtidos para um ou mais propósitos especificados e legais e não devem ser processados de maneira incompatível com esses propósitos; os dados pessoais devem ser adequados, relevantes e não excessivos em relação aos propósitos para os quais eles são processados; devem ser precisos e mantidos atualizados; não devem ser guardados por tempo maior que o necessário; devem ser processados de acordo os direitos pessoais dos indivíduos; devem ser adotadas medidas técnicas e organizacionais para impedir acesso não autorizado, processamento ilegal, perda acidental, destruição ou dano aos dados; e os dados pessoais não devem ser transferidos para fora da Área Econômica Europeia, a não ser sob garantia de adequado nível de proteção aos direitos e liberdades dos indivíduos detentores. Como resultado da aplicação desta lei no Reino Unido, entre 2007/2008, foram detectadas as seguintes irregularidades e as respectivas providências tomadas: a) A empresa *Infofind Ltd*, que atua no ramo de investigação privada, foi condenada por obtenção e venda ilegal de informações pessoais; b) Considerou-se que a empresa *Orange and Littlewoods Home Shopping* violou a legislação Act 1998, o que gerou uma investigação em seu processamento de informações de clientes; c) o *Northern Ireland Office* violou o Act 1998 depois que ele se recusou a fornecer dados pessoais de um cidadão; d) O *Foreign and Commonwealth Office* violou o Ato de Proteção de Dados, o que gerou uma investigação no sistema de requisição online de vistos do Reino Unid. Grifos deste trabalho.

[14] O National Data Center foi projetado para reunir as informações sobre os cidadãos norte-americanos disponíveis em diversos órgãos da administração federal em um único banco de dados – a partir de um projeto original, que pretendia unificar os cadastros do Censo, dos registros trabalhistas, do fisco e da previdência social, mas jamais foi concretizado.

DOI: 10.6084/m9.figshare.5632153

> ter o direito de participar na sua decisão sobre qual deve ser o conteúdo deste registro e qual a divulgação e utilização a ser feita das informações pessoais nele contida. Qualquer registro, divulgação e utilização das informações pessoais fora destes procedimentos não devem ser permitidas, por consistirem em uma prática desleal, a não ser que tal registro, utilização ou divulgação sejam autorizados por lei (DONEDA, 2010, p. 205).

Tal concepção conduz a requerer que sejam estabelecidas regras de garantia para o cidadão, que efetivamente vieram descritos como: a) Não deve existir um sistema de armazenamento de informações pessoais cuja existência seja mantida em segredo; b) deve existir um meio para um indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de qual forma ela é utilizada; c) deve existir um meio para um indivíduo evitar que a informação a seu respeito colhida para um determinado fim seja utilizada ou disponibilizada para outros propósitos sem o seu conhecimento; d) deve existir um meio para um indivíduo corrigir ou retificar um registro de informações a seu respeito; e) toda organização que estruture, mantenha, utilize ou divulgue registros com dados pessoais deve garantir a confiabilidade destes dados para os fins pretendidos e deve tomar as devidas precauções para evitar o mau uso destes dados (DONEDA, 2010, p. 205).

Estas regras apresentaram um conjunto de medidas que passou a ser encontrado em várias das normas de proteção de dados pessoais, às quais se passou a referir como Fair Information Principles (FIP).

Os FIP passaram a constituir um núcleo comum existente nas diversas normas sobre a proteção de dados, seja na Europa como nas Américas. Sua influência foi marcante, como pode ser observado em documentos normativos mais influentes sobre a matéria, da década de 1980, como a Convenção 108, do Conselho da Europa, de 28 de janeiro de 1981 e nas Diretrizes da Organização de Cooperação e de Desenvolvimento Econômico (OCDE), de 23 de setembro de 1980. Estes princípios podem ser sintetizados em (DONEDA, 2010, p. 206)[15]:

[15] Há diversas modificações e adaptações destes princípios, quase sempre a partir deste mesmo núcleo comum. Assim, por exemplo, leis como a alemã tratam de um princípio da necessidade, que vincularia o tratamento de dados pessoais quando estes forem estritamente necessários para se atingir um determinado objetivo legítimo, princípio este aparentado com o princípio da proporcionalidade e mesmo com a noção de data minimization, presente na última revisão dos Fair *Information Principles.*
O princípio da necessidade, ou da redução de dados, está presente na seção 3º(a) da Lei Federal de Proteção de Dados da Alemanha (Bundesdatenschutzgesetz) de 2002, na seguinte redação: "*Data processing systems are to be designed and selected in accordance with the aim of collecting, processing*

DOI: 10.6084/m9.figshare.5632153

1 - Princípio da transparência, pelo qual o tratamento de dados pessoais não pode ser realizado sem o conhecimento do titular dos dados, que deve ser informado especificamente sobre todas as informações relevantes concernentes a este tratamento;

2 - Princípio da qualidade ou da exatidão dos dados coletados, pelo qual os dados armazenados devem ser fieis à realidade, atualizados, completos e relevantes, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade;

3 - Princípio da finalidade, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade, fora do qual haveriam abusos;

4 - Princípio do livre acesso, pelo qual o indivíduo deve ter acesso às suas informações armazenadas em um banco de dados, podendo obter cópias destes registros; após este acesso e de acordo com o princípio da qualidade, as informações incorretas poderão ser corrigidas, aquelas registradas indevidamente poderão ser canceladas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos;

5 - Princípio da segurança física e lógica, através do qual os dados devem ser protegidos por meios técnicos e administrativos adequados contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado;

6- Princípio da publicidade dos bancos de dados que tratam as informações pessoais, sobre os quais deve existir um registro público.

---

or using no personal data or as little personal data as possible. In particular, use is to be made of the possibilities for aliasing and rendering persons anonymous, in so far as this is possible and the effort involved is reasonable in relation to the desired level of protection." Também está presente no Art. 3º do Código para a Proteção de Dados Pessoais da Itália, literalmente referido como princípio da necessidade do tratamento de dados e com o seguinte teor: "1. *I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità".*

DOI: 10.6084/m9.figshare.5632153

Como pode ser observado estes princípios nunca estiveram mais atualizados, pois a sociedade de informação carece de normatizações e a todo o momento observamos atos governamentais e/ou privados que são alheios aos princípios extraídos e que causa grande constrangimento entre Estados[16].

