LÍVIA FRONER MORENO RAMIRO

DO DIREITO AO ESQUECIMENTO AO DIREITO À DESVINCULAÇÃO: A TUTELA DOS DADOS PESSOAIS NOS MOTORES DE BUSCA NA INTERNET

Dissertação de Mestrado

Orientadora: Professora Associada Doutora Cíntia Rosa Pereira de Lima

UNIVERSIDADE DE SÃO PAULO

FACULDADE DE DIREITO

São Paulo-SP

2018

LÍVIA FRONER MORENO RAMIRO

Do direito ao esquecimento ao direito à desvinculação: a tutela dos dados pessoais nos motores de busca na internet

Dissertação apresentada à Banca Examinadora do Programa de Pós-Graduação em Direito, da Faculdade de Direito da Universidade de São Paulo, como exigência parcial para obtenção do título de Mestre em Direito, na área de concentração Direito Civil, sob a orientação da Professora Associada Doutora Cíntia Rosa Pereira de Lima.

Versão corrigida em 06 de julho de 2018, conforme orientações da banca examinadora da dissertação de mestrado. A versão original, em formato eletrônico, encontra-se disponível na CPG da Unidade.

UNIVERSIDADE DE SÃO PAULO

FACULDADE DE DIREITO

São Paulo-SP

2018

Ramiro, Lívia Froner Moreno

Do direito ao esquecimento ao direito à desvinculação: a tutela dos dados pessoais nos motores de busca na internet / Lívia Froner Moreno Ramiro; orientadora Cíntia Rosa Pereira de Lima - São Paulo, 2018. 163 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Direito Civil) - Faculdade de Direito, Universidade de São Paulo, 2018.

1. direito ao esquecimento. 2. tutela dos dados pessoais. 3. motores de busca. 4. sociedade informacional. 5. direitos da personalidade.

I. Lima, Cíntia Rosa Pereira de, orient. II. Título

LÍVIA FRONER MORENO RAMIRO

DO DIREITO AO ESQUECIMENTO AO DIREITO À DESVINCULAÇÃO: A TUTELA DOS DADOS PESSOAIS NOS MOTORES DE BUSCA NA INTERNET

Dissertação apresentada à Faculdade de Direito da Universidade de São Paulo, como exigência parcial para obtenção do título de Mestre em Direito, na área de concentração Direito Civil, sob a orientação da Professora Associada Doutora Cíntia Rosa Pereira de Lima.

Banca Examinadora:

Prof. Dr. _____
Instituição: _____
Julgamento: _____
Assinatura _____

Prof. Dr. _____
Instituição: _____
Julgamento: _____
Assinatura _____

Prof. Dr. _____
Instituição: _____
Julgamento: _____
Assinatura: _____

UNIVERSIDADE DE SÃO PAULO

FACULDADE DE DIREITO

São Paulo-SP

2018

A minha família, pelo apoio, coragem, e todo o amor incondicional a mim concedido, base do meu ser e viver.

AGRADECIMENTOS

À minha família pelo apoio, investimento em minha educação, meu exemplo de coragem, força e amor. Minha base e dedicação para todo o sempre.

À Professora Cíntia Rosa Pereira de Lima, pela oportunidade de estar sob a sua orientação e por acreditar neste presente trabalho. Agradeço por todos os momentos alegres, pelo carinho e incentivo constante.

Ao professor Newton De Lucca, a quem devoto profunda admiração, agradeço pelas considerações efetuadas na banca de qualificação e pela oportunidade de ter sido sua aluna durante o mestrado. Suas aulas eram inspiradoras.

Aos amigos e companheiros de mestrado, Caroline Narvaez Leite e Wévertton Gabriel Gomes Flumignan, por compartilharem seus conhecimentos jurídicos, pelas experiências trocadas e, em especial à Daphne Noronha Hachul, que se tornou uma grande amiga, pela força constante para a conclusão da dissertação. Sem eles o caminho no mestrado não teria sido tão gratificante e enriquecedor.

RESUMO

RAMIRO, Lívia Froner Moreno Ramiro. Do direito ao Esquecimento ao direito à desvinculação: a tutela dos dados pessoais nos motores de busca na internet. 163 p. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2018.

Essa dissertação tem como objetivo o estudo dos novos direitos da personalidade como a proteção dos dados pessoais e o direito ao esquecimento no contexto da sociedade informacional, especificamente, a internet. A coleta, o processamento, a utilização, o armazenamento e a circulação de dados pessoais, impulsionados pela economia informacional, podem revelar aspectos da privacidade e da identidade do indivíduo de maneira potencializada. A problematização da investigação científica realizada encontra-se em delimitar o conceito do direito ao esquecimento e a sua eventual autonomia. Para tanto, direitos correlatos como a privacidade, a proteção dos dados pessoais e suas faculdades jurídicas de desindexação e desvinculação serão abordados justamente para demonstrar as diferenças entre eles. Em meio aos desafios que são apresentados pela internet está a circulação das informações pessoais pretéritas, cujo acesso é facilitado pelos motores de busca. Nesse viés, o controle dos dados pessoais pelo seu titular se torna cada vez mais uma tarefa árdua. Ao mesmo tempo em que a ponderação de interesses é necessária por conta do embate com a liberdade de expressão e de informação. Nessa senda, imprescindível se tornou a análise dos recentes julgamentos que envolveram o tema como o do espanhol Mario Gonzáles pela Corte Europeia e o da apresentadora Xuxa Meneghel pelo Superior Tribunal de Justiça brasileiro. De modo conclusivo, situa-se um juízo crítico sobre as concepções de direito ao esquecimento, privacidade, proteção de dados pessoais e identidade.

Palavras-chave: Sociedade Informacional; Motores de Busca; Internet; Esquecimento; Proteção de Dados Pessoais; Privacidade; Direitos de Personalidade;

ABSTRACT

RAMIRO, Lívia Froner Moreno. From the right to forgetfulness to the right to untie: the protection of personal data in Internet search engines. 163 p. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2018.

This dissertation aims to study the new rights of the personality as the protection of personal data and the right to forgetfulness in the context of the information society, specifically the Internet. The collection, processing, use, storage and circulation of personal data, driven by the information economy, can reveal aspects of the individual's privacy and identity in a potentialized way. The problematization of the scientific investigation carried out is to delimit the concept of the right to forgetfulness and its eventual autonomy. To do so, right correlates such as privacy, protection of personal data and their legal faculties of de-indexing and untying will be approached precisely to demonstrate the differences between them. Amidst the challenges presented by the internet is the circulation of personal information, which access is facilitated by search engines. In this bias, the control of personal data by its owner becomes more and more an arduous task. At the same time, the balance of interests is necessary because of the clash with freedom of expression and information. In this way, the analysis of the recent judgments that involved the theme as the Spanish Mario Gonzales by the European Court and that of the presenter Xuxa Meneghel by the Brazilian Superior Court of Justice became essential. In a conclusive way, a critical judgment is placed on the conceptions of right to forgetfulness, privacy, protection of personal data and identity.

Keywords: Information Society; Search engines; Internet; Forgetfulness; Protection of Personal Data; Privacy; Rights of Personality.

SUMÁRIO

INTRODUÇÃO

Considerando que a internet[1] não é terra de ninguém, em que se pode tudo e contra todos, cabe ao Direito a regulação e tutela das diversas formas de violação de direitos da personalidade.

Atualmente, a disponibilização de fatos da esfera privada para ambiente público é prática recorrente. O surgimento da internet, ferramenta que facilitou a comunicação rápida e viabilizou a realização de pesquisas sobre quaisquer assuntos com uma maior facilidade de acesso, potencializou esse fenômeno de coleta, divulgação e compartilhamento de informações pessoais.

Ocorre que a circulação de informações e dados pessoais na internet pode gerar efeitos e consequências para a pessoa humana quando fatos pretéritos não fiquem somente no passado, assombrando-a no presente e prejudicando oportunidades para seu futuro. Esse fenômeno social que tem despertado a necessidade de resposta da Ciência do Direito justamente pela violação da personalidade e dignidade humana.

Com efeito, essa espécie de demanda tem sido enfrentada pelos julgadores nos tribunais, especialmente, no Brasil, que possui um forte modelo jurídico de proteção aos direitos da personalidade. Como o juiz não pode se escusar de dizer o direito, deve julgar o caso concreto, os pleitos por remoção de informações na internet exigiu o surgimento da discussão de um direito de personalidade chamado de direito ao esquecimento.

O termo direito ao esquecimento vem sendo utilizado no âmbito da jurisprudência e dos doutos doutrinadores com frequência, tendo a sua origem no âmbito criminal, nos casos de divulgação de fatos verídicos e pretéritos sobre a vida criminosa pregressa do réu que podem obstaculizar a sua reinserção na sociedade. No entanto, a grande procura pelo direito ao esquecimento se deu nos dias atuais em razão do uso da internet que potencializa e pereniza a informação.

[1] Adotou-se a palavra internet com a letra "i" em minúsculo em razão das considerações feitas pelo professor Newton De Lucca em diversas obras jurídicas, especialmente, na oportunidade em que prefaciou o livro "Tutela e privacidade na internet", do autor Marcel Leonardi, tendo expressado os seguintes argumentos para o fazê-lo: "É oportuno recordar que internet com 'i' minúsculo é a contração de *interconnected network*(rede interconectada), expressão que pode ser usada para se referir a redes de computadores privados interligados sem qualquer relação com a Internet global. Em outras palavras, a Internet é uma internet, mas a recíproca não é verdadeira". Logo, como a presente dissertação trata de redes de computadores privadas, a expressão internet com "i" minúsculo se justifica. LEONARDI, Marcel. *Tutela e Privacidade na Internet*. São Paulo: Saraiva, 2012, p.14-15.

Assim, passou-se a discutir sobre a utilização de um dado ou informação pessoal pretérita, bem como sobre o modo e finalidade com que são lembrados justamente pela eternização na internet que é corroborada pelas ferramentas de busca.

Além do direito ao esquecimento, outras duas controvérsias brotaram a partir de sua reflexão no que diz respeito aos motores de busca: a primeira sobre o acesso às informações pretéritas, irrelevantes e desatualizadas disponibilizadas pelos motores de busca e a segunda sobre dados pessoais que são vinculados com termos depreciativos por meio da sugestão do próprio motor de busca, seja por seu sistema ou pela influência dos resultados da pesquisa por terceiros.

A disponibilização de informações de forma perene e prejudicial, a circulação de dados pessoais irrelevantes e desatualizados, bem como a vinculação do nome da pessoa com fatos inverídicos ou termos prejudiciais, são três desafios que clamam por uma solução e estão na "ordem do dia".

Optou-se por pesquisar o tema do direito ao esquecimento ao direito à desvinculação de dados pessoais em razão da novidade em se tutelar a pessoa e os seus dados, principalmente, na seara da internet.

O direito ao esquecimento não é um fenômeno particularmente novo, porém teve a sua discussão reacendida por causa de alguns casos que tiveram grande repercussão no Brasil e na Europa.

Em outubro de 2010, Maria da Graça Meneghel, a "Xuxa", ajuizou uma ação com a finalidade de remover os resultados de busca ligados à expressão "Xuxa pedófila" e de qualquer informação que associasse o seu nome com condutas criminosas. Em sede liminar, deferiu-se a medida aclamada para que a *Google* deixasse de disponibilizar aqueles resultados aos internautas. Ao ser analisado pelo Superior Tribunal de Justiça, órgão de cúpula que salvaguarda as normas infraconstitucionais, a 3ª Turma decidiu de forma contrária. Entendeu que a *Google* é apenas um facilitador de informação e que não se pode reprimir o direito à informação. Nestes termos, a ação deveria ter sido ajuizada contra aqueles que veicularem o conteúdo como dados relacionados à imagem da apresentadora[2].

Tendo esse caso em destaque, exemplifica-se que este se amolda aos três direitos propostos uma vez que a apresentadora pode querer esquecer o fato passado, qual seja o filme "Amor, estranho amor", realizado em 1982, que conta a história de Hugo, menino de

[2] REsp 1316921/ RJ, Rel. Ministra Nancy Andrighi, Terceira Turma, julgado em 26/6/2012, DJe 29/6/2012.

12 anos, filho da dona de um bordel de luxo que é seduzido por Tamara, uma das prostitutas, vivida por Xuxa. A apresentadora de televisão, então, contava com 19 anos de idade quando interpretou esse seu primeiro papel em filme erótico. [3]

Tamanho o sucesso do filme no cinema que os produtores decidiram lançá-lo em videocassete para a sua comercialização no mercado. Todavia, alguns anos se passaram e Xuxa se tornou famosa, inclusive, por seu trabalho com programas infantis, com vasta atuação nesse meio. Em razão da mudança de comportamento e de sua imagem, a apresentadora ajuizou uma ação de busca e apreensão de todas as cópias não autorizadas do vídeo, tendo se entendido que: "a exploração através de videocassete tornava a obra acessível ao público infantil, gerando um desvirtuamento da sua imagem, incompatível com o seu perfil artístico atual". [4]

Embora a apresentadora tenha almejado sucesso na ação para o recolhimento dos videocassetes, a vinda da internet, modificou sobremaneira como as informações são potencializadas e compartilhadas.

A mudança de comportamento da Xuxa e o fato de ela desejar manter os fatos pretéritos no passado, aqueles que não mais merecem ser rememorados e que lhe causem certo constrangimento, poderia ser o fundamento da pretensão de um direito ao esquecimento.

Soma-se a essa questão justamente o contexto da sociedade informacional que, com o advento das novas tecnologias da informação, como a internet e os dispositivos móveis, formaram o solo cultivável para o alto fluxo de circulação de informações. Assim, como deixar o passado ficar no passado, sem que os seus efeitos interfiram no desenvolvimento das pessoas no presente?

Por consequência, a divulgação dos vídeos e imagens de nudez da apresentadora é facilitada pelos mecanismos de busca como o gigante *Google* que vasculha as informações na internet, através de seus robôs, passa a indexar o link, armazená-lo e depois transmiti-lo aos seus usuários por meio dos resultados de busca.

É certo que ela poderá almejar apenas a desindexação dos resultados a fim de que dificulte o acesso para os demais, o que configuraria o direito à desindexação, propriamente da seara da proteção dos dados pessoais, desde que o seu tratamento seja realizado de forma adequada.

---

[3] A história da apresentadora Xuxa transcrita com detalhes foi extraída do livro: BRANCO, Sérgio. *Memória e esquecimento na internet*. Porto Alegre: Editora: Arquipélago Editorial, 2017, p. 126-128.
[4] TJ-RJ. Acordão da Apelação Civel n. 3.819/91.

Voltando ao exemplo bem elucidativo da apresentadora Xuxa, a não associação das palavras “Xuxa” mais “pedófila”, termo sugerido pelo próprio mecanismo de busca, pode proteger o seu dado pessoal, a sua identidade pessoal, o seu bom nome, a sua imagem e a sua honra. Tal vinculação e associação de dado pessoal com termos depreciativos seria extremamente ofensiva e ilegal.

Nesse sentido, todas as nuances e desafios para a pessoa natural que podem surgir pela interação entre seres humanos, internet e os provedores de aplicação como o motor de busca ocorrem no contexto sociedade informacional. Logo, abordar-se-á no primeiro capítulo a sociedade informacional e o seu surgimento, o fluxo das informações como um poder econômico, a vigilância irrestrita na internet e o poder de transformação das pessoas naquilo que elas não são, isto é, a criação de perfis virtuais de acordo com o que é divulgado pelos mecanismos de busca.

No segundo capítulo, fez-se necessário desenvolver o conceito de dados pessoais, de tratamento de dados pessoais e a sua relação com outros direitos da personalidade. Elegeu-se, preferencialmente, adotar a abordagem pelo sistema europeu de proteção de dados pessoais, sobretudo porque, na União Europeia, foi estabelecido um nível elevado de proteção desde a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 1995, relativa à proteção das pessoas singulares , ao tratamento de dados pessoais e à livre circulação desses dados, até o seu aprimoramento com o Regulamento Geral de Proteção de Dados Pessoais aprovado em 2016.

A necessidade em se estudar a tutela dos dados pessoais nos motores de busca na internet se deu por causa do caso paradigmático do advogado espanhol Mario Costeja que pleiteou a remoção de uma informação pessoal constrangedora e verídica do site e do motor de busca Google, o que foi a principal inspiração para o presente trabalho.

Ainda mais, o segundo capítulo ganhou especial atenção justamente pela aprovação do novo Regulamento Geral de Proteção de Dados Pessoais Europeu que trouxe o direito ao apagamento como sendo um “direito a ser esquecido” causando a maior divergência sobre se existiria um direito ao esquecimento digital e o que o diferenciaria da concepção clássica de direito ao esquecimento das seara criminal.

Imagine-se, com um novo olhar, voltado para a internet e os meios de comunicação em massa, como seria o reconhecimento do direito ao esquecimento como um direito autônomo, com a sua devida conceituação, fundamento e características próprias.

Sob o viés do citado caso espanhol, uma pessoa teria o direito a obrigar um motor de busca da internet a efetuar a desindexação da informação pessoal disponibilizada aos internautas nos resultados em razão da pesquisa com o seu nome?

Tendo em vista a questão dos motores de busca que, no terceiro capítulo, de forma bem sucinta, o funcionamento dos motores de busca foi objeto de análise para que o leitor compreenda as atividades que ele desempenha para depois verificar se estas se enquadrariam ou não no conceito de tratamento de dados pessoais e, por conseguinte, na aplicação das leis de proteção aos dados pessoais.

No quarto capítulo, traçou-se o ponto mais controvertido da dissertação que seria categorizar o direito ao esquecimento, expondo a dificuldade de sua conceituação e da afirmação de sua natureza jurídica, a sua autonomia e legitimados ativa e passivamente. Se não bastasse, os limites para a sua aplicação também foi objeto de análise. A grande polêmica se dá pelo embate entre direitos fundamentais como a liberdade de expressão, a liberdade de informação, a liberdade de imprensa como um dos principais argumentos para a sua rejeição.

Após o estudo do direito ao esquecimento, fez-se imperiosa a distinção sobre o que não seria o direito ao esquecimento, isto é, a desindexação de dados pessoais, o que foi objeto de verificação no quinto capítulo.

Por último, pretendeu-se abrir um sexto capítulo para a compreensão sobre o que é a desvinculação de dados pessoais, para diferenciá-lo do direito à desindexação. Esclarece-se, nesse ponto, a ausência quase que completa de material bibliográfico sobre o tema, porém a sua não abordagem nesta dissertação, possivelmente prejudicaria o entendimento e alcance sobre o ato de desindexar dados pessoais. Com isso, objetiva-se o fomento da reflexão, da discussão e do desenvolvimento ainda que modesto da vinculação indevida de dados pessoais como fenômeno recorrente nos motores de busca na internet.

Logo, o presente trabalho, resumidamente e sem esgotar o vasto tema, visou encontrar respostas para os seguintes questionamentos: quais são os fatores e limitações do direito ao esquecimento? Existe um direito ao esquecimento voltado para os motores de busca? O que é o direito ao esquecimento? O que é desindexação? O que é desvinculação?

O resultado desta pesquisa é o convite para uma análise sobre o direito ao esquecimento, o direito à desindexação e o direito à desvinculação, tendo como parâmetro a sociedade informacional, notadamente, o funcionamento da internet e dos motores de

busca, para garantir e tutelar a proteção dos dados pessoais, a privacidade e a identidade pessoal do indivíduo.

CAPÍTULO I – A SOCIEDADE INFORMACIONAL

1.1. Sociedade Informacional: notas introdutórias e terminologia

O século XXI tem protagonizado a um novo estágio do desenvolvimento histórico, econômico, cultural, social, jurídico e político, denominado pelo sociólogo espanhol Manuel Castells de sociedade em rede. [5] O novo modo de produção capitalista, inaugurado pelo enlace da tecnologia e do meio digital, impulsionou o crescimento da produção de equipamentos informáticos e a disseminação da Internet em escala mundial.

Com base nesse pensamento, Barreto Junior destaca os três fenômenos que deram origem da mudança da sociedade industrial para a era pós-industrial, quais sejam:

> a) A convergência da base tecnológica – possibilidade de poder representar e processar qualquer informação de uma única forma, a digital. Essa convergência teve profundas implicações no processo de mundialização da economia, das telecomunicações e dos processos sócias, pois, sem uma padronização tecnológica mínima, este novo paradigma de sociedade seria inimaginável;
> b) Dinâmica da indústria – proporcionou contínua queda nos preços dos computadores, insumos tecnológicos, softwares, componentes de redes, permitindo maior acessibilidade à integração na rede;
> c) Crescimento e expansão da internet: aumento exponencial da população mundial com acesso à rede e evolução da conectividade internacional. [6]

Esses fenômenos ligados entre si acarretaram em "(...) um novo paradigma de sociedade, no qual a energia é progressivamente substituída pela informação, como fonte primeira do progresso social, tendo como produto essencial a prestação de serviços novos".[7]

---

[5] CASTELLS, Manuel. *A Era da Informação: economia, sociedade e cultura*. V.1, a sociedade em rede. 8 ª ed. São Paulo: Paz e Terra, 2005.
[6] BARRETO JUNIOR, Irineu Francisco. *Atualidade do Conceito Sociedade da Informação para a Pesquisa Jurídica*. In: PAESANO, Liliana Minardi (coord.). Direito na Sociedade da Informação. São Paulo: Atlas, 2007, p. 62.
[7] MARQUES, Garcia. LOURENÇO, Martins. *Direito da informática*. Coimbra: Almedina, 2000, p. 42.

Patente que os contornos dessa nova sociedade surgiram do que se convencionou denominar de "Sociedade da Informação", conceito que foi alvo de debates entre os doutrinadores.

O professor José de Oliveira da Ascensão prefere designar a atual sociedade como "sociedade da comunicação", nesse sentido aduz que "melhor se falaria até em sociedade da comunicação, uma vez que o que se pretende impulsionar é a comunicação, e só num sentido muito lato se pode qualificar a mensagem como informação". [8] Por outro lado, Pierre Lévy prefere denominar de "sociedade do conhecimento". [9]

Independente da expressão utilizada para designar a atual sociedade[10], como bem alertou o professor Newton De Lucca, seja denominada de "Digital, da Informação ou do Conhecimento", o que importa é que o jurista é um ser refratário a toda inovação, sendo uma tarefa extraordinária discorrer a respeito dela. [11]

Em contrapartida, o raciocínio de Manuel Castells, na obra "A sociedade em rede"[12], da trilogia "A Era da Informação: economia, sociedade e cultura" merece ser abordado sobre a terminologia de "sociedade da informação" em uma de suas notas de rodapé. Na citada obra, Castells analisa que seria um equívoco se falar em "sociedade da informação", como ficou conhecida, já que existe uma diferença entre "informação" e "informacional". Ao fazer um paralelo com "indústria" e "industrial", o autor revela que uma sociedade de indústria é aquela que possui muitas indústrias, ao passo que uma sociedade industrial é aquela em que a indústria exerce um forte papel em todos os setores da sociedade, sendo a principal fonte de produtividade e de poder econômico. Por esse motivo, a "sociedade informacional" é o melhor termo a ser usado.

A "sociedade informacional" então é aquela em que se evidencia o papel da informação em determinada sociedade, sendo esta fonte de produção de riqueza (economia informacional) e instrumento utilizado nas relações de poder.

---

[8]ASCENÇÃO, José de Oliveira da. A Sociedade da Informação. In: *Direito da Sociedade da Informação*. V. 1. Coimbra: Coimbra Editora, 1999, p. 167.). Por outro lado, Pierre Lévy prefere denominar de "sociedade do conhecimento". (LÈVY, Pierre. *Collective Inteligence:* mankind's emerging world in cyberspace. Tradução de Robert Bononno. Cambridge (MA): Perseus Books, 1997, p. 02).

[9]LÈVY, Pierre. *Collective Inteligence:* mankind's emerging world in cyberspace. Tradução de Robert Bononno. Cambridge (MA): Perseus Books, 1997, p. 02.

[10] Os portugueses Garcia e Lourenço também afirmam que a expressão "sociedade de informação" "(...) cada vez importa menos definir na medida em que se vai vivendo em maior escala – assenta sobre o uso óptimo das novas tecnologias da informação e da comunicação, em respeito pelos princípios democráticos, da igualdade e da solidariedade, visando o reforço da economia e da prestação de serviços públicos e, a final, a melhoria da qualidade de vida de todos os cidadãos". MARQUES, Garcia. LOURENÇO, Martins. Direito da informática. Coimbra: Almedina, 2000, p.43.

[11] DE LUCCA, Newton. Direito de Arrependimento no Âmbito do Comércio Eletrônico. In: MENDES, Gilmar F. (coord). *Direito, Inovação e Tecnologia*. São Paulo: Saraiva, 2015, p. 252.

[12] *Op. Cit.*, p. 64-65.

A relação entre a sociedade em rede e a sociedade informacional proposta por Castells deve permanecer já que uma não esgota o sentido da outra. Isso porque, a sociedade em rede é uma das características principais ou componentes da sociedade informacional. Outros componentes da sociedade informacional como movimentos sociais ou o Estado, embora sejam influenciados constantemente, não apresentam a característica da sociedade em redes, que são órgãos estruturados em rede, coligados. [13]

Cada vez mais, a informação possui funções das mais variadas, de forma exemplificativa, ela serve como moeda de troca, acumulação de riqueza, transforma os consumidores em mercadoria através de seus dados pessoais, bem como se alia à prevenção de doenças por meio de um estudo dos hábitos alimentares e costumes, ajuda na inovação tecnológica e facilita a comunicação entre pessoas que moram em países opostos com baixo custo. Isto é, a informação implica benefícios e malefícios.

O professor Roberto Senise Lisboa destaca o papel da sociedade informacional diante das facilidades que a internet proporciona:

> A sociedade da informação resulta desses acontecimentos, viabilizando-se a comunicação mais rápida e a obtenção adequada de dados. Verifica-se a concentração de empresas mundiais de informação. Busca-se o acesso a todo tipo de obra ou informação disponível inclusive em rede de telecomunicações, por meio de uma base de dados obtida em obras multimídia e em trabalhos desenvolvidos pela internet.[14]

Esse é o contexto atual pelo qual se desenvolve o homem enquanto ser, pessoa individual e intelectual, que se projeta no mundo exterior, na sua relação com terceiros e entre familiares.

De certo que "o *superinformacionismo* cria uma verdadeira massa de informações sobre tudo e sobre todos, queiram ou não estar naqueles conjuntos de dados ou informações" [15]. Isto porque, a informação se transformou no verdadeiro ativo da

---

[13] Idem.

[14] LISBOA, Roberto Senise. A inviolabilidade de correspondência na Internet. In: LUCCA, Newton De. SIMÃO FILHO, Adalberto. *Direito & Internet*. Aspectos Jurídicos Relevantes. Bauru, SP: EDIPRO, 2001.

[15] Os autores vão além ao dispor sobre os limites da difusão do manancial de informações: "Qual é o limite desse superinformacionismo? Sem dúvida um parâmetro para sua limitação são os direitos fundamentais e a lei. O superinformacionismo é esse contexto em que nos encontramos. Uma busca na internet diz mais que somos do que nós mesmos imaginamos. E não são apenas os dados que se coletam com facilidade, mas até mesmo os dados de acesso que nos expõem. Até que ponto pode ser divulgada, invadida, destruída ou desnudada a personalidade de cada um de nós? Quanto tempo uma pessoa pode pagar por um crime, mais que aquele em que permanece em uma prisão?". RULLI JUNIOR, Antonio; RULLI NETO, Antonio. *Direito ao esquecimento e o superinformacionaismo: apontamentos no direito brasileiro dentro do contexto de sociedade da informação*. Disponível em: https://www.cidp.pt/publicacoes/revistas/ridb/2012/01/2012_01_0419_0434.pdf. Acesso em: 04.05.2016.

economia e fonte de poder que, muitas vezes, está longe de ser controlada pelo individuo, seja pela ausência de conhecimento quanto pelo tratamento inadequado, sem o crivo de seu consentimento.

1.2. A informação como fonte de poderio econômico

A Internet modificou as suas bases ao passo que não há mais como afirmar que se trata de um ambiente em que a pessoa pode ficar totalmente anônima. Isso porque, a fórmula para enriquecer é saber os interesses do público, analisando cada pessoa e, assim, dirigindo as correspondentes propagandas. [16]

De início, os especialistas optaram por deixar a Web como um sistema aberto, livre e convidativo, o que, na verdade, foi uma estratégia. Os websites mais rentáveis partiam de uma distribuição de acesso "gratuito" e sem cobrança dos usuários e de terceiros. Aparentemente, inexistia remuneração, mas isso não quer dizer que ela se dava de maneira direta. Os anúncios de publicidade, taxas e comissões são o verdadeiro lucro das grandes corporações do mundo virtual. Há que se compreender que os consumidores não são observados como pessoas que navegam na internet, mas sim como o produto a ser vendido. [17]

Como bem ressaltou Eli Pariser, em sua obra "O filtro invisível: o que a internet está escondendo de você", cada indicador de clique que é enviado na internet é uma mercadoria para os comerciantes do mercado do comportamento, e assim sendo cada

[16] Segundo Parisier, "(...) o mundo digital está mudando em suas bases. O que um dia foi um meio anônimo em que qualquer pessoa podia ser quem quisesse – no qual, nas palavras de uma famosa charge da *New Yorker*, 'ninguém sabe que você é um cachorro' – transformou-se agora numa ferramenta dedicada a solicitar e analisar os nossos dados pessoais". (...) "A nova internet não só já sabe que você é um cachorro – ela conhece a sua raça e quer lhe vender um saco de ração *premium*". PARISER, Eli. O filtro invisível: o que a internet está escondendo de você. Tradução de Diego Alfaro. Rio de Janeiro: Zahar, 2011, p. 12.

[17] Ao discorrer sobre o Google, Siva alerta que o primeiro passo a se tomar é perceber a influencia do Google: "uma maneira de começar é perceber que não somos clientes do Google: somos seu produto. Nós - nossas fantasias, fetiches, predileções e preferências - são o que o Google vende para os anunciantes. Quando usamos o Google para descobrir coisas na Web, o Google usa nossas pesquisas na Web para descobrir coisas sobre nós"(tradução livre). Conforme o trecho original: "*One way to begin is by realizing tha we are not Google´s customers: we are its product. We – our fancies, fetiches, predilections, and preferences – are what Google sells to advertisers. When we use Google to find out things on the Web, Google uses our Web searches to find out things about us*." VAIDHYANATHAN, Siva. *The Glooglization of everything (and why we should worry)*. Los Angeles: University of California Press, 2011, p.3.

movimento que é feito "com o mouse pode ser leiloado em microssegundos a quem fizer a melhor oferta". [18]

A estratégia é simples quanto mais personalizadas forem as pesquisas de hábitos dos usuários (tráfego de dados pessoais) na Web, mais anúncios serão vendidos e maior será a chance de que o usuário compre os produtos oferecidos.[19]

Ora, baseado nesse ciclo, as empresas com maior capital investem em brilhantes especialistas do meio computacional capazes de desenvolver técnicas que assegurem uma coleta cada vez mais personalizada de dados pessoais e com isso obtêm lucro para potencializar o seu negócio.

Por conseguinte, apesar da expansão de novos negócios, como o é o mundo da rede, a informação não deixou de ser um sinônimo de "poder", em particular, econômico.

Necessário lembrar que a informação sempre foi um componente essencial de definição de poderes em uma sociedade.[20] O uso de informações pessoais pelo Estado predominou por muito tempo até que as tecnologias que possibilitaram a sua coleta e tratamento fossem desenvolvidas, estando disponível também aos particulares.

O atual controle da informação deve ser somado ao contexto das novas tecnologias que, em razão delas e, especialmente da informática, tornou-se possível uma disseminação de agentes detentores de tal poderio. Dessa maneira, Doneda afirma um fato incontestável: "a importância da informação aumenta na medida em que a tecnologia passa a fornecer meios para torná-la útil a um custo razoável". [21]

Visível se encontra uma nova estrutura de poder que pode ser chamada de "economia informacional"[22] resultante da revolução tecnológica, na qual a informação é o próprio produto[23], comercializada e não apenas utilizada para criar bens de consumo e prestar serviços através do conhecimento de acadêmicos e outras fontes.

Dentro desse contexto, a captação e a análise da informação pode tanto solucionar problemas quanto causá-los.

---

[18] Ibidem idem, 2011, p. 12.
[19] PARISER, Eli. *O filtro invisível: o que a internet está escondendo de você.* Tradução de Diego Alfaro. Rio de Janeiro: Zahar, 2011, p. 13.
[20] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 15.
[21] Idem, ibidem.
[22] CASTELLS, Manuel. *A Era da Informação: economia, sociedade e cultura*. V.1, a sociedade em rede. 8 ª ed. São Paulo: Paz e Terra, 2005, p. 150-152.
[23] LIMA, Cíntia Rosa Pereira de. *A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil*. Tese de livre-docência, apresentada à Faculdade de Direito de Ribeirão Preto da USP. Ribeirão Preto, 2015, p. 31.

O poder praticamente ilimitado para combinar, reunir e examinar informações pessoais derivado do avanço do conhecimento computacional pode assim implementar melhorias dos serviços de saúde. Como, no caso, de uma análise de dados genéticos para a criação de um mapa de fatores de risco da pessoa que poderá identificar e prevenir problemas de saúde ou tratá-los antes que piorem. Com a prevenção de doenças, o Estado e os particulares economizariam milhões de sua receita e remuneração, eliminando também a superlotação de hospitais que é uma das mazelas da saúde pública.

Do mesmo modo, as seguradoras de automóveis que já se valem de informações como distância percorrida e localização para avaliar a probabilidade de um motorista sofrer um acidente, poderiam obter um número maior de dados pessoais a fim de avaliar e reduzir custos. Isto é, na posse de outros dados como velocidade, tráfego e registros de manutenção do veículo, as seguradoras poderiam praticar um preço mais justo para o consumidor.

No campo da criminologia e psicologia, os dados pessoais coletados da população são capazes de determinar padrões de criminalidade para permitir um "policiamento preventivo", prevendo os locais com maiores índices de ocorrência de delitos.

Em contrapartida, como malefícios temos, em particular, a violação dos direitos da personalidade do homem. O usuário da internet que costuma divulgar informações e aspectos de sua vida privada sem notar o alto grau de exposição e visibilidade que emprega no meio virtual pode vir a sofrer prejuízos presentes e futuros.

Infortúnio que, na maioria das vezes, os internautas não notam que estão sendo vigiados a todo tempo. Por isso, será analisada a sociedade em outro aspecto sociológico guiado pelo monitoramento descomedido que, culmina, no uso dos dados pessoais.

1.3. A "Vigilância Líquida" de Zygmunt Bauman

A sociedade em rede combinada com a sociedade informacional causa o surgimento de um novo capitalismo cercado pela vigilância total. O conceito de vigilância líquida é disposto por Zygmunt Bauman como:

> Vigilância Líquida é menos uma forma completa de especificar a vigilância e mais uma orientação, um modo de situar as mudanças nessa área na modernidade fluida e perturbadora da atualidade. A vigilância suaviza-se especialmente no reino do consumo. Velhas amarras afrouxam à medida que fragmentos de dados pessoais obtidos para um objetivo são facilmente usados com outro fim. [24]

A apropriação de dados pessoais e a superexposição do indivíduo levam a um monitoramento desenfreado, cada qual vigiado e avaliado. Em verdade, o "consumo livre" transmite uma sensação de liberdade, de soltar as amarras, porém é apenas uma sensação ilusória, ora que continuamos a ser vigiados.