Os EUA não possuem uma Diretiva similar a 95/46/EC, do Parlamento Europeu e do Conselho da União Europeia, possuindo uma abordagem setorial, lastreada em várias leis específicas, na regulação da proteção de dados pessoais, denominada Safe Harbor, que certifica as companhias que a ela aderiram a proceder a transferência de dados pessoais, obedecendo as medidas adequadas de proteção de privacidade, com fundamento a garantia de acesso aos dados individuais dos cidadãos, segurança e integridade, entre outras (MORGADO, 2017).

O Japão possui o Ato de Proteção de Informações Pessoais, que tem vigência desde 1º de abril de 2005, que contém, em linhas gerais, como objeto promover a proteção dos direitos e interesses dos indivíduos no processamento de dados pessoais, onde a manipulação de dados pessoais deve ser feita com cautela e em respeito aos direitos individuais. Os órgãos do Estado devem promover medidas de proteção aos dados pessoais e para garantir o adequado atendimento de reclamações de indivíduos relativas a essa matéria[17].

Existe em tramitação no Congresso Nacional o Projeto de Lei nº 5.276/2016, que dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, tendo como fundamento o respeito a privacidade, conforme enunciado em seu artigo 2º, sendo tal dispositivo um avanço para o nosso ordenamento, que carecia de uma norma especifica nesta área de proteção ao

[16] Fato marcante, de alguns anos, foi o Caso Snowden, que em 2013 vazou informações sigilosas do governo americano, conduzindo a uma exposição da política de espionagem dos americanos junto aos governos aliados e inimigos.

[17] As entidades que manipulam dados pessoais devem: estabelecer o propósito para o uso dos dados; colher, com exceções, o prévio consentimento do indivíduo para o uso de seus dados pessoais; abster-se de, no processamento de dados, ir além do escopo do propósito estabelecido para a manipulação; abster-se de adquirir informação por meio fraudulento ou desonesto; manter os dados pessoais de forma precisa e atualizada; implementar medidas de segurança de dados; responder adequadamente a reclamações no uso de dados pessoais. Há previsões para garantir o acesso, correção, acréscimo e eliminação de dados pessoais dos indivíduos. São estabelecidas sanções penais em caso de desrespeito às disposições do Ato.

DOI: 10.6084/m9.figshare.5632153

indivíduo dos avanços tecnológicos, que estão no nosso cotidiano e, devem fornecer proteção ao cidadão comum dessa invasão tecnológico que sofremos quando do acesso as redes sociais.

2.3 A NOÇÃO DE DADOS PESSOAIS E SEUS TITULARES

A Diretiva 95/46/CE, do Parlamento Europeu e do Conselho da União Europeia**,** de 24 de outubro de 1995[18], foi influenciada pela Convenção 108, de 28 de janeiro de 1981, do Conselho da Europa, para a Proteção das Pessoas Físicas, no que diz respeito ao Tratamento Automatizado de Dados Pessoais, sendo que esta Convenção foi o primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados. Objetiva

> [...] garantir a todas as pessoas físicas [...] o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada[19], face ao tratamento automatizado dos dados de caráter pessoal.

Tal dispositivo, em seu artigo 2º, promove a definição de dados pessoais, como sendo:

[18] Interessante observar que em Portugal existe a Lei nº 67, de 26 de outubro de 1998, sendo esta a versão internalizada da Diretiva 95/46/CE.
Esta Lei veio a fornecer uma noção de dados pessoais, entendendo não ser só o nome das pessoas, considerando qualquer informação, de qualquer natureza e independentemente do suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável.
Esta pessoa será o titular dos dados pessoais (art. 3º, alínea "a", da Lei nº 67, de 26 de outubro de 1998), constituindo dados pessoais, toda a informação, seja ela numérica, alfabética, gráfica, fotográfica, acústica ou de qualquer outro tipo, relativa a uma pessoa física identificada ou identificável. Nos termos da Lei de Proteção de Dados considera-se "identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou a mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social".
Parece entender-se que são identificáveis, não apenas aqueles que o próprio titular possa, pelos seus próprios meios identificar, mas que possa ainda identificar com recurso a meios que disponha um terceiro. Podendo ser citado neste rol os dados tratados através da comunicação por Internet, assim como os dados do endereço do IP do utilizador.

[19] Neste ponto, vida privada, podemos considerar como violação desse direito ao recebimento de SMS, SPAM, etc., que contenham propaganda de suas organizações, objetivando captar clientes, sem que estes tenham manifestado o desejo de recebê-los. Tal procedimento é corriqueiro em nossa atualidade, onde o tratamento dado as informações pessoais servem de commodity, permitindo que pessoas de perfis específicos sejam atingidos em seus interesses.

DOI: 10.6084/m9.figshare.5632153

> Qualquer informação relativa a uma pessoa singular identificada ou identificável ("pessoa em causa"); uma pessoa identificável é aquela que pode ser identificada, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais fatores específicos da sua identidade física, fisiológica, mental, econômica, cultural ou social (EUROPARL, 2017; SARMENTO E CASTRO, 2013, p. 122)[20].

Já o Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho da União Europeia, de 27 de abril de 2016, expressa, em seu artigo 4º, por

> Dados pessoais a "informação relativa a uma pessoa singular identificada ou identificável ("titular dos dados")"; é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular (EUROPA, 2016)[21].

No Brasil o Projeto de Lei nº 5.276/2016, tramitando no Congresso Nacional, define em seu artigo 5º, inciso I dado pessoal e no inciso VI, quem seja o titular desses dados:

> I - Dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa; [...] VI - titular: a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

O Projeto de Lei define dado pessoal de forma simplificada e no singular, como ainda está em tramitação, poderá haver uma modificação para que esta definição seja mais abrangente para atender aos anseios da sociedade.

[20] Assim a título meramente exemplificativo, são dados pessoais, além do nome ou do local da residência, outros dados de identificação como: número de identidade civil, número do passaporte, número da seguridade social, número do CPF, ou de cliente de um estabelecimento comercial, estabelecimento bancário, assim como número de telefone, o e-mail, o IP do computador, a placa do veículo, o som da voz da pessoa registrada para permitir o acesso a uma conta bancária, as classificações escolares e *curriculum vitae*, o histórico clínico, as dívidas e créditos, as compras que alguém efetua, o registro dos meios de pagamento que utiliza desde que estejam associados a uma pessoa, permitindo sua identificação. É também o caso de uma impressão digital, de uma imagem biométrica do rosto, de uma imagem recolhida através do uso de uma câmera, como nos casos das câmeras de vigilância, ou fotos divulgadas na internet.

[21] O Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho da União Europeia, de 27 de abril de 2016 revogou a Diretiva 95/46/CE (Regulamento Geral sobre Proteção de Dados).

DOI: 10.6084/m9.figshare.5632153

2.4 TRATAMENTO DE DADOS

O Regulamento 2016/679, entende, em seu artigo 4(2), por tratamento de dados:

> Uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição (EUROPA, 2016).

Os dados pessoais são objeto de proteção quando sujeitos a qualquer operação ou conjunto de operações, ou seja, tratamento, efetuadas com ou sem meios automatizados (art. 15).

São exemplos de tratamento de dados, o recolhimento de dados, o seu registro, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, destruição ou apagar esses dados realizados por órgãos do Estado, como por empresas de cartão de crédito ou que atuam direta ou indiretamente no comércio, entre outros (EUROPA, 2003)[22].

No nosso ordenamento o Projeto de Lei nº 5.276/2016, define em seu artigo 5º, inciso II o que configura tratamento:

[22] O Tribunal de Justiça da União Europeia já teve ocasião de afirmar que a operação feita numa página da internet, a várias pessoas e a sua identificação pelo nome ou por outros meios, por exemplo, o número de telefone ou informações relativas às condições de trabalho e aos seus passatempos, constitui um "tratamento de dados pessoais por meios total ou parcialmente automatizados" na acepção do artigo 3(1), da Diretiva 95/46/CE (Acórdão Lindqvist, de 6 de novembro de 2003, Proc. C-101/01).

EMENTA: Acórdão do Tribunal de 6 de novembro de 2003.

Processo-crime contra Bodil Lindqvist. Pedido de decisão prejudicial: Göta hovrätt - Suécia. Directiva 95/46/CE - Âmbito de aplicação - Publicação de dados de carácter pessoal na Internet - Local da publicação - Conceito de transferência de dados de carácter pessoal para países terceiros - Liberdade de expressão - Compatibilidade com a Directiva 95/46 de uma maior protecção de dados de carácter pessoal pela legislação nacional de um Estado-Membro.

DOI: 10.6084/m9.figshare.5632153

> Art. 5º - Para os fins desta Lei, considera-se: [...] II- tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Observa-se neste Projeto de Lei, em seu artigo 7º, estão os requisitos para o tratamento de dados pessoais que somente poderão ser realizados nas seguintes hipóteses:

> Art.7º: I - Mediante o fornecimento pelo titular de consentimento livre, informado e inequívoco; II - para o cumprimento de uma obrigação legal pelo responsável; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos; IV - para a realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de um contrato ou de procedimentos preliminares relacionados a uni contrato do qual é parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial ou administrativo; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; IX - quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for menor de idade.

Já a Diretiva 95/46/CE excluía do seu âmbito de proteção os tratamentos de dados pessoais realizados por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas, exemplificando com a correspondência ou as listas de endereços.

A Lei nº 67, de 26 de outubro de 1998, de Portugal, estipulou a regra que as entidades que procedam a tratamento de dados pessoais são obrigadas a notificar esse tratamento à Comissão Nacional de Proteção de Dados (CNPD), conforme preceituado no art. 27(1)[23], antes da realização do mesmo. Obrigação que deve ser cumprida pelo responsável pelo tratamento de dados, determinando as finalidades e os meios de tratamento. Esta obrigação traduz-se no envio de um formulário

[23] O artigo correspondente a este na Diretiva 95/46/CE é o 28(1).

DOI: 10.6084/m9.figshare.5632153

disponibilizado pela Comissão e que lhe permite controlar os tratamentos e as condições em que estes se realizam.

Na legislação portuguesa existe uma controvérsia entre a Lei nº 67/1998 e a Lei de Acesso aos Documentos Administrativos (LADA) (DRE, 2016)[24], onde os dados "nome" e "morada", têm levantado questões especiais quanto o dever considerar-se ou não dados pessoais. Existindo uma falta de entendimento conceitual entre estes dois tipos regulamentares, já que a LADA, contrariamente à Lei de Proteção de Dados, não considera "nome" e "morada" como dados pessoais.

Esta discrepância acontece porque estas legislações pretendem proteger bem jurídicos diferentes, estabelecendo uma noção não coincidente. A Lei de Proteção de Dados de acordo com a Diretiva 95/46/CE, identificam nome e residência como dados pessoais, porque permitem identificar pessoas, contudo para a LADA estas informações não o são. Esta lei estabelece como dados pessoais "as informações sobre pessoa singular identificada ou identificável, que contenham apreciações, juízos de valor ou que sejam abrangidas pela reserva da intimidade da vida privada".

Esta diferença de concepção tem sido fonte de conflito entre o direito de acesso aos documentos administrativos dos cidadãos em geral, garantidos pelo art. 268º, nº 2, da Constituição da República Portuguesa (CRP), que protege o direito à informação procedimental e na LADA, e os direitos fundamentais à autodeterminação informática (art. 35º da CRP) e à reserva da intimidade da vida privada (art. 26º da CRP), também protegidos pela Lei de Proteção de Dados Pessoais, que proíbe o acesso de terceiros aos dados pessoais e impõe que estes dados não sejam utilizados para finalidades estranhas à determinante na recolha e/ou posterior tratamento.

Os titulares de dados pessoais gozam de um amplo direito de informação. A informação a prestar começa por ser aquela que é necessária à satisfação do direito à curiosidade, isto é, do direito que o titular tem de saber se os seus dados pessoais são tratados por um responsável, bem como de conhecer a identificação deste ou do seu representante. O exercício deste direito não necessita de ser justificado (SARMENTO E CASTRO, 2013, p. 124).

[24] Lei de Acesso aos Documentos Administrativos (LADA) - Lei nº 46, de 24 de agosto de 2007, que foi revogada pela Lei nº 26, de 22 de agosto de 2016.

DOI: 10.6084/m9.figshare.5632153

Aliado ao direito de saber se os dados são tratados, caso ocorram, o seu titular também deve saber quais as categorias de dados que é objeto de tratamento, para que finalidade ou finalidades este se realiza, se existe comunicação de dados a outras entidades e para que fins, e a que entidades, ou categorias, são os dados transmitidos. Este conjunto de direito formaliza o direito de informação do titular de dados, que a Diretiva específica.