A vigilância pode ser notada nos aeroportos e na entrada de eventos com inspeções realizadas por *scanners* corporais, nos bancos com o uso de aparelhos de checagem biométrica, nas lojas virtuais com as compras e venda de produtos, enfim, todo e qualquer acesso *on-line* ou participações em mídias sociais. [25]

Inegável que as ações do usuário são monitoradas pela Internet, isto é, estamos em uma verdadeira "sociedade da vigilância", como diz o título da obra de Stefano Rodotà[26], ao ponto de se colocar em xeque a própria privacidade e intimidade do indivíduo.

Tanto é que o fundador do site Wikileaks, Julian Assange, afirmou, no dia 13 de julho de 2016, durante o seminário internacional "Liberdade de Expressão, Direito à Comunicação Universal e Imprensa Plural para as Democracias do Mundo", ocorrido em Santiago, que as empresas de tecnologia como o *Google* e o *Facebook* recebem mais informações do que a Agência de Segurança Nacional dos Estados Unidos (NSA). Para ele, este é o novo modelo de negócio mundial estabelecido por um "capitalismo de vigilância". [27]

---

[24] BAUMAN, Zygmunt. *Vigilância: diálogos com David Lyon*. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar Editores, 2013, p. 10.

[25] É exatamente no contexto da sociedade informacional que Zygmunt Bauman encontra os tipos de vigilância seja para questões de segurança ou comerciais: "A vigilância é uma dimensão-chave do mundo moderno; e, na maioria dos países, as pessoas têm muita consciência de como ela as afeta. Não apenas em Londres e Nova York, mas também em Nova Délhi, Xangai e Rio de Janeiro, as câmeras de vídeo são elemento comum nos lugares públicos. Por toda parte, viajantes em passagem por aeroportos sabem que precisam atravessar não apenas o controle de passaportes em sua versão do século XXI, mas também por novos dispositivos, como escâneres corporais e aparelhos de checagem biométrica, que têm proliferado desde o 11 de Setembro. E se tudo isso tem a ver com segurança, outros tipos de vigilância, relativos a compras rotineiras e comuns, acesso on-line ou participação em mídias sociais, também se tornam cada vez mais onipresentes. Temos de mostrar documentos de identidade, inserir senhas e usar controles codificados em numerosos contextos, desde fazer compras pela internet até entrar em prédios". *Ibidem*, p. 06.

[26] RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Rio de Janeiro: Renovar, 2008.

[27] Disponível em: http://g1.globo.com/tecnologia/noticia/2016/07/google-e-facebook-tem-mais-dados-que-eua-diz-fundador-do-wikileaks.html. Acesso em: 01.07.2016.

O abuso do uso da informação é observado, por exemplo, na coleta de informações pessoais sem o consentimento de seu titular. As principais corporações como Google, Facebook, Amazon e Apple estão violando os limites que já foram impostos, transgredindo o direito do outro:

> Em 2004, quando o Google se preparava para abrir seu capital, Larry Page e Sergey Brin celebraram a máxima que deveria definir a empresa deles: "Don´t be evil" ("Não seja mau"). A última polêmica, naturalmente envolve a estranha história do Street View, projeto do Google para fotografar o mundo todo, uma rua de cada vez, para a sua ferramenta de mapas. Acontece que o Google estava coletando mais do que apenas imagens: autoridades federais dos EUA acusaram a companhia de também levantar dados pessoais a partir de sistemas wi-fi, inclusive e-mails e senhas. Muita gente deixaria por isso mesmo, se não fossem todas as outras coisas preocupantes com o Google. A empresa já foi acusada de violar propriedade intelectual, de alavancar o trabalho alheio para o seu benefício próprio e de violar as proteções europeias à privacidade pessoal, entre outras coisas. Marck Zuckerberg já pediu desculpas várias vezes pelas mudanças nas politicas do Facebook relativas à privacidade e propriedade dos dados. No ano passado, ele concordou com uma auditoria de 20 anos sobre as práticas do Facebook. Jeff Bezos é criticado pela forma como a Amazon partilha dados com outras empresas e quais informações armazena em seu navegador. E a Apple, antes mesmo de entrar na mira pelas práticas trabalhistas na chinesa Foxconn, teve problemas pela maneira como lidava com informações pessoais ao recomendar músicas. (...) então, se a tecnologia está conferindo novos sentidos ao privado e ao comum, a falha ao violar limites é também uma forma de saber onde esses limites mudaram. [28]

.

Infelizmente, na sociedade informacional, a disputa pela informação pode gerar certas agressões à pessoa humana como a intromissão na vida privada, a manipulação de ideias e controle dos anseios pessoais.

Além do mais, o professor Eduardo Tomacevicius Filho também riscou um panorama de aprisionamento da pessoa em razão do tratamento de dados pessoais fornecidos, observados, derivados e inferidos nas redes sociais, afirmação que se estende na internet como um todo:

> [...] cada pessoa em uma rede social cria um dossiê sobre si mesmo, voluntariamente. Mediante o tratamento desses dados por algoritmos, tenta-se prever comportamentos futuros e, com isso, estabelecer controles ou selecionar diretamente potenciais interessados em determinado produto ou serviço. [...] Durante os próximos quinze anos, certamente surgirão inovações e aperfeiçoamentos destinados ao recolhimento de informações sobre a vida privada de cada pessoa. Quanto mais se vive, mais informações são coletadas sobre as pessoas e a quantidade de informações coletadas tende ao infinito.

[28] HARDY, Quentin. *Impondo limites aos titãs da internet*. *The New York Times*, 30 abr. 2012.

> Poder-se-á ter a situação em que uma pessoa terá sido monitorada desde o seu nascimento até metade de sua vida esperada. Considerando que a informação é poder, a quantidade de informações a respeito de determinada pessoa é uma forma de controle sobre ela [...]. [29]

A consciência de que, os dados e informações pessoais que circulam na internet realmente possuem um valor, extraído da própria pessoa que é inimaginavelmente vigiada nos tempos atuais, impulsiona a reflexão sobre novos direitos passíveis de frear a invasão da personalidade, notadamente, na esfera da vida privada, do tratamento de seus dados pessoais e da própria identidade. E as razões para despertar esse novo interesse em se tutelar a pessoa humana no ambiente virtual são compreendidas por Bauman:

> De certo, ter uma noção da magnitude e da rápida difusão do processamento de dados é fundamental para que a onda de vigilância seja avaliada pelo que ela é; e descobrir exatamente quais chances e oportunidades de vida são afetadas por esse fenômeno irá galvanizar os esforços no sentido de controlá-lo.[30]

Nesse sentido, os esforços da presente dissertação estão exatamente em demonstrar as consequências modernas da difusão da informação que poderá afetar as chances e oportunidades da vida de uma pessoa. Portanto, instrumentos de controle necessitam ser evidenciados e criados por meio do exercício de direitos como o esquecimento, a desindexação e a desvinculação de dados pessoais na internet.

1.4. A "Googlelização" das pessoas

No início da *World Wide Web*, era quase que imprevisível se imaginar os rumos que ela tomou e a sua vastidão. Como uma nova realidade "virtual" em que privilegiados tinham o seu acesso e, contudo, desconheciam suas funcionalidades. Especialistas da tecnologia da informação observaram as dificuldades dos usuários de localizar aquilo que eles desejavam. Em razão dessa dificuldade, resolveram praticamente "mapear" a web a

[29] TOMACEVICIUS FILHO, Eduardo. *Em direção a um novo 1984? A tutela da vida privada entre a invasão da privacidade e a privacidade renunciada.* Revista da Faculdade de Direito da Universidade de São Paulo, vol. 109, p. 129-169, jan./dez. 2014, p. 140.
[30] BAUMAN, Zygmunt. *Op. cit.*, p. 6.

fim de guiar pesquisadores diante da imensidão de possibilidades da rede. Deu-se, então, a criação das ferramentas de busca.

Ocorre que, alguns serviços de busca eram incompletos e deficientes, outros aceitavam dinheiro para favorecer certos sites em detrimento dos demais. A criação da Google mudou o rumo e o futuro não somente das ferramentas de busca como do próprio uso da internet. A Google não aceitava dinheiro para indexar sites e tinha a missão de levar a informação até o usuário[31], cuja percepção do funcionamento da ferramenta e das vontades humanas fez com que aumentasse o número de usuários. Compreenderam a lógica do sistema, se um site fosse mais acessado do que outro implicava maior relevância para o usuário e, por tal razão, deveria aparecer na lista acima dos outros, nos primeiros resultados da lista.

A *Google Inc*. se tornou um dos maiores *players* (atores, "jogadores") da internet, uma empresa totalmente rentável com diversos produtos bem sucedidos, especialmente, destaca-se o *Google Search*, sendo o motor de busca mais utilizado da Web.[32]

Dados fornecidos pela própria empresa apontam que, no ano de 2001, a Google teve uma receita de 86,426 milhões de dólares, o que foi totalmente superado, em 2015, cujas suas receitas somaram o importe de 66,001 bilhões de dólares. [3334]

A dominação da *Google Inc* no mercado informático foi possibilitada, de início, pelo seu *PageRank*, um algoritmo do motor de busca, cuja fórmula era encontrar a "relevância" das páginas da "web" segundo uma nova noção: a de incluir apenas os melhores documentos. A maioria dos motores de busca rastreava e indexava as páginas que

[31] A missão do Google até os dias atuais é "organizar as informações do mundo e torná-las mundialmente acessíveis e úteis". Disponível em: http://www.google.com/intl/pt-BR/about/. Acesso em: 28.06.2016.

[32] Como exemplo, no Brasil, durante uma pesquisa de quatro semanas realizada pela Serasa Experian, constatou-se que no mês de dezembro de 2014, o Google Brasil registrou 94,31% de acessos nas buscas realizadas na Web. Em segundo lugar ficou o Google.com com 2,05%, seguido pelo Bing com 1,71% e, por fim, o Yahoo! Brasil em quarto lugar com 1,18% e o Ask com 0,54% das buscas ficou em quinto lugar. Interessante notar que a pesquisa foi feita pela Hitwise, uma ferramenta global de inteligência artificial, cuja utilização resulta na realização de campanhas digitais, no monitoramento de concorrência e na possibilidade de antecipar tendências por meio do comportamento de busca e navegação de milhões de pessoas em todo mundo. *Google Brasil tem 94,31% de participação nas buscas em dezembro, segundo Hitwise.* Disponível em: https://marketing.serasaexperian.com.br/imprensa/google-brasil-tem-9431-de-participacao-nas-buscas-em-dezembro-segundo-hitwise-2/. Acesso em: 30.06.2016.

[33] Disponível em: <https://investor.google.com/financial/tables.html.>. Acesso em: 30.06.2016.

[34] Eric Schmidt, presidente executivo. e Jonathan Rosenberg, conselheiro de Larry Page e CEO, ambos da Google, revelam que "hoje, o Google é uma empresa de 50 bilhões de dólares com mais de 45 mil funcionários em mais de quarenta países". SCHMIDT, Eric. ROSENBERG, Jonathan. EAGLE, Alan. *Como o Google funciona*. Trad. André Gordirro. Rio de Janeiro: Intrinseca, 2015, p. 26.

continham a palavra pesquisada, isso quer dizer, tentavam descobrir qual página era mais relevante para aquela palavra-chave. [35]

Com o tempo, os fundadores do Google, Larry Page e Sergey Brin, notaram que da lista de busca formada era possível se avaliar os interesses dos internautas segundo a análise dos dados, vistos como verdadeiras pistas (indicadores) tais como os cliques, posicionamento do link, tamanho e idade da página. O "indicador de clique", grande descoberta dos visionários, funcionava, por exemplo, da seguinte maneira: "se alguém pesquisasse 'Larry Page' e clicasse no segundo resultado da pesquisa, esse era outro tipo de voto: sugeria que o segundo resultado era mais importante para o usuário do que o primeiro". [36]

Nessa esteira, um desafio se impõe constantemente para o motor de busca, qual seja o de descobrir o que cada pessoa quer dizer com uma palavra. A solução para uma pesquisa extremamente personalizada seria desvendar subjetivamente quem aquela pessoa é.

Tendo isso em mente que, outros serviços passaram a ser ofertados pela Google como o Gmail que mantinha um serviço de correio eletrônico (e-mail) e, ao mesmo tempo, servia para o cruzamento dos dados do conteúdo dos e-mails com o comportamento do usuário no motor de busca. [37] Dessa forma, as buscas passaram a ser cada vez mais personalizadas.

Desde 2003, o Google aperfeiçoa a sua infraestrutura, investe largamente para poder rastrear os dados e conteúdo on-line que cresce exponencialmente. [38]

A notoriedade do Google é tão perceptível que as pessoas já incluíram em seus vocabulários o termo "Dar um Google" para encontrar o que se deseja. Tal expressão é comumente dita pelos adolescentes, adultos e atores em filmes e seriados como *Sex and*

[35] Os fundadores do Google, Larry Page e Sergey Brin, em 1997, ao escreverem um artigo, explicitaram tal lógica no sentido de que: "Queremos que a nossa noção de 'relevante' inclua apenas os melhores documentos'(...), pois pode haver dezenas de milhares de documentos ligeiramente relevantes". Além disso, não se conformaram que três dos quatro principais motores de busca não conseguiam sequer encontrar a si mesmos. PARISER, Eli. *Op. cit.*, p. 33.

[36] Idem, ibidem, p. 34.

[37] Idem, ibidem, p. 35.

[38] Decerto que não se pode negar que a intenção também foi a de concorrer com a Microsoft que tentava derrubá-los com os serviços de *MSN Search, Windows Live* e *Bing*. Para tanto, um plano chamado "Finlândia" foi instituído na Google. Aprimoraram seu motor de busca adicionando imagens, livros, vídeos do *Youtube*, dados de compra e outros tipos de informações. Também criaram seus próprios aplicativos como o *Gmail, o Google Docs e Google Maps*. Expandiram seus produtos para outras áreas ao lançar o seu navegador próprio, o *Google Chrome*, tornando-o o navegador mais rápido e seguro do que o da Microsoft. SCHMIDT, Eric. ROSENBERG, Jonathan. EAGLE, Alan. *Op. cit.*, p. 25-26.

The City ou até mesmo pelos representantes de governos[39], fatos que são observados pela emergência de uma verdadeira cultura, a "Googlelização".

A "Googlelização" é o termo escolhido por Siva Vaidhyanathan no seu livro "A *Gloogle*lização de tudo (e porque devemos nos preocupar)" que não trata sobre o funcionamento do Google, mas como o uso dos produtos do Google causam efeitos diários que afetam o desenvolvimento do ser humano:

> O Google coloca os recursos antes inimagináveis na ponta dos dedos - enormes bibliotecas, arquivos, depósitos de registros do governo, tesouros de mercadorias, idas e vindas de toda a humanidade. É isso que quero dizer com a Googlelização de "tudo". A googlização afeta três grandes áreas de preocupação e conduta humana: "nós" (através dos efeitos do Gloogle sobre nossas informações pessoais, hábitos, opiniões e juízos); "O mundo" (através da globalização de um tipo estranho de vigilância e o que eu chamarei de imperialismo infraestrutural); e "Conhecimento" (através de seus efeitos sobre o uso dos grandes corpos de conhecimento acumulados em livros, bancos de dados online e na Web). (Tadução livre) [40]

Dentre os três maiores efeitos causados pelo Google está às implicações em "nós", isto é, o rastreamento de dados diários das informações pessoais, hábitos, opiniões e juízos de valor que influenciam a opinião coletiva.

Os índices de pesquisa oferecidos pelo Google sobre determinada pessoa pode vir a refletir na sua reputação ou juízo de valor que o grupo social ou terceiros realiza.

O autor Siva demonstra que o Google é a lente de contato pela qual o mundo é visto, pois reflete qual pensamento é verdadeiro e importante. Ele filtra e focaliza as indagações e navegações da pessoa pelo mundo. Ele processa, seleciona, indexa e distribui conhecimento que determina o que é considerado como bom, verdadeiro, relevante e de valor. [41]

---

[39] VAIDHYANATHAN, Siva. *Op. cit.* , p. 2.

[40] Segue trecho original: "*Google puts previously unimaginable resources a tour fingertips – huge libraries, archives, warehouses of government records, troves of goods, the comings and goings of whole swaths of humanity. That is what I mean by the Googlization of "everything". Googlization affects three large areas of human concern and conduct: "us" (through Gloogle´s effects on our personal information, habits, opinions, and judgments); "the world" (through the globalization of a strange kind of surveillance and what I'll call infrastructural imperialism); and "Knowledge" (through its effects on the use of the great bodies of knowledge accumulated in books, online databases, and the Web).*" Idem, ibidem, p. 2.