O exercício do direito de informação como o direito de acesso é exercido diretamente, junto ao responsável pelo tratamento de dados pessoais, salvo nos casos especialmente previstos em lei. Havendo, exceção, no acesso a dados contidos em arquivos policiais, que só podem ser exercidos, através da autoridade judiciária.

1.4.1 Tratamento de dados para fins comerciais

O processo de coleta de informações pessoais, se não é algo novo em si, desenvolveu-se bastante com a sofisticação das estruturas administrativas estatais e privadas. Com o advento do computador e da possibilidade de digitalizar informações, ela se torna mais útil e também praticamente onipresente. Juntamente com a circulação destas informações, estes seriam os requisitos para a construção da *datasphere* – um conjunto de informações que compreenderia dados sobre nós e nossas ações:

> Uma vez que os eventos do nosso cotidiano são sistematicamente armazenados em um formato legível por uma máquina, esta informação ganha uma vida toda própria. Ela ganha novas utilidades. Ela se torna indispensável em operações comerciais. E ela usualmente é transmitida de um computador a outro, de um negócio a outro, entre os setores públicos e privados (WIERNER, 2010, p. 31).

A mudança qualitativa no tratamento de dados pessoais baseia-se na utilização de novos métodos, algoritmos e técnicas. Dentre elas está a elaboração de perfis de comportamento de uma pessoa a partir de informações que ela disponibiliza ou que são colhidas. Esta técnica, conhecida como *profiling*, onde os dados pessoais são tratados, com o auxílio de métodos estatísticos e de técnicas de inteligência

DOI: 10.6084/m9.figshare.5632153

artificial, com o fim de formular uma “meta-informação”, que consistiria numa síntese dos hábitos, preferências pessoais e outros registros vários da vida desta pessoa.

Resultando na possibilidade de se obter um quadro das tendências de futuras decisões e comportamentos de uma pessoa ou grupo.

A técnica pode ter várias aplicações desde, por exemplo, o controle de entrada de pessoas em um determinado país pela alfândega, que selecionaria para um exame acurado as pessoas às quais se atribuísse maior possibilidade de realizar atos contra o interesse nacional; bem como uma finalidade privada, como o envio seletivo de mensagens publicitárias de um produto apenas para seus potenciais compradores - possibilitando, portanto, a publicidade comportamental, dentre inumeráveis outras (WIENER, 2010, p. 45).

A partir do momento em que um perfil eletrônico é a única parte da personalidade de uma pessoa visível a alguém, as técnicas de previsão de padrões de comportamento podem levar a uma diminuição de sua esfera de liberdade, visto que entes com os quais ela se relaciona levam em consideração o pressuposto de que ela adotará um comportamento predefinido de acordo com seu determinado perfil aliado a técnicas preditivas de seu comportamento, o que tem como consequência uma efetiva diminuição de sua liberdade de escolha (WIENER, 2010, p. 46)[25].

O fato de este perfil ser algo que se contraponha à própria realidade da pessoa foi percebido no decorrer dos anos por pessoas que atuam no ramo, que verificaram a criação de um nosso correlato digital, um corpo eletrônico, composto de nossos dados.

O sistema ECHELON consiste na busca de correlações, recorrências, formas, tendências e padrões significativos a partir de quantidades muito grandes de dados, com o auxílio de instrumentos estatísticos e matemáticos. Assim, a partir de uma grande quantidade de informação em estado bruto e não classificada podem ser identificadas informações de potencial interesse (WIENER, 2010, p. 48)[26].

[25] Para além do senso comum de que “não se oferece fraldas para pessoas que não possuam filhos”, a utilização de técnicas de *direct marketing* e, de forma geral, o aumento das informações em mãos de fornecedores sobre os consumidores apresenta uma série de implicações que podem efetivamente cercear a liberdade de escolha do consumidor.

[26] ECHELON é uma rede de vigilância global e de espionagem para a coleta e análise de sinais de inteligência (SIGINT), operada inicialmente pelos cinco Estados signatários do Tratado de Segurança UK-USA, conhecido como "Cinco Olhos": Estados Unidos, Canadá, Austrália, Nova Zelândia e Reino

DOI: 10.6084/m9.figshare.5632153

2.5 DIREITO AO ESQUECIMENTO

Conforme abordado por WIENER (2010, p.46), tratando do direito ao esquecimento, desde 1966 já havia manifestações no sentido de que: “com episódios de nosso passado, sendo cada vez mais armazenados em arquivos de computadores, a possibilidade de ‘começar de novo’ está se tornando sempre mais difícil. A noção cristã de redenção é incompreensível para o computador”.

O direito ao esquecimento pode ser compreendido como o direito que uma pessoa possui de não permitir que um fato, ainda que verídico ocorrido em determinado período de sua vida, seja exposto ao público em geral de forma perpétua, causando-lhe sofrimento ou transtornos, mas deve se dar a ela a prerrogativa de escolha se e como serão expostas tais informações, desde simples dados pessoais, até vídeos, fotos, entre outros meios de divulgação de fatos que tenham feito parte de momentos já superados e que não haja um concreto interesse público envolvido (PEREIRA, 2017)[27].

Existindo a necessidade da perenidade das informações, tornando-se o principal objeto do direito ao esquecimento: a compreensão do alcance e limite temporal que as informações sobre um indivíduo possuem, sendo analisado de acordo com as peculiaridades do caso em questão.

O direito ao esquecimento pode ser caracterizado como um derivado do princípio da dignidade da pessoa humana, se configurando como algo real e materialmente concretizável que possibilita aos indivíduos o efetivo controle sobre fatos pretéritos ligados a suas vidas, permitindo que tomem o rumo que desejarem sem que precisem ter seus nomes compulsoriamente associados a atividades, acontecimentos e notícias que não mais fazem parte de seu cotidiano atual.

Unido A possibilidade de se obter informações úteis a partir do *data mining* cresce à medida em que aumenta a quantidade de informação em “estado bruto” disponível. Esta é a consequência do aumento da capacidade de armazenamento de informações em diversos tipos de memória, desde os remotos cartões perfurados, passando pelos DVD-ROM e chegando ao panorama atual da *cloud computing,* facilitando a identificação do perfil do usuário da internet.