[41] É o que se pode resumir: "Cada vez mais, o Google é a lente através da qual vemos o mundo. O Google absorve, mais do que reflete, o que achamos que é verdadeiro e importante. Ele filtra e concentra nossas consultas e explorações no mundo da informação digitalizada. Ele classifica as informações e as liga tão rápida e sucintamente, reduzindo as preocupações da expressão humana. Em uma lista tão limpa e navegável, isso gera a ilusão reconfortante e talvez necessária tanto da abrangência quanto da precisão. Seu processo de coletar, classificar, vincular e exibir conhecimento determina o que consideramos bom, verdadeiro, valioso e relevante. As apostas não poderiam ser mais altas". Conforme o trecho original: "*Increasingly, Google is the*

E a cultura da "*Glooglization*" tende tão somente a permanecer em razão do "aprisionamento tecnológico" que Parisier se dedica a explicar e definir como:

> O aprisionamento é o ponto no qual os usuários estão tão envolvidos com a tecnologia que, mesmo que um concorrente ofereça um serviço melhor, não vale a pena mudar. Se você for membro do *Facebook*, pense no que representaria mudar para outro site de relacionamento social, mesmo que ele tivesse características muito superiores. Provavelmente daria bastante trabalho – seria extremamente maçante recriar todo o seu perfil, enviar todas as fotos outra vez e digitar arduamente os nomes de seus amigos. Você já está bastante preso. Da mesma forma, o Gmail, o Google Chat, o Google Voice, o Google Docs e muitos outros produtos fazem parte de uma campanha orquestrada de aprisionamento tecnológico do Google. (...) A dinâmica do aprisionamento é descrita pela lei de Metcalfe, um princípio cunhado por Bob Metcalfe, inventor do protocolo Ethernet que conecta computadores. A lei diz que a utilidade de uma rede aumenta cada vez mais rápido sempre que acrescentamos uma nova pessoa à rede. [42]

Toda pessoa que se conecta a rede de computadores e opta por usar os serviços "gratuitos" do Google, aprisiona-se cada vez mais na teia desse gigante econômico. Imperioso destacar que esse aprisionamento em conjunto com a filtragem realizada pelos motores de busca acaba controlando a opinião pública e o modo pelo qual a pessoa se apresenta.

A grande problemática dessa lógica de controle de acessos e de conteúdo está nas consequências causadas para a dignidade humana e para os direitos da personalidade. Os usuários ficam reféns daquilo que os sítios eletrônicos e os motores de busca pretendem divulgar sobre eles e a sua esfera privada. Ainda que a divulgação seja de informações verídicas, o transcurso do tempo pode justificar a retirada, exclusão ou a interrupção do acesso de notícias sobre acontecimentos que causam transtornos para a pessoa, sem causar grande prejuízo para a liberdade de expressão e de informação. Nesse contexto que transita a importância do debate sobre o direito ao esquecimento e direito à desindexação de dados pessoais, o que será mais bem delimitado no capítulo próprio.

---

lens trough which we view the world. Google refracts, more than reflects, what we think é true and important. It filters and focuses our queries and explorations through the world of digitized information. It ranks and links so quickly and succinctly, reducing the boiling tempest of human expression. Into such a clean and navigable list, that is generates the comforting and perhaps necessary illusion of both comprehensiveness and precision. Its process of collecting, ranking, linking, and displaying knowledge determines what we consider to be good, true, valuable, and relevant. The stakes could not be higher".Idem, ibidem, p. 7.

[42] PARISER, Eli. *Op. cit.*, p. 42.

CAPÍTULO II – A PROTEÇÃO E O TRATAMENTO DE DADOS PESSOAIS

2.1. Da privacidade ao direito à proteção de dados pessoais

A sociedade informacional contribuiu para que os dados pessoais se tornassem um bem em si mesmo. A facilidade na sua coleta, armazenamento, circulação e utilização transformaram esse aspecto da pessoa natural em "coisa", sendo algo objetivamente tratável. Fato é que os dados pessoais são uma expressão direta da própria personalidade, capazes de identificar e também representar uma pessoa.

Ocorre que, perante o contexto que foi demonstrado no capítulo anterior, o tratamento automatizado de dados pode oferecer riscos para a pessoa seja economicamente como a filtragem dos valores de uma compra, bem como pessoalmente como a divulgação e reprodução de vídeos infantis que causem transtornos psicológicos para o seu titular. Além disso, as grandes empresas se valem do poder da informação para influenciar o mercado econômico, competirem deslealmente e obterem lucro, ocasionando um desequilíbrio na sociedade como um todo. Por essas e outras razões que se dá a importância de tutelar os dados pessoais e traçar mecanismos que possibilitem o seu controle e conhecimento do seu uso pelo titular, notadamente no âmbito do ordenamento jurídico brasileiro.

Todavia, imprescindível entender o que são os dados pessoais, se estes representam um direito e de onde surgiu essa figura jurídica para que então seja possível traçar o caminho que levará ao ponto complexo de discussão sobre o fenômeno do direito ao esquecimento ao direito à desindexação.

De início, observa-se que o debate sobre os dados pessoais surgiu do estudo e da compreensão da privacidade na contemporaneidade.

A doutrina moderna do direito à privacidade teve como o seu marco fundador[43] o famoso artigo de Samuel Warren e Louis Brandreis, intitulado de "*The right to privacy*", no ano de 1890.[44] Totalmente inédito, tal artigo foi o primeiro que deslocou a privacidade

[43] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006, p. 9.
[44] WARREN, Samuel D. BRANDEIS, Louis D. The right to privacy. In: *Harvard Law Review.* Cambridge: Harvard University Press, v.4, n. 5, p. 193-220, Dec.1890.

das estruturas de direito de propriedade e responsabilidade civil, levando com que as pessoas observassem o caráter pessoal em se exigir que o indivíduo seja deixado em paz. [45] Assim, assinalaram a importância da liberdade, do sentimento, do sossego, da reputação e intelecto que não devem ser enquadrados na ampla noção de propriedade.[46]

A princípio, a iniciativa de escrever o artigo partiu de Warren em razão dos jornais sensacionalistas de Boston que se ocupavam com a sua vida privada e de sua família, temendo que "o que é sussurrado no closet pode vir a ser proclamado, em alta voz, a partir do telhado" [47].

Posteriormente, a privacidade passou a ser entendida como o "direito a ser deixado só" [48], caracterizado pelo isolamento da pessoa, cuja proteção se dava puramente de forma negativa, isto é, verificado por um dever de abstenção do Estado e de terceiros na

[45] Danilo Doneda assevera que: "No entanto, o artigo é inédito ao propor uma força inédita ao novo *right to privacy*, e também é mais que mero reflexo de uma época, fazendo estender sua influencia por algumas de duas características: (i) partia-se de um novo fato social, que eram as mudanças trazidas para a sociedade pelas tecnologias da informação (jornais, fotografias) e a comunicação de massa, fenômeno que se renova e continua moldando a sociedade futura; (ii) o novo 'direito à privacidade' era de natureza pessoal, e não se aproveitava da estrutura da tutela da propriedade para proteger aspectos da privacidade; (iii) no que interessa somente aos EUA, o artigo abriu o caminho para o reconhecimento (que porém ainda tardaria décadas) do direito à privacidade como um direito constitucionalmente garantido". DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006, p. 138-139.

[46] Nesse sentido: "Mais tarde, veio o reconhecimento da natureza espiritual do homem, de seus sentimentos e intelecto. Gradualmente, o escopo desses direitos legais se ampliou; e agora o direito à vida passou a significar o direito de aproveitar a vida - o direito de ser deixado em paz; o direito à liberdade assegura o exercício de amplos privilégios civis; e o termo 'propriedade' cresceu para abranger todas as formas de posses - intangíveis, assim como tangíveis" (tradução livre). Segue trecho original: "*Later, there came recognition of man's spiritual nature, of his feelings and intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, - the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term 'property' has grown to comprise every form of possession – intangible, as well as tangible*". WARREN, Samuel D. BRANDEIS, Louis D. *The right to privacy....Op.cit*. p. 193

[47] Dessa forma, Warren já percebia os embaraços causados pela tecnologia: "Recentes invenções e métodos de negócios chamam a atenção para o próximo passo que deve ser dado para a proteção da pessoa, e para garantir ao indivíduo o que o juiz Cooley chama de "direito a ser deixado só". Fotografias instantâneas e empreendimentos jornalísticos invadiram os recintos sagrados da vida privada e doméstica; e numerosos dispositivos mecânicos ameaçam fazer valer a previsão de que 'o que é sussurrado no closet pode vir a ser proclamado, em alta voz,a partir do telhado de casa'"(tradução livre). Segue trecho original: "*Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone'. Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestoc life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops*'." WARREN, Samuel D. BRANDEIS, Louis D. The right to privacy. In: *Harvard Law Review.* Cambridge: Harvard University Press, v.4, n. 5, p. 193-220, Dec.1890, p. 194.

[48] A expressão "direito a ser deixado só" foi alcunhada pela primeira vez pelo juiz norte-americano Thomas McIntyre Cooley em sua obra *A Treatise on the Law of Torts* que cuidava sobre a responsabilidade civil. Ocorre que, embora tenha mencionado o "direito a ser deixado só", afastou este da ideia de *privacy*, o que, na época, não trouxe certa notoriedade como o artigo de Warren e Brandeis o fez. A passagem que cuida da expressão é a seguinte: "O direito a uma pessoa pode ser considerado um direito de imunidade completa: ser deixado só" (tradução livre). Segue trecho original: *"The right to one´s person may be said to be a right of complete immunity: to be let alone*". COOLEY, Thomas McIntyre. *A Treatise on the law of torts*. Chicago: Callaghan, 1880, p. 29.

vida privada e na convivência familiar do individuo. Contudo, adiante, demonstrar-se-á que essa tradicional compreensão do direito à privacidade foi se modificando com o tempo.

Embora a grande contribuição de Samuel e Louis para o tema tenha sido de extrema relevância, a sua regulamentação apenas ganhou prestígio após a Segunda Guerra Mundial e, por essa razão, pode-se afirmar que se desenvolve em conjunto com o movimento humanístico, protagonizado pela dignidade da pessoa humana e pelos direitos da personalidade.

Destarte, o direito à privacidade encontra-se positivado internacionalmente *a prima facie* na Declaração Universal dos Direitos do Homem, de 1948, no art. 12 que estipula: "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 interferências ou ataques". Em seguida, outros documentos internacionais passaram a prever tal direito como na Declaração Universal dos Direitos do Homem, aprovada pela Assembléia Geral das Nações Unidas em 1948; na Convenção Européia dos Direitos do Homem em 1950; na Convenção Americana dos Direitos do Homem, conhecido como "Pacto de San José da Costa Rica" em 1969; e, por fim, mais recentemente, em 2000, na Carta dos Direitos Fundamentais da União Europeia.

A Constituição Federal brasileira também apresenta a vida privada em seu bojo, especificamente, nos termos do art. 5º, inciso X ao prever que "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", sendo um direito e garantia fundamental que constitui, por conseguinte, verdadeira clausula pétrea.

Diversas discussões sobrevieram a respeito da distinção feita entre vida privada e intimidade, descolando a discussão para qual foi a intenção do constituinte na escolha dos dois termos. Basicamente, em síntese, as seguintes correntes são perceptíveis: (i) o constituinte pretendeu tratar os termos como sinônimos para reforçar a sua tutela, pecando pelo exagero; (ii) a privacidade seria gênero, dos quais a vida privada e a intimidade são espécies; (iii) a criação da teoria das esferas ou círculos concêntricos, a qual gradua a intensidade e diferencia a vida privada, a intimidade e o segredo.[49]

Imperioso destacar a corrente que criou a teoria dos círculos concêntricos desenvolvida por Heinrich Hubmann em 1953 e Heinrich Henkel em 1957, segundo a qual

[49] Esclarece-se que não é o objetivo da presente dissertação discorrer em profundidade o conceito e as correntes que explicam a diferença entre privacidade, vida privada e intimidade, mas apenas citar a discussão para mostrar a dificuldade na delimitação e conceituação de categorias jurídicas, quiçá, na demonstração de novos direitos da personalidade.

três esferas concêntricas com diferentes graus representariam a privacidade. As esferas seriam a privacidade (*Privatsphäre*) como a camada externa que englobaria a intimidade (*Intimsphäre*) e no centro estaria o núcleo do segredo (*Geheimsphäre*). [50] A utilização das esferas teria uma utilidade para determinar o grau da penalidade que seria aplicada, se a intromissão for mais perto do núcleo do segredo, maior deveria ser a sua repreensão e mais intensa deverá ser a proteção garantida. [51]

Majoritariamente seguida pela doutrina, a teoria dos círculos concêntricos determinou que intimidade e vida privada são termos específicos em que o segundo é mais abrangente do que o primeiro, renegando a afirmação de que sejam sinônimos. A distinção entre esses termos não revela verdadeiramente uma contribuição prática uma vez que ambos são direitos da personalidade e a sua violação poderá acarretar em um dano moral.

Por outro lado, a teoria das esferas desponta a imprecisão até no que se entende por privacidade já que as fronteiras dos círculos não são bem delimitadas, sobre quais informações apropriadas ou pertencentes para cada circulo, sendo demasiadamente genérica a adoção dessa teoria.

Ora, indispensável perquirir o conceito de privacidade que aloca a discussão sobre qual interesse tal direito protege, se seria o direito de isolar-se, o direito de se resguardar contra interferências alheias, o direito ao sigilo, o direito ao controle de seus dados pessoais ou seria um direito plural que se adequa de acordo com a pluralidade de problemas distintos que se relacionam entre si. [52]

A privacidade, no sentido do direito de isolar-se, isto é, de ser deixado só partiu da noção individual de se afastar da coletividade, de terceiros. Os críticos dessa concepção entendem que essa formulação é ampla demais e que esse seria impossível, atualmente, o isolamento total do individuo tampouco saudável. [53]

---

[50] O que diferencia a concepção de Hubmann daquela desenvolvida por Henkel seria justamente o posicionamento do segredo e da intimidade. Razoável seria adotar o pensamento de Helkel para quem o segredo deve ser mais protegido do que a intimidade e estão em esferas distintas. Essa teoria foi trazida ao Brasil por Paulo José da Costa Junior, adepto de Henkel, que apresenta uma notável compreensão dos conteúdos das esferas. Segundo o autor, na esfera *Privatsphäre,* encontram-se os fatos ou comportamentos que se deseja manter longe do domínio público. Na esfera da *Intimsphäre* concentram-se as informações compartilhadas para certos indivíduos, os que sejam de confiança e próximos do titular. Por fim, na esfera *Geheimsphäre* estão as informações para as quais se busca o segredo absoluto, mas que podem até ser reveladas para as pessoas com extrema intimidade. COSTA JUNIOR, Paulo José da. *O direito de estar só: tutela penal da intimidade*. São Paulo: Ed. Revista dos Tribunais, 1970, p. 34.

[51] SZANIAWSKI, E. *Direitos de Personalidade e sua Tutela, op. cit.*, p. 361.

[52] Para aprofundamento da questão com um compilado das diversas concepções, sugere-se a leitura de LEONARDI, Marcel. *Tutela e Privacidade na Internet*. São Paulo: Saraiva, 2012.

[53] Marcel Leornardi assim pontua que: "(...) o direito a ser deixado só entende a privacidade como uma espécie de imunidade do indivíduo perante terceiros, um isolamento social, verdadeira *privação*. (...) é falho, pois é amplo demais, definido dessa maneira, seria possível concluir que qualquer conduta direcionada a

Além disso, o direito de ser deixado só que se origina da formulação de Samuel D. Warren e Louis D. Brandeis impulsionou a discussão e o desenvolvimento da privacidade no cenário mundial, porém não definiu um conceito[54]. Percebe-se que o direito de ser deixado só poderia caracterizar apenas um dos atributos da privacidade.

O direito de se resguardar contra interferências alheias decorre do direito a ser deixado só, mas compreende a privacidade como o poder do individuo de se afastar, de impedir que determinadas pessoas tenham acesso às suas informações e divulguem certas particularidades que pretende manter para si. Adota-se, nesse caso, um mínimo de interferência de outrem que seja este conhecido e autorizado pelo titular.

A dificuldade em se reconhecer se o indivíduo consegue fazer uma análise qualitativa sobre quais acessos às informações podem ou não serem realizados, inclusive, o direito de guardar para si toda e qualquer informação ainda que seja de interesse público são as principais censuras dessa concepção. Se não bastasse, estaria excluída dessa concepção a coleta, o armazenamento e o processamento automatizado de dados pessoais.

O direito ao sigilo é uma subdivisão do direito a se resguardar contra interferências alheias já que quando o individuo oculta informações ou fatos desabonadores, ele está, ao mesmo tempo, resguardando-se. Nessa acepção, renega-se as outras tentativas de conceptualização como a intimidade, a vida privada, o direito de se manter sozinho e em silêncio. O direito ao segredo e ao sigilo pressupõe que ocorra uma ocultação da informação.

Em contrapartida, nem toda atividade privada ocorre de forma oculta e nem por isso deixa de transgredir a privacidade da pessoa. Observa-se que o sigilo de correspondência, o

---

outra pessoa, quer ilícita ou não – uma agressão física, ou simplesmente pedir informações quando se está perdido, por exemplo – seria uma violação de sua privacidade". LEONARDI, Marcel. *Tutela e Privacidade na Internet*. São Paulo: Saraiva, 2012, p. 54.

[54] Solove destaca que a privacidade citada por juízes e juristas como o "direito de ser deixado só" apresenta uma conceituação vaga*: "*Para seu crédito, o artigo estava muito à frente de seu tempo, e continha flashes de insights sobre uma teoria mais robusta da privacidade. E, para ser justo, o objetivo de Warren e Brandeis não era fornecer uma concepção abrangente de privacidade, mas explorar as raízes do direito à privacidade na lei comum e explicar como ela poderia se desenvolver. O artigo foi certamente um começo profundo para o desenvolvimento de uma concepção de privacidade. No entanto, embora o direito de ser deixado só tenha sido frequentemente invocado por juízes e comentaristas, ainda permanece uma concepção bastante ampla e vaga de privacidade." (tradução livre). Segue trecho original: *"To its credit, the article was far ahead of its time, and it contained flashes of insight into a more robust theory of privacy. And to be fair, Warren and Brandeis´s aim was not to provide a comprehensive conception of privacy but instead to explore the roots of the right to privacy in the common law and explain how it could develop. The article was certainly a profound beginning toward developing a conception of privacy. However, although the right to be let alone has often been invoked by judges and commentators, it still remains a rather broad and vague conception of privacy"*. SOLOVE, Daniel J. *Understanding Privacy*. Cambridge, Massachusetts: Harvard University Press, 2009, p. 18.

sigilo bancário e o sigilo profissional caracterizam a tutela desse direito, o que, tão somente, induz a uma concepção extremamente restritiva do que seja a privacidade.