[27] É importante assentar que o exercício do direito ao esquecimento não confere a ninguém a liberdade de apagar fatos ou reescrever a própria história, mas assegura a possibilidade de discutir o uso que é feito dos fatos pretéritos, mais especificamente o modo e a finalidade com que são lembrados.

DOI: 10.6084/m9.figshare.5632153

Desse modo, a efetivação do direito ao esquecimento impede, por exemplo, o sofrimento já vivido no passado seja constantemente lembrado, como também possibilita a reconstrução da imagem dos sujeitos de acordo com a vontade deles e não com as fortes marcas estigmatizadas no passado (PEREIRA, 2017; MORAES; KONDER, 2012, p. 292[28]; PÉREZ LUÑO, 2012, p. 102[29]).

Salienta Martinez que dentre esse complexo de direitos e deveres fundamentais, já se associam conceitos relacionados com a potencialidade de lesão a tais direitos que ocorre com a ampliação do uso da Internet, nascendo, a partir desse vetor, o chamado "direito ao esquecimento", explanando que:

[28] O caso Lebach, fato ocorrido no interior da Alemanha, no ano de 1969. Quando, três homens assassinaram brutalmente quatro soldados, ferindo outro gravemente, ocasião em que roubaram armas e munições do deposito guarnecido pelos soldados. Em relação aos três autores do crime, dois foram condenados à prisão perpétua e um deles, cuja conduta foi menos gravosa, foi condenado à seis anos de reclusão.
Quando o terceiro autor estava próximo de ser solto, um canal de televisão decidiu publicar um documentário retratando todo o ocorrido. O réu buscou o Poder Judiciário para impedir a exibição, sob o argumento de que o documentário dificultaria seu processo de ressocialização. O Tribunal Constitucional Federal acolheu o pleito do agente e impediu a transmissão do documentário, optando claramente por proteger o direito do autor de ser esquecido em relação ao crime praticado, conforme descrito em parte da decisão do Tribunal:
1. Uma instituição de Rádio ou Televisão pode se valer, em princípio, em face de cada programa, primeiramente da proteção do Art. 5 I 2 GG. A liberdade de radiodifusão abrange tanto a seleção do conteúdo apresentado como também a decisão sobre o tipo e o modo da apresentação, incluindo a forma escolhida de programa. Só quando a liberdade de radiodifusão colidir com outros bens jurídicos pode importar o interesse perseguido pelo programa concreto, o tipo e o modo de configuração e o efeito atingido ou previsto.
2. As normas dos §§ 22, 23 da Lei da Propriedade Intelectual-Artística (Kunsturhebergesetz) oferecem espaço suficiente para uma ponderação de interesses que leve em consideração a eficácia horizontal (Ausstrahlungswirkung) da liberdade de radiodifusão segundo o Art. 5 I 2 GG, de um lado, e a proteção à personalidade segundo o Art. 2 I c. c. Art. 5 I 2 GG, do outro. Aqui não se pode outorgar a nenhum dos dois valores constitucionais, em princípio, a prevalência [absoluta] sobre o outro. No caso particular, a intensidade da intervenção no âmbito da personalidade deve ser ponderada com o interesse de informação da população.
3. Em face do noticiário atual sobre delitos graves, o interesse de informação da população merece em geral prevalência sobre o direito de personalidade do criminoso. Porém, deve ser observado, além do respeito à mais íntima e intangível área da vida, o 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 documentário. 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).

[29] Outra decisão do gênero foi a prolatada pelo Tribunal Constitucional Espanhol, referente à ação movida por Isabel Pantoja em face da comercialização de um vídeo que reproduzia a agonia de seu marido, o toureiro Paquirri, decisão esta de outubro de 1986. O Tribunal Constitucional anulou decisão anterior na qual o Tribunal Supremo entendia que a morte do toureiro não constituía sua esfera íntima. O Tribunal Constitucional entendeu que as cenas vividas dentro da enfermaria não faziam parte do espetáculo taurino. Sendo assim, demonstra-se que o tema já vinha sendo efetivamente trabalhado na doutrina e na jurisprudência, assumindo relevância nos últimos anos.

DOI: 10.6084/m9.figshare.5632153

> O direito ao esquecimento não é uma descoberta atual, tendo se erigido mundialmente o tema à ordem do dia quando do surgimento e a consolidação da Internet, que, em razão de sua possibilidade ilimitada de armazenamento, permite que questões consolidadas no tempo possam ser debatidas, prejudicando interesses de terceiros (MARTINEZ, 2014, p. 88).

A questão da veracidade e da licitude da informação e dos dados publicados não inibe o reconhecimento do direito ao esquecimento, conforme já foi decidido pela sentença nº 545/2015, proferida pelo Tribunal Supremo da Espanha:

> *El problema no es que el tratamiento de los datos personales sea inveraz, sino que pueda no ser adecuado a la finalidad con la que los datos personales fueron recogidos y tratados inicialmente. El factor tiempo tiene una importancia fundamental en esta cuestión, puesto que el tratamiento de los datos personales debe cumplir con los principios de calidad de datos no solo en el momento en que son recogidos e inicialmente tratados, sino durante todo el tiempo que se produce ese tratamiento. Un tratamiento que inicialmente pudo ser adecuado a la finalidad que lo justificaba puede devenir con el transcurso del tiempo inadecuado para esa finalidad, y el daño que cause em derechos de la personalidad como el honor y la intimidad, desproporcionado en relación al derecho que ampara el tratamiento de datos (SILVA, 2017).*

Induzindo que os dados pessoais somente podem ser tratados durante um determinado período de tempo, podendo exigir o titular dos dados, que decorrido um período de tempo que esses dados sejam apagados. Tal procedimento é conhecido como direito ao esquecimento, também chamado pelos norte-americanos "*right to be let alone*" ou, simplesmente, "direito de ser deixado em paz"[30].