Tratando sob a perspectiva da privacidade como um direito de controlar as suas informações pessoais está o autor Alan Westin que foi o pioneiro em estipular que os indivíduos, grupos ou instituições devem ter o direito de determinar quando, como e quais as informações sobre si mesmos que podem ser comunicadas para terceiros. [55]

Nesse sentido, Arnoldo Wald também examina a privacidade como "a pretensão do individuo de decidir por si, quando, como e até que ponto uma informação pessoal pode vir a ser de conhecimento de outrem". [56] Dessa forma, tal concepção englobaria aspectos tanto do direito de se resguardar contra interferências alheias quanto do direito ao sigilo já que o controle da sua própria informação, a sua manutenção, conservação e se ela será ou não comunicada a terceiros caracterizam a essência desse conceito de privacidade.

O norte-americano Daniel Solove desenvolve em sua obra "*Understanding privacy*" um conceito plural de privacidade baseado na teoria de "*Family Resemblances*" proposta pelo filósofo austríaco Ludwig Wittgenstein. [57]

Com base nessa teoria, o método tradicional de linguagem de encontrar um núcleo ou a essência do fenômeno não é a única forma de se abordar a questão da conceituação.

O filósofo Wittgenstein propõe que a definição de algo nem sempre é uma verdade objetiva da relação entre uma palavra e a coisa à que ela se refere. Segundo ele, o significado da palavra acompanha a forma como ela é usada pela linguagem[58]. Contrariamente, pelo método tradicional, parte-se do ponto em comum, ou da essência da coisa ou fato para então conceituá-lo.

---

[55] Segundo Alan Westin: "privacidade é a reivindicação de indivíduos, grupos ou instituições para determinar por si mesmos quando, como e em que medida as informações sobre eles são comunicadas a outras pessoas". (tradução livre) Segue trecho original: "*privacy is the claim of individuals, groups, or institutions to determinate for themselves when, how, and to what extent information about them is communicated to others*". WESTIN, Alan. *Privacy and Freedom*. Nova York: Atheneum, 1967, p. 7.

[56] WALD, Arnoldo. *Curso de direito civil brasileiro: introdução e parte geral*. 7. Ed. São Paulo: Ed. Revista dos Tribunais, 1992, p. 135.

[57] Assim, Solove compreende que: "Sob minha concepção, devemos entender a privacidade como um conjunto de proteções contra uma pluralidade de problemas distintos, mas relacionados. Esses problemas não estão relacionados por um denominador comum ou elemento central. Em vez disso, cada problema tem elementos em comum com os outros, mas não necessariamente o mesmo elemento - eles compartilham semelhanças de família uns com os outros. (...) Além disso, é mais proveitoso discutir e analisar cada tipo de problema especificamente"(tradução livre). Segue trecho original: "*Under my conception, we should understand privacy as a set of protections against a plurality of distinct but related problemas. These problems are not related by common denominator or core element. Instead, each problem has elements in common with others, yet not necessarily the same element – they share family resemblances with each other. (...) Beyond that, it is more fruitful to discuss and analyze each type of problem specifically*". SOLOVE, Daniel J. *Understanding Privacy*. Cambridge, Massachusetts: Harvard University Press, 2009 p. 171-172.

[58] WITTGENSTEIN, L. *Philosophical Investigations*, 1953, trad. alem. de G.E.M. Anscombe, *Philosophische Untersuchungen*, 2a ed., Basil Blackwell Ltd., 1958, p.20.

Valendo-se da teoria de "semelhanças familiares", Solove define a privacidade como um conjunto de proteções contra grupos diferentes de problemas, mas que são relacionados entre si.[59] Tal perspectiva abrangeria uma série de questões que poderiam ser encaradas como violação à privacidade. Ocorre que a determinação do laço relacional desses acontecimentos possivelmente danosos provoca uma indeterminação real, que "parece englobar tudo, mas aparenta ser nada em si mesma" [60]. Essa indeterminação não corrobora para a identificação do que merece ser protegido como sendo objeto do direito à privacidade.

Aparentemente a vinda de teorias pluralísticas que ilustram a privacidade de forma alargada com o intuito de envolver uma série de situações da vida, originou-se pela mudança do contexto social, ou seja, a razão está na transformação do cenário da sociedade feudal para uma sociedade informacional[61].

A intensificação da sociedade informacional com o advento das novas tecnologias da informação, o crescimento e massificação das relações sociais e a realização de operações com alto fluxo de circulação de informações impulsionaram a normatização da proteção dos dados pessoais.

Daí porque diversos autores identificam uma evolução do direito à privacidade à proteção de dados pessoais[62] como sendo hoje uma tutela dinâmica, abandonando as

[59] Segundo Daniel Solove: "Privacidade, em resumo, envolve um conjunto de proteções contra um grupo de problemas diferentes, mas relacionados" (tradução livre). Segue trecho original: "*Privacy, in short, involves a cluster of protections against a group of different but related problems". Op. cit*.p. 174.

[60] LEONARDI, Marcel. *Tutela e Privacidade na Internet*. São Paulo: Saraiva, 2012, p. 47.

[61] Rodotà explica o nascimento histórico da privacidade que é associado à "desagregação da sociedade feudal, na qual os indivíduos eram todos ligados por uma complexa série de relações que se refletiam na sua própria organização de sua vida cotidiana: o isolamento era privilégio de pouquíssimos eleitos ou daqueles que, por necessidade ou opção, viviam distantes da comunidade – místicos ou monges, pastores ou bandidos". Em suma, a pessoa que tinha condições materiais para construir habitações familiares com a separação do lugar em que se habita e o lugar em que se trabalha, caracterizaria o mencionado isolamento protegido pela privacidade. Posteriormente, identificou-se no século XIX, na segunda metade, a "idade de ouro' da privacidade nos Estados Unidos, sendo este um direito da classe burguesa, sobretudo graças às transformações socioeconômicas derivadas da revolução industrial. A imprensa escrita, as fotografias instantâneas e a televisão impulsionaram para os casos de invasão da privacidade. O que, antigamente, era privilégio de poucos, voltado para a esfera individual, agora se tornou instrumento disponível a todos da população com um tratamento igualitário. Além disso, a privacidade está regulamentada em âmbito internacional, como já fora aludido. RODOTÀ, Stefano. *A vida na sociedade de vigilância: a privacidade...Op. cit*., 2008, p.26.

[62] Laura Mendes assim entende: "Nesse contexto de desenvolvimento da tecnologia de informação o direito à privacidade transforma-se para dar origem à disciplina da proteção de dados pessoais, de modo a se adaptar aos desafios impostos pelo avanço da técnica. Assim, a proteção de dados pessoais pode ser compreendida como uma dimensão do direito à privacidade, que, por consequência, partilha dos mesmos fundamentos: a tutela da personalidade e da dignidade do individuo". MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 35.

concepções unitárias tradicionais como direito de isolamento, de sigilo, de ser deixado em paz ou de ficar livre de interferências alheias.

Essa tendência se vislumbra principalmente entre os autores norte-americanos que angariam apenas a *privacy* como refúgio para encontrar soluções para os problemas jurídicos enfrentados com o uso da internet. Os autores que tratam a proteção dos dados pessoais como um dos atributos da privacidade, o fazem, muitas vezes, por importar as teorias estrangeiras para a realidade brasileira. Em suma, há uma expansão do conteúdo da *privacy*, pois naquele sistema jurídico não há a construção dos direitos da personalidade de forma ampla como acontece no Brasil.[63] Dessa forma, para tutelar o ser humano e sua projeção, eles adotam uma visão de que a privacidade seria uma "palavra-camaleão"[64], de impossível conceituação ou uma palavra "guarda-chuva"[65], absorvendo também a noção de dados pessoais, objeto que será revisitado no item subsequente.

Em verdade, a privacidade não precisa ser identificada como uma pluralidade de significados, um termo indeterminado ou como palavra-camaleão. É possível definir a sua essência através do método tradicional de linguagem e conceituação.

Apesar do artigo "*The right to privacy"* ter contribuído para o desenvolvimento da privacidade como direito autônomo, outro contorno foi lhe dado na era da internet, qual seja a facilidade na divulgação e propagação de informações pessoais e privadas, trazendo certa complexidade para o tema[66]. Por isso, a necessidade da adoção de seu aspecto negativo e positivo. Compreende-se que a privacidade seria o poder de abstenção contra interferências alheias (aspecto negativo), quanto do controle dinâmico de suas informações pessoais íntimas ou privadas (aspecto positivo).

---

[63] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006, p. 137.
[64] LEONARDI, Marcel. *Tutela e Privacidade na Internet*. São Paulo: Saraiva, 2012, p. 46.
[65] Tal expressão foi utilizada por Claudio Giacomo sobre a noção "guarda-chuva": "Se puó apparire persino intuitivo considerache che col ricorso al termine privacy si entende sempre far riferimento ad uma nozione-ombrello (...)". GIACOMO, Claudio de. *Diritto, libertà e privacy nel mondo dela comunicazione globale*. Milano: Giuffrè, 1999, p.16.
[66] Como explica Doneda: "(...) o centenário diagnóstico realizado pelos autores, então advogados em Boston, ainda é valioso, tanto que *The right to privacy* continua sendo lido e citado com invejável constância de que se trata de um trabalho circunstancialmente datado e que respondia às condições específicas de seu tempo. (...) subsiste a forte constatação de que a *privacy*, hoje, compreende algo muito mais complexo do que o isolamento ou a tranquilidade – algo de que o próprio Brandeis, tendo se ocupado do assunto posteriormente, tenha ciência.". Com a devida *vênia*, vislumbra-se, todavia, que tal aspecto negativo, de abstenção, ainda possui serventia nos dias atuais como, por exemplo, a não interferência no domicílio da pessoa e as atividades privadas que acontecem ali. Acontecimentos que violem essa prerrogativa merecem a proteção própria da privacidade. Assim, não houve uma superação e abandono da sua concepção tradicional. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006, p.10.

As esferas pública e privada, isto é, "coisas da vida pública e coisas da vida privada" [67] ainda são parâmetros para distinguir a infringência ou não da privacidade do indivíduo, englobando nessa tutela, de forma ampla, os termos vida privada, intimidade e segredo.

Necessário esclarecer que não se está confundindo esfera pública e privada com o espaço público e o privado[68]. Ora, em que pese à cena tenha ocorrido em um espaço público, o simples fato de uma pessoa ter sido fotografada na rua pública aos beijos com certo indivíduo não concede o direito do jornal de publicar essa foto. Caso os identifique, com até um "close" dos seus rostos, levando transtornos para a pessoa, essa publicação poderá infringir o direito à privacidade e à imagem desse casal.

Importante destacar que o direito à privacidade também abrange as figuras públicas que mesmo no local público poderão também obter tal proteção, apesar de divergências na jurisprudência dependendo do caso concreto.[69] Foi exatamente o que aconteceu com o caso da Daniele Cicarelli, no qual a atriz e apresentadora foi flagrada em momentos íntimos em uma praia na Espanha. O vídeo "viralizou", isto é, teve inúmeros compartilhamentos na internet, sendo que uma medida judicial bloqueou até o aplicativo *You Tube*. [70]

---

[67] Ao tratar das distinções entre vida privada, privacidade e intimidade, Danilo Doneda explica a lógica do termo vida privada ter sido valorado com a distinção entre vida pública e vida privada que advém das sociedades antigas como a romana. Todavia, discorda da utilização desse termo que intensifica a dicotomia entre interesses públicos e privados sendo um "indicativo de uma escolha ideológica que arrisca afastar a ideia de um ordenamento jurídico unitário e ordenando em torno de uma tábua axiológica comum". Por isso, prefere-se o termo privacidade ao invés de vida privada. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006, p. 109.

[68] Para delimitar a questão sobre espaço público, homem público, esfera pública e esfera privada, sugere-se: HIRATA, Alessandro. O público e o privado no direito de intimidade perante os novos desafios do direito. In: DE LIMA, Cíntia Rosa Pereira de. NUNES, Lydia Neves Bastos Telles. *Estudos avançados de direito digital.* Rio de Janeiro: Elsevier, 2014, p. 29-37.

[69] O Superior Tribunal de Justiça, certa vez, decidiu que, no caso da pessoa ainda que não fosse pública ser fotografada e divulgada foto de *topless* (mulher sem o sutiã do biquíni, ou seja, com o busto desnudo) em praia pública, por veículo de comunicação, não ocorre a violação ao direito à imagem e à privacidade da pessoa.

Ementa: DIREITO CIVIL. DIREITO DE IMAGEM. TOPLESS PRATICADO EM CENÁRIO PÚBLICO.

Não se pode cometer o delírio de, em nome do direito de privacidade, estabelecer-se uma redoma protetora em torno de uma pessoa para torná-la imune de qualquer veiculação atinente a sua imagem. Se a demandante expõe sua imagem em cenário público, não é ilícita ou indevida sua reprodução pela imprensa, uma vez que a proteção à privacidade encontra limite na própria exposição realizada. Recurso especial não conhecido. (STJ - REsp: 595600 SC 2003/0177033-2, Relator: Ministro CESAR ASFOR ROCHA, Data de Julgamento: 18/03/2004, T4 - QUARTA TURMA, Data de Publicação: DJ 13/09/2004 p. 259).

[70] **Ementa:** Pedido de antecipação de sentença por violação do direito à imagem, privacidade, intimidade e honra de pessoas fotografadas e filmadas em posições amorosas em areia e mar espanhóis - Tutela inibitória que se revela adequada para fazer cessar a exposição dos filmes e fotografias em web-sites, por ser verossímil a presunção de falta de consentimento para a publicação [art. 273, do CPC] - Interpretação do art. 461, do CPC e 12 e 21, do CC - Provimento, com cominação de multa diária de R$ 250.000,00, para inibir

A esfera privada pode assim ser considerada "como um conjunto de ações, preferências, opiniões e comportamentos pessoais sobre os quais o interessado pretende manter um controle exclusivo (...)". [71]

Nota-se que as "coisas da vida privada" merecem tutela no sentido de exclusão e controle da divulgação de informações pessoais que agridam o íntimo do ser ou aquilo que se almeje manter fora do domínio do público, razão pela qual, em sua essência, a concepção de Alan Westin e o desenvolvimento desta corrente seria o melhor caminho.

Para tanto, acalenta o posicionamento de Stefano Rodotà que compreende que o direito à privacidade gravita em "pessoa-informação-circulação-controle", diversamente do que antes se sugeria em apenas "pessoa-informação-segredo"[72].

No mesmo sentido do professor Rodotà, adota-se a concepção da professora Cíntia Rosa Pereira de Lima para quem a privacidade seria "o direito de controlar o acesso à sua vida privada e intimidade" e exemplifica o que seria uma espécie de violação a tal direito:

> Por exemplo, o Facebook viabiliza a criação de perfis nos quais são inseridas as mais variadas informações de cunho privado e íntimo. Isso não significa que o individuo abriu mão de seu direito à privacidade. Mas a tecnologia deve viabilizar que tal indivíduo possa decidir quais informações serão públicas, quais serão privadas e com quais pessoas o individuo quer compartilhar alguns aspectos de sua vida privada e íntima. [73]

Em contrapartida, a proteção de dados pessoais merece ser destacada da noção de privacidade para ganhar a sua autonomia como um direito de personalidade, razão pela qual se passa a discorrer no próximo item.

---

transgressão ao comando de abstenção. (SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. Agravo de Instrumento n.º 472.738-4. Renato Aufiero Malzoni Filho e Daniella Cicarelli Lemos versus Internet Group do Brasil Ltda., Organizações Globo de Comunicação e Youtube Inc. Relator: Des. Ênio Santarelli Zuliani. Julg. 28 set. 2006).

[71] KLEE, Antonia Espíndola Longoni. MARTINS, Guilherme Magalhães. A privacidade, a proteção dos dados e dos registros pessoais e a liberdade de expressão: algumas reflexões sobre o Marco Civil da Internet no Brasil (Lei nº 12.965/2014). In: LUCCA, Newton de. FILHO, Adalberto Simão. LIMA, Cíntia Rosa Pereira de. (coords.) *Direito & Internet III – Tomo I: Marco Civil da internet (Lei º 12.965/2014)*. São Paulo: Quartier Latin, 2015, p. 298.

[72] RODOTÀ, Stefano. *Tecnologie e diritti*. Bologna: Il Mulino, 1995, p.102.

[73] LIMA, Cíntia Rosa Pereira. *A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil*. Tese de Livre Docência apresentada junto à Faculdade de Direito de Ribeirão Preto. Ribeirão Preto: USP, 2015, p. 129.

2.2. O conceito de dados pessoais e a sua autonomia como um direito de personalidade

A confusão em se abordar a proteção dos dados pessoais como integrante do direito à privacidade vem do início do século XX, quando o Estado liberal transformou-se em *Welfare State*, ou seja, Estado do bem estar social. A coleta de informações dos cidadãos era um dos instrumentos que se valia o governo para aumentar a sua eficiência, melhorar a qualidade de vida dos habitantes e a distribuição de renda.

A partir de 1970 que, diante dos avanços tecnológicos e da facilidade na circulação de dados pessoais, despontou a preocupação sobre o controle desses dados pessoais coletados inicialmente pelo Estado.