Tomando por base o Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho da União Europeia, de 27 de abril de 2016, para que o direito ao esquecimento seja exercido se faz necessário a ocorrência de um dos seguintes

[30] Cumpre mencionar que diversas são as expressões utilizadas para identificar o direito à Intimidade ou ao esquecimento: na Alemanha, utilizando a doutrina das esferas, adotam-se as expressões *privatsphäre* (esfera privada); *intimsphäre* (esfera íntima), *gehermsphäre* (esfera secreta) e *individualsphäre* (esfera individual); na Espanha define-se como *derecho a la intimidad* e *derecho a la vida privada*; nos Estados Unidos é definida pelo nome de *right of privacy* ou *right to be let alone*; na França, como *droit a la vie privée* ou *droit a l'intimité;* na Itália temos o *diritto allá riservatezza,* que seria *o* direito de impedir a divulgação de aspectos da Intimidade, depois de conhecida por terceiro e *diritto Allá segretezza* ou *al rispetto della vita privata*, que é o direito de impedir que terceiros invadam a Intimidade da vida privada; em Portugal, como *direito a proteção da Intimidade da vida privada e direito a zona de Intimidade da esfera privada*.(Grifos do autos deste trabalho)

DOI: 10.6084/m9.figshare.5632153

motivos: a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; b) o titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6(1), alínea "a", ou do artigo 9(2), alínea "a" e se não existir outro fundamento jurídico para o referido tratamento; c) o titular opõe-se ao tratamento nos termos do artigo 21(1), e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21(2); d) os dados pessoais foram tratados ilicitamente; e) os dados pessoais têm de ser apagado para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; f) os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8(1).

Havendo de ser ressalvado, preliminarmente, que quando o responsável pelo tratamento tiver tornado público os dados pessoais e for obrigado a apagá-los nos termos do nº 1, do artigo 17, do Regulamento (UE) 2016/679, toma as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos.

E também deve ser observado que os nºs 1 e 2 do artigo 17, do Regulamento (UE) 2016/679, não se aplicam na medida em que o tratamento se revele necessário: a) ao exercício da liberdade de expressão e de informação; b) ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento; c) por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9(2), alíneas "h" e "i", bem como do artigo 9(3); d) para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89 (1), na medida em que o direito referido no nº 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento; ou e) para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

DOI: 10.6084/m9.figshare.5632153

No nosso ordenamento jurídico, encontramos na Lei de Execuções Penais, Lei nº 7.210, de 11 de julho de 1984 (artigo 202) e no Estatuto da Criança e do Adolescente, Lei nº 8.069, de 13 de julho de 1990 (artigo 143), onde foram assegurados o direito ao esquecimento, respectivamente, ao criminoso e ao menor infrator com a finalidade de garantir efetividade à ressocialização da pessoa envolvida com a Justiça.

O Superior Tribunal de Justiça, que em março de 2013, organizou a VI Jornada de Direito Civil, resultando, naquela ocasião, a elaboração do Enunciado 531, com a seguinte redação: "A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento".

Observando-se que não é qualquer informação negativa que será eliminada do mundo virtual. É apenas uma garantia contra o que a doutrina tem chamado de 'superinformacionismo', que nada mais é do uma verdadeira massa de informações sobre tudo e sobre todos. O enunciado contribui, e muito, para a discussão do tema, mas ainda há muito espaço para o amadurecimento do assunto, de modo a serem fixados os parâmetros para que seja acolhido o 'esquecimento' de determinado fato, com a decretação judicial da sua eliminação das mídias eletrônicas (TRF4, 2013)[31].

O Projeto de Lei nº 5.276 de 2016, aborda o direito ao esquecimento de forma genérica, esclarecendo que o titular dos dados pessoais tem direito a obter, em relação a seus dados, "anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei" (em seu art. 18, IV). Esclarecendo que o responsável deverá informar aos terceiros a quem os dados tenham sido comunicados sobre a realização de correção, eliminação, anonimização ou bloqueio dos dados, para que repitam idêntico procedimento (18, § 5º).

2.6 DIREITO DOS TITULARES DOS DADOS E DEVERES DOS RESPONSÁVEIS PELOS TRATAMENTOS DE DADOS

[31] Sobre este tema temos a Resp. n. 1.334.097-RJ, Rel. Min. Luís Felipe Salomão, 4.ª T., j. 28/05/2013.

DOI: 10.6084/m9.figshare.5632153

A CDFUE, artigo 8(2), expõe os principais direitos do titular dos dados pessoais objeto de tratamento, quando assegura a ele o direito de acesso e o direito de retificação. Havendo obrigação de respeitar e de garantir o exercício destes direitos por parte do responsável pelo tratamento de dados pessoais.

Existindo, especificamente, na Diretiva 95/46/CE o esclarecimento que a pessoa responsável por um tratamento de dados é 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 de dados pessoais.

Observe-se que o titular tem direito de acesso aos dados objeto de um tratamento de que tenha conhecimento, ou seja, tem o direito à comunicação das informações tratadas, para que possa conhecê-las.

Ressalve-se que ao titular não é apenas garantido o direito de acesso, sendo também assegurado o direito a obter informações acerca da própria realização do tratamento e das suas condições.

Atrelado ao acima citado o Regulamento (UE) 2016/679, no seu artigo 18º, garante ao titular de dados o direito de obter do responsável pelo tratamento a limitação do tratamento, se se aplicar uma das seguintes situações: a) Contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão; b) o tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização; c) o responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial; d) se tiver oposto ao tratamento nos termos do artigo 21(1), deste mesmo Regulamento, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

Ocorrendo a limitação do tratamento de dados, conforme delineado no nº 1, do artigo 18º, os dados pessoais só podem, à exceção da conservação, ser objeto de tratamento com o consentimento do titular, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa

DOI: 10.6084/m9.figshare.5632153

singular ou coletiva, ou por motivos ponderosos de interesse público da União ou de um Estado-Membro[32].

Fica o responsável pelo tratamento comunicar a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais ou limitação do tratamento a que se tenha procedido em conformidade com os artigos 16º, 17º, 17(1) e o 18º, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado. Se o titular dos dados solicitá-lo, o responsável pelo tratamento fornece-lhe informações sobre os referidos destinatários.

Tal posicionamento explicita que o manuseio dos dados pessoais de cada indivíduo, sem sua anuência, se caracteriza como uma violação de seu direito fundamental a intimidade.

Verificamos na Declaração de Santa Cruz de La Sierra, documento elaborado ao final da XIII Cumbre Ibero-Americana de Chefes de Estado e de Governo, firmada pelo governo brasileiro, em 15 de novembro de 2003, que a proteção dos dados pessoais é um direito fundamental das pessoas, conforme expresso em seu item 45, onde lê-se:

> Estamos também conscientes de que a proteção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras ibero-americanas para proteger a privacidade dos cidadãos, contidas na Declaração de Antígua, pela qual se cria a Rede Ibero-Americana de Proteção de Dados, aberta a todos os países da nossa Comunidade*"*. Parece existir no direito brasileiro, de forma generalizada, uma consciência de que seria possível tratar de forma satisfatória dos problemas relacionados às informações pessoais em bancos de dados a partir de uma série de categorizações, geralmente generalistas e algo abstratas: sobre o caráter rigidamente público ou particular de uma espécie de informação; sobre a característica sigilosa ou não de uma determinada comunicação, e assim por diante.