O uso da informação pessoal por órgãos ou empresas privadas dependia de uma reestruturação do sistema, pois os custos para realizar um tratamento de dados eram elevados e dificultava tal operação[74].

Esse quase "monopólio" estatal da informação durou até o momento em que instrumentos tecnológicos viáveis fossem criados como meio de democratizar o uso de dados[75] e torná-lo acessível ao setor privado.

O aumento na capacidade de armazenamento de dados pessoais destacou-se na década de 90[76] com os computadores e o desenvolvimento da Web que possibilitaram ainda a coleta, manipulação, transmissão e retenção de uma quantidade praticamente infinita de dados. Com isso, riscos também foram criados como o rastreamento das informações por meio de mecanismos como *cookies* e o envio de e-mails *spams*, sem o consentimento do usuário, entre outros inúmeros exemplos.

Muito foi dito sobre a invasão da pessoa, especialmente, no que diz respeito à coleta dos seus dados pessoais, o que abriu as portas para a corrente desenvolvida por Alan

[74] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006, p. 15.

[75] É o que entende de: "Desta forma, a importância da informação aumenta na medida em que a tecnologia passa a fornecer meios para torna-la útil a um custo razoável". DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006, p. 15

[76] Em sua tese de livre docência, a professora Cíntia Rosa desenvolveu todo um arcabouço da proteção de dados pessoais e constatou uma mudança com o advento dos computadores: "(...) porém, a partir da década de 90 outro fator chamou a atenção de toda a comunidade internacional, qual seja: o grande aumento na capacidade de armazenamento de dados pessoais de maneira autônoma. Em razão dessas novas tecnologias digitais (mais baratas e com maior capacidade de armazenamento), há um acúmulo de informações coletadas a todo momento e armazenadas, além de o acesso a tais informações por qualquer pessoa de maneira rápida e cômoda". LIMA, Cíntia Rosa Pereira. *A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil*. Tese de Livre Docência apresentada junto à Faculdade de Direito de Ribeirão Preto. Ribeirão Preto: USP, 2015, p. 42.

Westin e pela jurisprudência norte-americana sobre a privacidade como o controle das informações pessoais, como aludido anteriormente.

Acontece que, por reclamar mecanismos específicos de tutela, a proteção de dados pessoais deve ser observada sobre o viés que reclama autonomia em relação ao direito à privacidade.

A internet promoveu uma maior interação entre as pessoas e a facilidade na divulgação de acontecimentos pessoais desabonadores ou não tais como a embriaguez, o uso de substâncias ilícitas, quais amores foram correspondidos, vídeos das pessoas dançando e cantando ainda enquanto crianças, fotos comprometedoras, entre outros. Se não bastasse, enfatizou a captação e o armazenamento de dados pessoais como nome, estado civil, filiação, raça, sexo, endereço, tipo sanguíneo e atividade profissional disponíveis em banco de dados. Apesar da relação que se possa identificar entre esses acontecimentos pessoais e os dados coletados do indivíduo, garante-se que a privacidade e a proteção aos dados pessoais são tutelas diferenciadas e cada qual com conteúdo próprio.

A professora Cíntia Rosa Pereira de Lima exemplifica bem a relação do direito à privacidade e do direito à proteção de dados pessoais perante uma perspectiva relacional:

> (...) por exemplo, o paciente portador de uma doença grave e sexualmente transmissível como a AIDS tem o direito de não ter tal informação divulgada no seu ambiente de trabalho (não havendo justificativa para tal divulgação, o que seria apenas com condão discriminatório). No entanto, este mesmo paciente pode ter tal informação comunicada e compartilhada entre autoridades sanitárias competentes para fins de controle da doença.[77]

Em outras palavras, a divulgação indevida da doença do paciente no ambiente de trabalho ou até mesmo na internet, caracterizaria uma afronta à sua vida privada e também à proteção dos seus dados pessoais devassados como nome ou imagem. O compartilhamento dos dados pessoais entre autoridades sanitárias, caracterizaria um tratamento para fins de interesse público, sendo portanto permitido e encontra-se no campo da proteção de dados pessoais.

[77] LIMA, Cíntia Rosa Pereira. *A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil*. Tese de Livre Docência apresentada junto à Faculdade de Direito de Ribeirão Preto. Ribeirão Preto: USP, 2015, p. 129.

Como bem exposto, a privacidade apresenta a esfera privada como parâmetro e se define pelo poder de controlar o acesso às suas informações pessoais (aspecto positivo) e, ao mesmo tempo, de se resguardar contra interferências alheias (aspecto negativo).

Por outro lado, a proteção aos dados pessoais não leva em consideração a esfera privada da pessoa, mas evidencia uma tutela dinâmica de controlar a circulação de dados que se inicia com a coleta e permanece até com a circulação e armazenamento ainda que esses dados estejam à disposição do público[78]. A dicotomia entre público e privado não é capaz de satisfazer a tutela necessária dos dados pessoais já que, por exemplo, um dado pessoal como a informação de inadimplência do titular nos cadastros dos órgãos de proteção ao crédito, plataforma de acesso público, cujo valor da dívida divulgado esteja incorreto, o devedor possui o direito de pleitear a correção e retificação de tal dado com a finalidade de buscar a exatidão da informação ali contida.

O direito à proteção aos dados pessoais pode ser conceituado como o direito de uma pessoa física ou jurídica, individualizada ou individualizável, de controlar seus dados pessoais, corrigi-los ou apagá-los nos termos da lei. [79] O parâmetro para se averiguar se incide tal proteção é justamente a estipulação do que venha a ser um dado pessoal.

Para tanto, mister conhecer o conceito de dado pessoal que também não é um termo pacificado na doutrina. Necessário ressaltar que no Brasil, ainda não há uma legislação própria e específica para o tema, embora projetos de lei estão em debate junto ao Poder Legislativo, problemática que será abordada em momento oportuno ainda neste capítulo.

Preliminarmente, por sua vez, urge a máxima que informação e dados não se confundem. Embora se reconheça que há uma certa promiscuidade[80] na utilização dos termos "informação" e "dado", observável é a diferença entre eles. Até porque

[78] Nesse sentido, Cíntia explica que: "Em suma, o objeto do direito à privacidade é diverso do objeto do direito à proteção dos dados pessoais. O primeiro é assegurar o resguardo de parcela de sua vida privada; o segundo, por sua vez, é proteger os dados e as informações (ainda que de conhecimento público) de serem objeto de tratamento em desacordo com as regras e códigos de conduta". LIMA, Cíntia Rosa Pereira. *A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil*. Tese de Livre Docência apresentada junto à Faculdade de Direito de Ribeirão Preto. Ribeirão Preto: USP, 2015, p. 88-89.

[79] Conceito proposto pela professora Cíntia Rosa. LIMA, Cíntia Rosa Pereira. *A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil*. Tese de Livre Docência apresentada junto à Faculdade de Direito de Ribeirão Preto. Ribeirão Preto: USP, 2015, p.111.

[80] Assim discorre Danilo Doneda: "Em relação à utilização dos termos 'informação' e 'dado', é necessário notar preliminarmente que o conteúdo de ambos os vocábulos se sobrepõe em várias circunstancias, o que justifica uma certa promiscuidade na sua utilização. Ambos os termos servem a representar um fato, um determinado aspecto de uma realidade. Não obstante, cada uma carrega um peso particular a ser levado em conta". DONEDA, Danilo. *Da privacidade à proteção de dados pessoais* Op. cit., p. 152

etimologicamente "dado"[81] seria uma informação em seu estado natural, latente, como se fosse um estágio anterior à informação. Considera-se "informação" tanto a representação do que se extrai do dado quanto o que reduz o estado de incerteza, tendo em vista o processo cognitivo.[82]

Dados pessoais, como sugestão do próprio nome, são aqueles que se referem a qualquer pessoa singular identificada ou identificável como, por exemplo, o nome, profissão, fotos, vídeos, registros de acessos, registros de consumo e endereço. Constituem então um prolongamento da própria pessoa, cuja afronta violaria a dignidade da pessoa humana e o seu livre desenvolvimento pessoal.

Em contrapartida, não seria dado pessoal, por exclusão, os dados anônimos:

> Quando os dados não permitam identificar uma pessoa, mesmo que sejam dados que se referem, em abstracto, a pessoas, não são dados pessoais: é o caso dos dados estatísticos que não permitem "voltar" a saber a quem se referiam. Constituirão dados pessoais, toda informação, seja ela numérica, alfabética, gráfica, fotográfica, acústica ou de qualquer outro tipo, relativa a uma pessoa física identificada ou identificável. [83]

Quando um dado refere-se a uma pessoa indeterminada estar-se-á perante um dado "anônimo" como é o caso dos dados de uma coletividade de pessoas relativos ao fluxo telefônico de uma determinada empresa de telecomunicações, sem que haja a identificação pessoal do emissor e do receptador das chamadas. [84]

Mesmo que identifique certa pessoa, Danilo Doneda esclarece que as opiniões alheias sobre ela e a sua produção intelectual, em si considerada, não é um dado ou

---

[81] Segundo a professora Cíntia Rosa: "O vocábulo 'dado' tem origem etimológica na palavra 'datum' que, por sua vez, é declinação da palavra 'dare'. Esta última tem o sentido de algo ser entregue, passado, ministrado. Desta forma, a sua origem etimológica reforça a ideia de que 'dado' é uma informação em seu estado natural, 'entregue' pelos sentidos sem qualquer reforço de interpretação lógico-racional, pertinente à informação". LIMA, Cíntia Rosa Pereira. *A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil*. Tese de Livre Docência apresentada junto à Faculdade de Direito de Ribeirão Preto. Ribeirão Preto: USP, 2015, p. 89.

[82] Mais uma vez, Doneda esclarece que: "Assim, o 'dado' apresenta conotação um pouco mais primitiva e fragmentada (...); o dado estaria associado a uma espécie de 'pré-informação', anterior à interpretação e ao processo de elaboração. A informação, por usa vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição, e mesmo nos efeitos que esta pode apresentar para o seu receptor. Sem aludir ao significado ou conteúdo em si, na informação já se pressupõe uma fase inicial de depuração de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido de uma redução do estado de incerteza. A doutrina não raro trata estes dois termos indistintamente". DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006, p. 152.

[83] CASTRO, Catarina Sarmento. *Direito da Informática, Privacidade e Dados Pessoais.* Coimbra: Almedina, 2005, p. 71.

[84] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Op. cit.,, p. 157.

informação pessoal (embora, no caso da produção intelectual, a sua autoria o seja).[85] Ocorre que há autores que incluem tais dados na categoria de dados pessoais observados, como será exposto no tópico a respeito da taxonomia de dados pessoais.

O processo que retira a identificação da informação a qual a pessoa se refere chama-se "anonimização" de dados pessoais. Alguns autores criticam a classificação de dados anônimos, uma vez que o cruzamento e agregação desses dados pode vir a identificar uma pessoa, o que significaria uma "re-identificação".

Para elucidar o óbvio, a re-identificação acarretaria os mesmos benefícios que os dados pessoais na perspectiva do mercado de consumo. Ora, quanto mais individualizado o dado, maior será o conhecimento que se tem sobre as preferências e características da pessoa e maior será o interesse do Estado e de expressivas corporações.

Principalmente as grandes empresas se valem da argumentação de que os dados anônimos não representam potencial de risco para os indivíduos e, por isso, seria dispensável qualquer proteção legal. Isto porque, os reais motivos para a coleta de dados seria o poder da informação voltado para segmentar produtos e serviços, reduzir os riscos de perdas, aumentar a eficiência da empresa e, com isso, expandir a eficácia da publicidade destinada aos consumidores, o que importaria uma avulta lucratividade e consequente monopólio do mercado.

Além da classificação de dados anônimos, há os dados sensíveis que seriam, por assim se dizer, uma subclassificação dos dados pessoais, isto é, necessitam de tratamento e regulamentação diferenciada diante da sua extrema vulnerabilidade em comparação aos outros dados pessoais. São conhecidos como dados sensíveis aqueles que tocam os basilares aspectos da vida como, por exemplo, preferência sexual, ideologias, religião, crenças, associação sindical e estado de saúde. O grande potencial discriminatório fez com que em alguns países fossem editadas leis mais rígidas para tal subcategoria de dados pessoais.[86]

[85]Idem, ibidem, p.156.

[86] Na própria Constituição Portuguesa há expressa proibição para o tratamento de dados pessoais sensíveis em seu artigo 35º: "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". (Grifo nosso). PORTUGAL. Constituição da República Portuguesa de 1976. Disponível em: https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx. Acesso em: 31.11.2017.

Na era do *Big Data*[87], ferramenta tecnológica capaz de prever comportamentos, estruturar dados para se criar um perfil (*profiling*)[88], identificar individualidades e estabelecer estatísticas do que pode acontecer no futuro, entre outras funções, leva ao reforço da proteção de dados pessoais. Com a utilização de tal ferramenta, a transformação de dados pessoais em sensíveis passa a ser uma realidade acessível e ameaçadora. Acontece que, por exemplo, obter conhecimento da doença que o indivíduo possui ou que poderá adquirir através de seus hábitos alimentares ou fatores genéticos revela o alto poder discriminatório que as empresas como seguradoras de vida ou planos de saúde podem fazer o seu uso e aumentar os valores da contratação. Como dito, as combinações de aspectos da individualidade, da união de vários dados comuns, poderá surgir uma informação sensível. Por essa razão, o tratamento de dados sensíveis é até proibido em alguns lugares do mundo como na Europa[89], ressalvadas raras exceções.

Para fins regulatórios, todo dado que não contenha a adjetivação "pessoal" deixa de ter a qualidade de ser um verdadeiro prolongamento da pessoa, o que não convém para integrar um sistema protetivo.

Isso acontece justamente porque o direito à proteção dos dados pessoais é um direito autônomo de personalidade. Embora o Código Civil brasileiro tenha elencado apenas certos direitos especiais que são direito ao nome, direito à honra, direito à imagem,

---

[87] MAYER-SCHÖNBERGER, Victor. CUKIER, Kenneth. *Big Data: a revolution that will transform how we live, work, and think.* Boston: Houghton Mifflin Harcourt Publishing Company, 2013, p. 13 e 170/197.

[88] O *Profiling* seria uma técnica utilizada para "elaboração de perfis de comportamento de uma pessoa a partir de informações que ela disponibiliza ou que são colhidas", isto é, dados fornecidos e obervados. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006, p. 173.

[89] A regra, pela Diretiva nº 95/46/CE, se dá pela possibilidade de proibição do tratamento de dados sensíveis em seu art. 8º, salvo algumas exceções. Cada membro da União Europeia transpôs em sua legislação os mecanismos adequados de proteção a essa categoria de dados, por exemplo, a Itália que, atualmente, opera em vigor o *Codice della Privacy*, estabeleceu em seu art. 4º sobre a definição dos dados sensíveis e no art. 26º o tratamento de dados pessoais por particulares. Segundo este artigo, os dados pessoais sensíveis apenas podem ser armazenados por particulares se o responsável pela tratamento obter o consentimento do titular de dados e uma autorização da autoridade *Garante* de proteção de dados pessoais, salvo três raríssimas exceções. É o que se compreende do seguinte trecho: "Art. 26. Garantias de dados sensíveis 1. Os dados sensíveis só poderão ser tratados com o consentimento por escrito do interessado e com a prévia autorização da autoridade garante, observadas as condições e limites estabelecidos por este código, bem como por lei e dos regulamentos. (...) "; "Art. 4. Definições 1. Para os fins deste código, queremos dizer: (...) d) "dados sensíveis", dados pessoais adequados para revelar a origem racial e étnica, crenças religiosas, filosóficas ou outras, opiniões políticas, participação de partidos, sindicatos, associações ou organizações de natureza religiosa, filosófica, política ou sindical, bem como dados pessoais adequados para revelar o estado de saúde e vida sexual". (tradução livre). Trecho original da lei: "***Art. 26. Garanzie per i dati sensibili*** *1. I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti. (...)*"; "***Art. 4. Definizioni*** *1. Ai fini del presente codice si intende per: (...)d) "dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;*".

direito ao corpo e direito à privacidade como direitos da personalidade, não quer dizer que o rol dos artigos 11 a 21 seja estanque.

Por força da aplicação direta da cláusula da dignidade da pessoa humana contida no art. 1º, III, da Constituição Federal brasileira, outros direitos podem ser reconhecidos uma vez que não há uma proibição expressa. Desse modo, inegável que os dados pessoais sejam um prolongamento da pessoa, identificando-a, cuja utilização incorreta provoca consequências para a sua vida. Nessa senda, cabe ao Direito intervir na relação entre o indivíduo e o responsável pelo tratamento desses dados, pois a exploração dos dados pessoais e a transformação da pessoa em "coisa" significa um fato relevante para o meio jurídico.

2.3. A autodeterminação informacional e a Lei de Recenseamento Alemã de 1983

Atualmente, a proteção de dados pessoais possui como fundamento a autodeterminação informacional caracterizada pelo fato do próprio indivíduo ter e manter o controle sobre as suas informações pessoais.

O termo "autodeterminação informacional" ficou assim conhecido a partir de um julgamento do Tribunal Constitucional Alemão, no ano de 1983, sobre a "Lei de Recenseamento de População, Profissão, Moradia e Trabalho" que foi considerada parcialmente inconstitucional com base nos artigos da lei fundamental que disciplinavam a dignidade humana e o livre desenvolvimento da personalidade [90] Tal lei autorizava a coleta de dados atinentes ao domicilio, profissão e renda da população com o objetivo de efetuar um levantamento para reunir dados sobre o crescimento populacional, densidade demográfica e social; a atividades econômicas.[91]

A Lei do Censo de 1983 listava os dados e determinava ainda quais eram os cidadãos que estavam obrigados a fornecer tais informações.