Conforme preceituado no Projeto de Lei nº 5.276 de 2016, temos que: "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais, garantidos os direitos fundamentais de liberdade, intimidade e privacidade" (artigo 17). Estando assegurado, conforme artigo 18, ao titular dos dados pessoais o direito a obter, em relação aos seus dados: I - confirmação da existência de tratamento; II- acesso aos

[32] Observando que o titular que tiver obtido a limitação do tratamento, nos termos do nº 1, é informado pelo responsável pelo tratamento antes de ser anulada a limitação ao referido tratamento.

DOI: 10.6084/m9.figshare.5632153

dados; III- correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade, mediante requisição, de seus dados pessoais a outro fornecedor de serviço ou produto; VI - eliminação, a qualquer momento, de dados pessoais com cujo tratamento o titular tenha consentido; e VII - aplicação das normas de defesa do consumidor, quando for o caso, na tutela da proteção de dados pessoais.

Observa-se que o tratamento de dados pessoais procedido pelas pessoas jurídicas de direito público referenciado no artigo 1º, da Lei nº 12.527, de 18 de novembro de 2011, deverá ser realizado para o atendimento de sua finalidade pública, na persecução de um interesse público, tendo por objetivo a execução de competências legais ou o cumprimento de atribuição legal pelo serviço público.

2.7 PROTEÇÃO DE DADOS NO ORDENAMENTO BRASILEIRO

Mergulhando em nosso ordenamento jurídico, podemos encontrar as garantias relacionadas à intimidade, à vida privada e à ação de *Habeas Data* (art. 5º, LXXII CF/1988)[33], e no âmbito da proteção às informações do consumidor podemos nos socorrer ao contido no Código de Defesa do Consumidor (CDC), em seu artigo 43, que enuncia uma série de direitos e garantias direcionadas ao consumidor, visando garantir suas informações pessoais presentes em bancos de dados e cadastros, todos ligados ao sistema FIP, fatos relacionados à matéria de concessão de crédito, sendo asseverado, por parte da doutrina, que este texto serve de paradigma aos princípios de proteção de dados pessoais no direito brasileiro (DONEDA, 2010, p. 40)[34].

[33] Regulamentado pela Lei nº 9.507, de 12 de novembro de 1997, vide artigo 7º.

[34] Conforme o autor: “As disposições do CDC revelam o estabelecimento de equilíbrio na relação de consumo através da interposição de limites ao uso da informação sobre o consumidor pelo fornecedor (que estaria justificado, de um certo ponto de vista, na efetivação da transação com maior segurança). Assim, por exemplo, o registro de dados negativos sobre um consumidor não poderá ser mantido por um período maior de 5 anos; é prevista a necessidade de comunicação escrita sobre o tratamento da informação ao consumidor em certos casos, assim como o direito de acesso, correção e, implicitamente, o cancelamento justificado”.

DOI: 10.6084/m9.figshare.5632153

O Projeto de Lei nº 5276/2016, que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural, sendo ele uma esperança de uma norma voltada para esta área especifica, onde outros Estados já possuem tal tipo de ordenamento jurídico protetor há vários anos e, que já enfrentam de frente este problema atual, mas que em nosso País ainda está desprovido de leis protetores dos direitos fundamentais do cidadão nesta área especifica.

CONCLUSÃO

Conforme observado, no decorrer deste artigo, o fluxo de informações, no mundo globalizado, possibilitou um maior entrelaçamento entre as pessoas, fato tornado possível a toda pessoa pelo direito à liberdade de opinião e expressão, incluindo esse direito à liberdade, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e sem tolhimento de fronteiras, mas também, delineou a necessidade da proteção dos dados lançados nas redes sociais, material que pode ser utilizado de diversas formas, entre elas aqueles com finalidades ilícitas, onde quase todas visando lucro, violando o direito a intimidade e, por via de consequência, rompendo com os direitos fundamentais, hoje sedimentado em nossa sociedade internacional.

Este preceito fundamental que desenha a importância do alcance da liberdade ao acesso da informação, no mundo atual, que com a internet, favorece o enfeixamento de dados automatizados da forma dispersa para a forma sistematizada, contendo desde dados universais até os dados pessoais, tão caros a cada pessoa, configurando uma nova explicação dos poderes e direitos em face as informações pessoais. Desenvolvendo, com isto, uma preocupação com o controle dos dados pessoais e sua influência na proteção dos dados de caráter pessoal, já que seu uso desordenado afetará ao direito fundamental.

Observe-se que alguns países despertaram, primeiramente, para uma solução dessa fragilidade criada com as redes sociais e, inicialmente procederam a tutela autônoma dos dados pessoais, nivelando-os a um direito fundamental,

DOI: 10.6084/m9.figshare.5632153

erguendo-os, em seguida, a nível constitucional. Tal proceder se inicia na década de 1970 e 1980, do século passado.

Para a proteção de dados de caráter pessoal, alguns Estados, no passar dos anos, promoveram o acompanhamento do desenvolvimento tecnológico, na área da informática, direcionada especificamente as redes sociais, objetivando a criação de legislações que estivessem niveladas com este desenvolvimento, em sua terminologia, posto que com a mudança tecnológica acelerada como vem ocorrendo, desde o século passado, se fez e se faz ainda necessário a mudança do ordenamento jurídico em suas definições e suas determinações para que a lei não perca sua eficácia, acompanhando a tecnologia e suas definições, advindas da primeira, para poder solucionar a violação dos direitos fundamentais, representados aqui na proteção de dados pessoais e o direito a intimidade de cada pessoa, assegurados de há muito tempo e que deve ser preservado.

Tal proceder tem como pano de fundo a percepção de que o fornecimento de dados pessoais, pelos cidadãos, tornou-se um requisito indispensável para que este (cidadão) possa participar na vida social, hoje globalizada, via internet. Mas, também, deve ser considerado se este membro da sociedade deseja ou não fornecer seus próprios dados pessoais, garantindo a ele o exercício desta liberdade, como fator de seu direito fundamental a intimidade.