Outrossim, o § 9 desta lei autorizava a comparação dos dados fornecidos com os dados armazenados em registros públicos para o fim de aferir a veracidade das

[90] MARTINS, Leonardo. *Introdução à jurisprudência do Tribunal Constitucional Alemão*. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Organização e introdução: Leornado Martins. Trad. Beatriz Henning et al. Prefácio: Jan Woischnik. Montevidéu: Fundação Konrad Adenauer, 2005, p. 233-245.
[91] Idem, ibidem, p. 234.

informações coletadas e também possibilitava o envio desses dados que eram tornados anônimos a repartições públicas federais, estaduais e municipais.

Várias Reclamações Constitucionais foram ajuizadas contra a lei com o fundamento de que infringiria alguns direitos fundamentais, especialmente, o direito ao livre desenvolvimento da personalidade. O Tribunal Constitucional Federal alemão considerou que as condições processuais estavam presentes, pois atingiam diretamente os reclamantes. No mérito, entendeu que os dispositivos sobre comparação de dados, a sua transmissão e a competência de troca eram nulos.

Imperioso notar que, embora a Lei Fundamental alemã (*Grundgesetz*) não abarcava a proteção de dados pessoais como um direito autônomo, o Tribunal Constitucional Alemão fundamentou-se no livre desenvolvimento da personalidade para constituir o que nomeou de autodeterminação informativa, sendo este "o poder do indivíduo de decidir ele mesmo, em princípio, sobre a exibição e o uso de seus dados pessoais". [92] [93]

O moderno processamento de dados automatizado possui uma enorme capacidade de armazenamento praticamente ilimitado, com acesso de todos em qualquer tempo e lugar, razão pela qual se necessita de uma proteção intensa dos dados pessoais. O cidadão deve ter a ciência para o que e para quem os seus dados pessoais serão transmitidos, até para conferir a exatidão deles. [94]

A gestão e capacidade de processamento de dados pessoais que antes era conduzido manualmente para a evolução do processamento eletrônico estendeu as possibilidades de vazamento de dados e a sua utilização distante da finalidade de estatística proposta pela Lei

---

[92] MARTINS, Leonardo. *Introdução à jurisprudência do Tribunal Constitucional Alemão*. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Organização e introdução: Leornado Martins. Trad. Beatriz Henning et al. Prefácio: Jan Woischnik. Montevidéu: Fundação Konrad Adenauer, 2005, p. 234.

[93] No caso da Lei do Censo alemã, os julgadores decidiram que "o livre desenvolvimento da personalidade pressupõe, sob as modernas condições do processamento de dados, a proteção do indivíduo contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais. Esta proteção, portanto, é abrangida pelo direito fundamental do Art. 2 I c. c. Art. 1 I GG. O direito fundamental garante o poder do cidadão de determinar em princípio ele mesmo sobre a exibição e o uso de seus dados pessoais". *Idem*, *Ibidem*, p. 238.

[94] Nesse sentido, a decisão do Tribunal Constitucional alemão expressamente aludiu: "Esse poder necessita, sob as condições atuais e futuras do processamento automático de dados, de uma proteção especialmente intensa. Ele está ameaçado, sobretudo porque em processos decisórios não se precisa mais lançar mão, como antigamente, de fichas e pastas compostos manualmente. Hoje, com ajuda do processamento eletrônico de dados, informações detalhadas sobre relações pessoais ou objetivas de uma pessoa determinada ou determinável (dados relativos à pessoa [cf. § 2 I BDSG – Lei Federal sobre a Proteção de Dados Pessoais]) podem ser, do ponto de vista técnico, ilimitadamente armazenados e consultados a qualquer momento, a qualquer distância e em segundos. Além disso, podem ser combinados, sobretudo na estruturação de sistemas de informação integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou quase, sem que a pessoa atingida possa controlar suficientemente sua exatidão e seu uso." *Idem*, *Ibidem*, p. 237.

de recenseamento. A transmissão de dados pessoais para outras repartições públicas e as combinações de dados pessoais distanciavam-se do objetivo principal de implantar "execuções administrativas" como benefícios fiscais ou tributação. Desse modo, "ampliaram-se, de maneira até então desconhecida, as possibilidades de consulta e influência que podem atuar sobre o comportamento do indivíduo em função da pressão psíquica causada pela participação pública em suas informações privadas". [95]

O tratamento de dados pelas autoridades públicas com o seu respectivo armazenamento como "pessoal", sem que se transformassem anônimo, acarretaria um grande risco e ameaça para o desenvolvimento da pessoa, pela utilização deles por terceiros com finalidade diversa para qual foi coletado.

O mesmo pode-se infirmar em relação aos dados sensíveis uma vez que a aglomeração dos dados pessoais poderia resultar na obtenção de informações íntimas, como por exemplo, se certa pessoa faz uso de drogas. Tal informação ficaria armazenada de forma ilimitada como pessoal e exposta a todo tipo de risco. Por isso, o Tribunal Alemão alertou que não existem dados insignificantes[96] perante o momento tecnológico, o que revela a importância do processo de "anonimização" de dados e a utilização dos mesmos[97]. De tal modo, o legislador deveria ter definido precisamente a finalidade do seu uso sem que isso acarretasse em ameaça ou constrangimento ao indivíduo. [98]

[95] *Idem, ibidem.*

[96] Conforme, pode-se observar: "Neste mister não se pode apenas condicionar o tipo de dados [que podem ser levantados, transmitidos etc.]. Decisivos são sua utilidade e possibilidade de uso. Estas dependem, por um lado, da finalidade a que serve a estatística e, por outro lado, das possibilidades de ligação e processamento próprias da tecnologia de informação. Com isso, um dado em si insignificante pode adquirir um novo valor: desse modo, não existem mais dados "insignificantes" no contexto do processamento eletrônico de dados. *Idem, Ibidem*, p. 239.

[97] Extraído dos fundamentos da mencionada decisão: "O fato de informações dizerem respeito a processos íntimos não decide por si só se elas são sensíveis ou não. É muito mais necessário o conhecimento do contexto de utilização, para que se constate a importância do dado em termos de direito da personalidade: Só quando existe clareza sobre a finalidade para a qual os dados são solicitados e quais são as possibilidades de uso e ligação [destes com outros] que existem, pode-se saber se a restrição do direito de autodeterminação da informação (no caso) é admissível. Deve-se distinguir entre dados referentes à pessoa, que são levantados e manipulados de forma individualizada e não anônima (v. item "a" abaixo), e aqueles que são destinados a fins estatísticos (v. item "b" abaixo)". *Idem, ibidem.*

[98] De acordo com o seguinte trecho: "A obrigação de fornecer dados pessoais pressupõe que o legislador defina a finalidade de uso por área e de forma precisa, e que os dados sejam adequados e necessários para essa finalidade. Com isso não seria compatível a armazenagem de dados reunidos, não anônimos, para fins indeterminados ou ainda indetermináveis. Todas as autoridades que reúnem dados pessoais para cumprir suas tarefas devem se restringir ao mínimo indispensável para alcançar seu objetivo definido". *Idem*, Ibidem, p. 240.

Na decisão de 1983, frisou-se ainda a questão da confiança do cidadão como pressuposto essencial para concretizar a finalidade estatística de recenseamento da população pelo Estado. [99]

Por outro lado, alegou-se que a autodeterminação informacional como uma faculdade do direito à proteção de dados pessoais não é algo absoluto, ilimitado, mas pelo contrário, encontraria a sua barreira na coletividade, "no interesse geral predominante"[100], isto é, no interesse público.

Por consequência, a autodeterminação informacional proposta pela Corte alemã abriu os olhos do mundo para a proteção de dados pessoais a fim de que o "indivíduo não se torne um simples objeto"[101].

Considerando o contexto que se estabeleceu a autodeterminação informacional, parabeniza-se os nobres julgadores que criaram as balizas para a teoria da proteção de dados pessoais e determinaram que se trata de um direito fundamental subjetivo com status "constitucional", merecendo ser observado pelos legisladores alemãs.

Como se observou, a concepção de autodeterminação informativa ratifica um adequado tratamento para a matéria de dados pessoais destacado do que se venha a compreender como privacidade. Hoje, prontamente, o direito à proteção de dados pessoais é um direito fundamental autônomo. [102]

---

[99] Ao comparar a Lei de Recenseamento de 1983 com a antiga de 1950, os julgadores enfatizaram a importância da finalidade e transparência no tratamento de dados pessoais: "Para que a estatística oficial cumpra seu papel, é necessário o maior grau possível de exatidão e veracidade dos dados coletados. Esse objetivo somente será atingido se for criada no cidadão, que é obrigado a fornecer informações, a confiança necessária na proteção de seus dados coletados para fins estatísticos, sem a qual não se pode contar com sua prontidão em fornecer dados verdadeiros (correta a fundamentação do governo federal sobre o projeto da Lei do Recenseamento de 1950, cf. *BTDrucks*. 1/1982, p. 20 sobre o § 10)". *Idem, Ibidem,* p. 243.

[100] Todavia, assevera-se na decisão que: "Esse direito à 'autodeterminação sobre a informação' não é garantido ilimitadamente. O indivíduo não tem um direito no sentido de um domínio absoluto, ilimitado, sobre "seus" dados; ele é muito mais uma personalidade em desenvolvimento, dependente da comunicação, dentro da comunidade social. A informação, também quando ela é relativa à pessoa, representa um recorte da realidade social que não pode ser associado exclusivamente ao indivíduo atingido [por causa da demanda de informações do Estado ou de terceiros]. (...) Por isso, em princípio o indivíduo tem que aceitar limitações de seu direito à autodeterminação sobre a informação em favor do interesse geral predominante". *Idem, Ibidem,* p. 238.

[101] Nesse sentido: "Se a diversidade das possibilidades de uso e associação de dados não é determinável antecipadamente, pela natureza da estatística, são necessários limites compensatórios no levantamento e no uso da informação dentro do sistema de informação. É necessário criar condições de manipulação claramente definidas que garantam que o indivíduo não se torne um simples objeto de informação, no contexto de um levantamento e manipulação automáticos dos dados relativos à sua pessoa". *Idem, Ibidem,* p. 241.

[102] LIMBERGER, Têmis. Proteção dos dados pessoais e comércio eletrônico: os desafios do século XXI. *Revista de Direito do Consumidor.* São Paulo, ano 17, nº 65, p. 225, jul./set. 2008.

2.4. Uma taxonomia para o direito à proteção dos dados pessoais

A taxonomia para a proteção dos dados pessoais adotada nesta dissertação foi baseada na origem dos dados e desenvolvida por Martin Abrams, diretor executivo da *Information Accountability Foundation* (AFA)[103], que conta com mais de 35 anos de experiência e estudos sobre a proteção de dados pessoais no mundo. [104]

Para tanto, analisou-se o artigo "*The Marco Civil and Beyond: Privacy Governance For The Future*" escrito por Martin que apresentou a sua visão pessoal de uma nova taxonomia para proporcionar um maior controle de dados pessoais quando estes estiverem *online*, ou seja, na internet, bem como para incentivar discussões sobre o que constituiria uma efetiva, prática e equilibrada governança da proteção de dados pessoais no Brasil.[105]

Esclarece-se que o autor Martin pontuou que no estudo intitulado de "*Exploring the Economics of Personal Data*"[106], da OECD[107], realizado em 2013, também há outras taxonomias de dados pessoais como a de Bruce Schneier que classificou os dados a partir da interação nas redes sociais, porém a OECD elegeu uma taxonomia com fundamento no conceito de coleta de dados, emprestado do Fórum Econômico Mundial[108]. Nota-se que, ao

[103] Informações sobre a AFA e o trabalho desempenhado pela organização, basta acessar o seu site: http://informationaccountability.org/. Acesso em: 03.11.2017.

[104] Esclarece-se que, em pesquisa sobre o tema, não foram localizadas muitas classificações de proteção de dados pessoais propostas, porém optou-se pela estudo de Martin uma vez que a taxonomia proposta por ele, aborda a origem dos dados pessoais com a exposição de exemplos e o nível de proteção que deveria ser adotado por meio de leis e políticas públicas. Assim, a escolha adveio da facilidade em se visualizar toda a problemática que o tratamento de dados pessoais poderia acarretar.

[105] ABRAMS, Martin. *The Marco Civil and Beyond: Privacy Governance for the Future*. In: ARTESE, Gustavo (coord.). *Marco Civil da Internet: análise jurídica sob uma perspectiva empresarial*. São Paulo: Quartier, 2015, p. 98.

[106] OECD. *Exploring the Economics of Personal Data: a survey of methodologies for measuring monetary value*. In: The OECD Digital Economy Papers. (nº 220). Publicado em 02 de abril de 2013. Disponível em: <http://www.oecd-ilibrary.org/docserver/download/5k486qtxldmq-en.pdf?expires=1515318608&id=id&accname=guest&checksum=A1A7FF2A4D6C418E522518EBE4906E81>. Acesso em: 04.11.2017.

[107] A sigla OCDE significa Organização de Cooperação e de Desenvolvimento Econômico que foi criada em 1961. É uma organização internacional composta por 35 países e com sede em Paris, na França. A OCDE tem por objetivo promover políticas que visem o desenvolvimento econômico e o bem-estar social de pessoas por todo o mundo. Disponível em: http://www.oecd.org/about/. Acesso em: 02.11.2017.

[108] Nesse sentido, Martin Abrams desenvolveu essa taxonomia e a publicou, primeiramente, no site da *Information Accountabulity Foundation*, em 2014. Para tanto, explicou que o *paper* da OECD também trouxe outras taxonomias: "A origem não é a única lente ou critério que se pode usar para classificar os dados. Os Documentos da Economia Digital da OCDE No. 220, "Explorando a Economia dos Dados Pessoais", contêm uma taxonomia de dados baseada no conceito de coleta de dados emprestado do Fórum Econômico Mundial. A taxonomia analisa os dados de uma perspectiva de coleção relacionada a um ciclo de vida de dados. O documento da OCDE também faz referência à "Taxonomia de dados de redes sociais" de Bruce Schneier, que foi revisada no blog de Schneier em 10 de agosto de 2010. A taxonomia de Schneier faz um excelente trabalho ao catalogar dados sob a perspectiva das redes sociais. O documento da OCDE também faz referência a classificações baseadas na natureza da relação do indivíduo com o colecionador." (tradução

analisar os dois estudos, ainda que Martin não tenha feito referência expressa, pode-se considerar que ele se inspirou nesse *paper* da OECD para desenvolver a sua original taxonomia.

De início, os conceitos chaves de privacidade e proteção de dados pessoais não são facetas do mesmo fenômeno. Como dito anteriormente, principalmente a Declaração Universal de Direitos Humanos e a Convenção Europeia de Direitos do Homem definem a privacidade como o direito de respeito à vida privada e à convivência familiar, à inviolabilidade de sua casa e de correspondência. Por outro lado, o conceito de proteção dos dados pessoais é mais amplo do que esse conceito tradicional de privacidade, afirmação da qual o autor Martin também compartilha.[109]

Por outro lado, Martin adota uma visão de que proteção de dados pessoais corresponderia ou seria tratada no referido artigo como sendo uma "privacidade informativa". Para ele, existiriam dois tipos de privacidade que são denominadas de privacidade informativa e privacidade física.

A privacidade física se relacionaria com o que os outros podem ver e ouvir sobre "nós". Por exemplo, uma pessoa que através de uma câmera nos assiste enquanto trocamos de roupa, configura-se um abuso à privacidade física. Em verdade, a pessoa está nos assistindo enquanto não esperamos que ocorra. Por outro lado, quando essas imagens capturadas pela câmera são digitalizadas e armazenadas para posterior processamento na internet, configura-se a violação à privacidade informacional[110], tema que será tratado em seu estudo.

---

livre). Segue trecho original: "*Origin is not the only lens one might use to classify data. The OECD Digital Economy Papers No. 220, 'Exploring the Economics of Personal Data,' contains a taxonomy of data based on the concept of data collection borrowed from the World Economic Forum. The taxonomy looks at the data from a collection perspective related to a data lifecycle. The OECD paper also references Bruce Schneier's 'Taxonomy of Social Networking Data' that was revised in Schneier's blog on 10 August, 2010. Schneier's taxonomy does an excellent job of cataloging data from the perspective of social networking. The OECD paper also references classifications based on the nature of the relationship of the individual to the collector*". ABRAMS, Martin. *The Origins of Personal Data and its Implications For Governance*. The Information Accountability Foundation, 2014. Disponível em: <http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf>. Acesso em: 04.11.2017.

[109] ABRAMS, Martin. *The Marco Civil and Beyond: Privacy Governance for the Future*. In: ARTESE, Gustavo (coord.). *Marco Civil da Internet: análise jurídica sob uma perspectiva empresarial*. São Paulo: Quartier, 2015, p. 100-101.