Para formatação desses direitos existe hoje um núcleo básico dos princípios de proteção de dados, que conduzem a obediência de regras de garantia para o cidadão. Como foi abordado, no corpo deste artigo, estas regras encontram-se em várias normas de proteção de dados pessoais, que passaram a ser denominadas como Fair Information Principles, na sociedade internacional, seja nas Américas como na Europa, assim como no Japão e, de forma tímida, no nosso ordenamento jurídico.

Para o enfeixamento desses direitos se fez necessário a definição de dados pessoais e seus titulares, objetivando um sincronismo que pudesse atingir a todas as situações que corressem.

O tratamento de dados pessoais, também passou pelo crivo dessas normas, para que ocorra a proteção quando sujeitos a qualquer operação ou conjunto de operações, ressalvando casos específicos como no seu âmbito de proteção o

DOI: 10.6084/m9.figshare.5632153

tratamento de dados pessoais realizados por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas.

Ponto relevante, no trato do direito fundamental, aqui em comento, é o direito ao esquecimento, que pode ser caracterizado como um derivado do princípio da dignidade da pessoa humana, assegurado a todos que tenham praticado algum ato, em determinado período de suas vidas. E, que sua exposição posterior ao fato venha a causar sofrimentos ou transtornos, que inibam que esta pessoa possa prosseguir sua vida em paz, sem sofrer o assédio público pelo ato perpetrado no passado, inibindo que seja constantemente lembrado de sua ação. Favorecendo que possa reconstruir sua imagem no ambiente social em que viva, sem que ocorra o "remake" de seus atos, conduzindo a sua reinserção social.

Constata-se que com o passar dos anos e com o adento do avanço tecnológico, que ocorre no mundo, a intimidade das pessoas ficam cada vez mais expostas, necessitando de meios eficazes para sua manutenção, aliado ao respeito que cada um deve nutrir do seu próximo.

As legislações existentes devem manter-se em consonância com a mudança tecnológica, para que não percam sua objetividade, na repressão ao ataque a dignidade da pessoa humana. Sendo que em nosso País, a materialização de um ordenamento de ponta, nesta área, caminha vagarosamente e de forma tímida, levando a temer-se pelo direito a intimidade em nosso Estado. Devendo ser utilizado como paradigma as legislações internacionais que acompanham, em pé de igualdade, o desenvolvimento tecnológico para possibilitar que a dignidade da pessoa humana não fique defasada com esse avanço.

REFERÊNCIAS

DONEDA, Danilo Cesar Maganhoto. Proteção de dados pessoais e relações de Consumo. In: **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Caderno de Investigações Científicas. Organizador: Danilo Cesar Maganhoto Doneda. Brasília: SDE/DPDC, 2010, p. 37-57.

_____. Privacidade e transparência no acesso a informação pública. *In*: **Democracia eletrônica.** MEZZAROBA, Oribes; GALINDO, Fernando. Espanha (Zaragoza): Prenzas Universitarias de Zaragoza, 2010, p. 205.

DOI: 10.6084/m9.figshare.5632153

DRE. Lei nº 26, de 22 de agosto de 2016. **Diário da República nº 160, de 22 de agosto de 2016**. Disponível em:< https://dre.pt/home/-/dre/75177807/details/maximized?p_auth=VLJzFY4y>. Acesso em: 26 mar. 2017.

EUROPA. Disponível em:<http://curia.europa.eu/juris/liste.jsf?language=pt&num=C-101/01>. Acesso em: 25.mar.2017.

_____. **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995**. Disponível em: <eur-lex.europa.eu› EUROPA› EU law and publications› EUR-Lex>. Acesso em: 26 jan. 2017.

EUROPARL. **Carta de Direitos Fundamentais da União Europeia**. Disponível em: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em: 05 jan. 2017.

_____. Disponível em: <http://www.europarl.europa.eu/atyourservice/pt/displayFtu.html?ftuId=FTU_5.12.8.html>. Acesso em: 06 jan. 2017

MACARIO, Francesco. La protezione dei dati personali nel diritto privato europeo. *In*: ***La disciplina del trattamento dei dati personali.*** CUFFARO, Vicenzo; RICCIUTO, Vicenzo. Torino: Giappechelli, 1997.

MARTINEZ, Pablo Domingues. **Direito ao esquecimento:** a proteção da memória individual na sociedade da informação. Rio de Janeiro: Lumem Juris, 2014.

MORGADO, Laerte Ferreira. **O cenário internacional de proteção de dados pessoais.** Necessitamos de um código brasileiro? Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=6336>. Acesso em: 27 jan. 2017.

OECD. **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.** Disponível em: <www.oecd.org/bookshop/>. Acesso em: 13 jan. 2017.

PÉREZ LUÑO, Antonio-Enrique. ***Los derechos humanos en la Sociedad Tecnológica.*** Madrid: ed. Universitas S.A., 2012.

REGULAMENTO (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016. **Jornal Oficial da União Europeia**. Livro 119/1, de 4 de maio de 2016.Disponível em: <https://www.icjp.pt/cursos/8879/pdf>. Acesso em: 26 jan.2017.

SARMENTO E CASTRO, Catarina. Artigo 8º - Proteção de dados Pessoais. In: **Carta dos Direitos Fundamentais da União Europeia.** SILVEIRA, Alessandra: CANOTILHO, Mariana - Coordenadores. Coimbra (Portugal): Almedina, 2013, p.120-128.

DOI: 10.6084/m9.figshare.5632153

SILVA, Bruno Batista. **Direito ao Esquecimento:** mecanismo de proteção dos direitos da personalidade. Disponível em: <https://jus.com.br/artigos/55014/direito-ao-esquecimento-mecanismo-de-protecao-dos-direitos-da-personalidade/3>. Acesso em: 16 fev. 2017.

TRF4. Disponível em: <http://www2.trf4.jus.br/trf4/controlador.php?acao=noticia_visualizar&id_noticia=9059>. Acesso em: 16 fev. 2017.

WIENER, Norbert. Informação é informação, não é matéria nem energia. In: **A proteção de dados pessoais nas relações de consumo:** para além da informação creditícia. Caderno de Investigações Científicas. Organizador: Danilo Cesar Maganhoto Doneda. Brasília: SDE/DPDC, 2010, p 17-38.