[110] Os exemplos citados são traduções do autor norte-americano Martin Abrams, diretor executivo da *Information Accountability Foundation*, que, ao que tudo indica, não trata a proteção de dados pessoais como um direito autônomo, mas sim como um sistema para prevenir o processamento inadequado de dados pessoais. Desse forma, em seu artigo que será explorado neste tópico, o autor adota a noção de privacidade informativa para tratar da "privacy". Compreende que o conceito de privacidade informativa seria: "(...) por privacidade, quero dizer a ausência do processamento inadequado de informação que pertence a uma pessoa identificável. Pode ser propriamente definida por leis, regulamentos, acordos, contratos e até expectativas bem estabelecidas. Por exemplo, usar minhas informações de saúde para me discriminar em termos de

Em análise ao exemplo de Martin, é primordial abstrair uma certa ressalva a respeito da nomenclatura e de se tratarem de categorias jurídicas diferenciadas, de acordo com o que fizemos no tópico 2.1 e 2.2. No primeiro momento, inegável que uma pessoa que assiste à outra trocando de roupa no recôndito de seu quarto comete uma violação à privacidade (aspecto negativo da privacidade). No segundo momento, verifica-se que o processamento indevido de imagens também levou à violação do direito à privacidade, pois a divulgação do conteúdo com a nudez da pessoa, sem o seu consentimento, pode vir a ser considerado constrangedor e infringir a sua esfera pessoal (aspecto positivo da privacidade). Além disso, concomitantemente, ocorreu a violação dos dados pessoais, pois estes identificam a pessoa retratada e a divulgação das imagens com a sua respectiva circulação dificultaria o desenvolvimento da sua personalidade (aspecto subjetivo da proteção dos dados pessoais). Os provedores de aplicação que disponibilizarem as imagens para terceiros poderão obter lucro com a quantidade de acessos, o que impulsionaria ainda mais a sua circulação e o seu armazenamento. A lucratividade do provedor advinda de anúncios publicitários e da coleta dos dados de registro de navegação dos usuários que acessariam tal conteúdo refletirá no aumento do poder econômico informacional, o que implicaria ainda, partindo da visão concorrencial, em danos para toda a coletividade (aspecto relacional da proteção dos dados pessoais). Por isto, o exemplo das imagens com cenas de nudez, configura-se uma afronta à privacidade e à proteção dos dados pessoais.

Apesar de enriquecedora a tentativa de classificação entre privacidade física e privacidade informativa, observa-se que esta última nada mais é que a própria proteção dos dados pessoais. Mesmo na internet, a ameaça da privacidade "física" está presente com "*o que os outros podem ver e ouvir sobre 'nós'*". Portanto, quando o autor tratar de

---

emprego seria uma violação de privacidade, porque a lei proíbe que essas informações sejam usadas para essa finalidade. Eu não limito a privacidade à capacidade do indivíduo de manter o controle sobre os dados ou o direito de ser deixado em paz. Essas estão entre as definições de privacidade mais restritas" (tradução livre). Segue trecho original: *"(...) by privacy, I mean the absence of the inappropriate processing of information tha pertains to na identifiable person. Appropriate may be defined by laws, regulations, agréments, contracts and even well-established expectations. For example, using my health information to discriminate against me in terms of employment would be a privacy violation, because law prohibits that information from being used for that purpose. I do not limit privacy to the individual´s ability to maintain control over data or the right to be left alone. Those are among the privacy definitions that are more constrained."*. Já a proteção de dados pessoais a define como: "A proteção de dados é o sistema de regras que impede o processamento inadequado. Por exemplo, a lei europeia de proteção de dados exige que as organizações tenham uma base legal para fazer qualquer processamento de dados " (tradução livre). Segue trecho original: "*Data protection is the system of rules that prevent the inappropriate processing. For example, European data protection law requires organizations to have a legal basis to do any processing of data*". Ao final,o autor reconhece que "O conceito amplo de privacidade que descrevo é muito semelhante à proteção de dado". Segue trecho original: "*The broad concept of privacy I describe is very similar to data protection*". *Idem, ibidem.,* p. 101.

privacidade informativa, reportar-se-á como se fosse o direito à proteção dos dados pessoais.

Preliminarmente, Martin esclarece que nem todo dado coletado é fornecido diretamente pelo indivíduo. As pessoas são curiosas, observam outros indivíduos e essas observações se transformam em impressões. Quando memoriza-se, armazena-se essa impressão, ela passa a pertencer aos outros, o que não quer dizer que estão sob o controle deles. As impressões sempre existiram como em notas ou livros. Ao longo do tempo, as impressões aumentaram, tornando-se uma parte significativa de todos os dados produzidos e passaram a ser encontrados na forma de dados digitais. Hoje, para se obter as impressões e observações pessoais não necessitaria mais dos olhos, ouvidos e nariz de um indivíduo. Graças às novas tecnologias como "*cookies*" ou "*beacons*", dispositivos com sensores ou sistemas como CCTV (Circuito fechado de televisão), os dados digitais observados são coletados.[111]

Nesse contexto que se desenvolve a taxonomia baseada na origem do dado, seja este fornecido pelo indivíduo ou "observado pela internet', isto é, captado por tecnologias. Para compreender as diferenças entre esses dois tipos de dados, apresentar-se-ão também os dados que não são frequentemente citados pelos juristas ou expressos em legislações, de forma individualizada, mas que podem ser aglomerados a fim de se identificar um certo indivíduo.[112]

Ao analisar a evolução do processamento de dados, quatro classificações de dados com base em suas origens foram isoladas para estampar o plano de fundo desta taxonomia.

---

[111] *Idem, ibidem*, p. 104.

[112] Martin assim esclarece: "Para entender as diferenças entre os dois tipos de dados, além dos dados não explicitados pela legislação, uma taxonomia de dados seria útil. A lei de privacidade da informação é essencialmente a regulação do processamento de dados que pertence aos indivíduos de uma forma que pode estar ligada a esses mesmos indivíduos. O tipo de dados que estão no domínio ou abrangencia de aplicação da lei de privacidade é o de dados pessoais. Dados sobre animais, vegetação e materiais não são do domínio da lei de privacidade. Os dados sobre pessoas humanas como nome, endereço ou identificadores estão claramente dentro do domínio da lei de privacidade. Os dados que podem ser combinados para vincular a um indivíduo único podem ser de domínio da lei de privacidade. Esta última categoria, dados que são combinados, foi expandida exponencialmente pelo surgimento de novas tecnologias de informação e comunicação." (tradução livre). Segue trecho original: "*To understand the differences between these two types of data in addition to data not explicitly by the legislation, a data taxonomy would be useful. Information privacy law is essentially the regulation of the processing of data that pertains to individuals in a fashion that may be linked to those same individuals. The term for data that is the domain for privacy law enforcement is personal data. Data about animals, vegetation and materials, are not the domain for privacy law. Data about human individuals by the name, address or identifiers are clearly within the domain of privacy law. Data that may be Knitted together to link to a unique individual might be the domain for privacy law. This last category, data that be knitted together, has been expanded exponentially by the emergence of new information and communications technology*". *Idem, Ibidem*, p. 105.

As quatro classificações de fundo são: fornecido (*Provided*), observado (*Observed*), derivado (*Derived*) e inferido (*Inferred*).

2.4.1. Fornecido

Na década de 60, quando o livro "*Privacy and Freedom*", do professor da Universidade de Columbia Alan Westin, foi publicado, a grande maioria dos dados processados por computadores pertencentes aos indivíduos era fornecida diretamente por eles, ou seja, decorriam das suas ações conscientes e voluntárias. De forma exemplificativa, o indivíduo que registra uma escritura, abre uma conta, paga uma dívida, solicita um empréstimo e se forma na faculdade são fatos ou ações que foram coletadas. Essas ações discretas criam um registro que envolve essa pessoa. Esses registros foram coletados e podem ser verificados por onde a pessoa passou. Nesse contexto, a coleta de dados e a sua origem derivam do mesmo lugar. [113] Ora, os dados dizem respeito ao indivíduo e foram fornecidos por ele.

Como já fora constado, a internet modificou esse cenário, pois os registros que antes eram dispersos, agora tornam-se em registros organizados[114] e, por pressuposto, com maior facilidade de serem localizados e tornados disponíveis.

De todo modo, entende-se por "dados fornecidos" aquelas ações diretas dos indivíduos em que ele ou ela tem a completa consciência de que estas levaram a originar esses dados. Logo, os dados fornecidos incluem os cadastros, as pesquisas realizadas, entre outros. Portanto, os indivíduos tem consciência de que forneceram esses dados. [115]

Da classificação de dados fornecidos, destacam-se três subcategorias que são os dados iniciados, os dados transacionados e os dados postados. Os dados iniciados são aqueles fornecidos pela iniciativa do usuário, sem qualquer ameaça ou provocação, mas

[113] *Idem, Ibidem*, p. 107-108.

[114] Essa é a lógica que, em 1973, o saudoso professor Stefano Rodotà sublinhou: "[...] a novidade fundamental introduzida pelos computadores é a transformação de informação dispersa em informação organizada." RODOTÀ, Stefano. *Elaboratori elettronici e controllo sociale*. Bologna: II Mulino, 1973, p. 14.

[115] É a essência do que se extrai de: "Os dados fornecidos são originados por meio de ações diretas tomadas pelo indivíduo, nas quais ele ou ela está plenamente ciente das ações que levaram à originação dos dados. Os dados fornecidos incluem registros, pesquisas de aplicativos e quaisquer casos em que o indivíduo forneça dados com total consciência de que está fazendo isso." (tradução livre). Segue trecho original: "*Provided data originates via direct actions taken by the individual in which he or she is fully aware of actions that led to the data origination. Provided data includes registrations, surveys applications and any instances when the individual provides data with a full awareness that he ou she is doing so*". *Idem, ibidem*.

que iniciam uma relação. Os dados transacionais são aqueles fornecidos em troca de determinado produto ou serviço. Por fim, os dados postados são aqueles fornecidos de livre e espontânea vontade do usuário que pretende compartilhar suas impressões, fotos e vídeos na internet, entre outros exemplos. [116]

2.4.2. Observado

Há um tempo, havia alguns conjuntos de dados observacionais, mas que não eram computadorizados. Por exemplo, os médicos escreviam notas sobre seus pacientes em papel, os pequenos comerciantes faziam uma relação de quem eram os seus melhores consumidores e até poderiam observar semelhanças de compras entre os seus clientes. Estes pequenos conjuntos de dados manuais, criados sem o envolvimento do titular dos dados, não foram, em sua maior parte, suficientemente significativos para afetar um

[116] As subcategorias de Martin Abrams foram melhores abordadas no estudo de 2014, "*The Origins of Personal Data and its Implications For Governance"*. Assim, o autor esclarece: "Os **dados iniciados** são o produto de indivíduos realizando uma ação que inicia um relacionamento. Essas ações podem incluir a solicitação de um empréstimo, o registro para votar, a retirada de uma licença ou o registro em um site. O indivíduo está ciente da ação que ele ou ela está tomando. Embora o indivíduo nem sempre considere as implicações, seria intuitivo para o indivíduo que suas ações criassem dados que dizem respeito a ele. **Dados transacionados** são criados quando um indivíduo está envolvido em uma transação. As transações podem incluir a compra de um produto com cartão de crédito, o pagamento de uma fatura, a resposta a uma pergunta ou a realização de um teste. Embora o indivíduo possa não estar pensando no fato de estar criando um registro, ele entende que a transação deve ser registrada, os registros precisam ser atualizados e as histórias modificadas. O indivíduo é um participante ativo na origem dos dados. **Postado** Quando os indivíduos se expressam proativamente, eles estão cientes de que estão criando expressões que serão vistas ou ouvidas pelos outros. Nos últimos anos, os dados registrados podem ser uma reportagem de jornal ou televisão. O crescimento das redes sociais aumentou ativamente a originação de dados com base na fala pró-ativa. Enquanto o indivíduo nem sempre está ciente de quem pode ver ou ouvir a expressão, eles estão totalmente envolvidos em sua criação". (tradução livre). Segue trecho original: "***Initiated*** *data is the product of individuals taking an action that begins a relationship. These actions might include applying for a loan, registering to vote, taking out a license, or registering on a website. The individual is aware of the action he or she is taking. While the individual doesn't always consider the implications, it would be intuitive to the individual that his or her actions would create data that pertains to him or her.* ***Transactional*** *data is created when an individual is involved in a transaction. Transactions may include buying a product with a credit card, paying a bill, responding to a question, or taking a test. While the individual might not be thinking about the fact that he or she is creating a record, they understand the transaction must be recorded, records need to be updated, and histories modified. The individual is an active participant in the origin of the data.* ***Posted*** *When individuals proactively express themselves, they are aware that they are creating expression that will be seen or heard by others. In past years, the recorded data might be a newspaper or television story. The growth of social networks has actively increased the origination of data based on proactive speech. While the individual is not always aware of who might see or hear the expression, they are fully involved in its creation*". (Grifo nosso). ABRAMS, Martin. *The Origins of Personal Data and...Op cit.* Disponível em: <http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf>. Acesso em: 04.11.2017.

modelo de governança global baseado na autonomia individual. Essa taxonomia classificará essa categoria de dados como observados.[117]

Dessa forma, os dados observados podem ser definidos como tudo o que é observado e gravado. O surgimento da Internet como meio de consumo interativo tornou possível a observação e a digitalização de dados em um modo mais robusto. Na internet, onde se pode observar a *geolocalização*[118] (de onde o usuário está posicionado) do indivíduo, o que ele ou ela olham/escutam, com que frequência ele ou ela olham/escutam para isso e por quanto tempo param para observar aquele conteúdo.

Para além dos computadores, esse é o campo contemporâneo de atuação em que o reconhecimento facial[119] e a "Internet das Coisas", por meio de seus sensores nos produtos, estão produzindo milhares de observações de maneira digital que antes era impraticável de se captar essa quantidade de dados no "mundo físico". [120]

Os dados observados são subdivididos em três categorias, quais sejam a de dados acionados, de não previstos e de passivos. Os dados acionados são, muitas vezes, caracterizados pela notificação recebida pelo usuário de que o site se vale de *cookies* para captar dados pessoais. Caso não seja notificado no início da navegação, o usuário tem consciência de que em algum momento esses dados serão coletados. Os dados observados não previstos são aqueles em que o usuário sabe que no produto há sensores que podem captar dados, mas não espera que novos dados sejam criados como o modo em que cuida do carro. Por derradeira, os dados passivos são característicos de lugares públicos em que

[117] *Idem, The Marco Civil and Beyond...Op. cit.,* p. 106.

[118] A *geolocalização* é uma tecnologia que necessita da conexão da internet para se valer dos dados que identifiquem a posição geográfica do indivíduo por meio dos dispositivos móveis com a funcionalidade de um GPS (móvel) ou de computadores (fixo). Nesse sentido, aplicado aos motores de busca, se o usuário digitar a palavra restaurante no site que não dispõe do serviço de *geolocalização*, inúmeros resultados de pesquisa serão listados, independentemente do local que ele esteja. Com a ferramenta, o site que possuir tal suporte, elencará nos primeiros resultados os restaurantes que estejam próximos ao local em que o usuário está. HOLDENER, Antony. *Geolocation*. Sebastopol: O'Reilly Media, 2011, p. 87.

[119] O reconhecimento fácil é um tecnologia que está presente em provedores de aplicação como no *Facebook* em que as fotos postadas pelos usuário, isto é, dados fornecidos, decorrem a coleta de dados observados que seria o reconhecimento fácil nas fotos. O mesmo pode-se falar de celulares *smarthphones* que se valem da tecnologia de reconhecimento facial como meio de desbloqueio da tela de início, entre tantos outros exemplos.

[120] A definição proposta por Martin: "Os dados observados são simplesmente o que é observado e registrado. O surgimento da Internet como meio de consumo interativo tornou possível observar e digitalizar dados de maneira mais robusta. Na internet, pode-se observar de onde veio o indivíduo, o que ele olha, com que frequência ele olha, e até a duração das pausas. O reconhecimento facial e a Internet das Coisas estão fazendo a observação de maneira digital possível no mundo físico" (tradução livre). Segue trecho original: "*Observed data is simply whats is observed and recorded. The emergence of the Internet as na interactive consumer médium has made it possible to observe and digitise data in a more robust manner. On the Internet, onde may observe where the individual came from, what he ou she looks at, how often he or she look at it, and even the length of pauses. Facial recognition and the Internet of Things are making observation in a digital manner possible in the physical world*". ABRAMS, Martin, *The Marco Civil and Beyond: Privacy Governance for the Future*. Op. Cit., p. 108.

câmeras observam a pessoa e criam novos dados em razão dessa ação, porém a pessoa não sabe que está sendo vigiada. [121]

.

2.4.3. Derivado

Como a própria nomenclatura assinala, os dados derivados são dados que derivam de outros dados. Isto é, a partir dos dados fornecidos e observados, busca-se as semelhanças entre eles. Antigamente, de forma singular, os comerciantes classificavam os seus clientes com base em atributos comuns, preferencias comuns.

A partir do século 19, na América do Norte, os comerciantes criaram cooperativas para compartilhar informações de crédito e classificá-las a partir dos dados compartilhados

---

[121] Os dados observados apresentam as seguintes subcategorias: "Os **dados observados engajados (dados acionados)** incluem dados que se originam de cookies on-line, cartões de fidelidade e outras instâncias em que o indivíduo é informado da observação em algum momento. Enquanto o indivíduo pode esquecer que os dados estão sendo criados, há uma consciência geral de que está ocorrendo. Em alguns casos, o indivíduo pode objetar ou cancelar ou impedir a criação desses dados. Por exemplo, uma pessoa pode desativar o Wi-Fi em seu dispositivo móvel se não quiser ser observado. A regulamentação e a prática do setor têm implicações sobre qual subclassificação um tipo de dado pode ser adequado. Por exemplo, os cookies são incluídos no engajamento porque vários regulamentos e códigos do setor tornaram a transparência uma norma crescente. A **criação não antecipada de dados (não previstos)** é uma instância em que os indivíduos estão cientes de que existem sensores, mas têm pouca noção de que os sensores estão criando dados que podem pertencer ao indivíduo. Por exemplo, uma pessoa pode estar ciente de que há sensores nos pneus do carro e no cárter do motor, mas a pessoa pode não estar ciente de que a maneira pela qual ele ou ela mantém o carro é um elemento de dados que pode pertencer a eles. Essa subclassificação seria apropriada para muitos dos aplicativos relacionados à Internet das Coisas. Indivíduos típicos teriam conhecimento limitado desse tipo de dados. **Passivo** A última subcategoria é dados observacionais passivamente criados. Um exemplo é o CCTV em locais públicos quando combinado com o reconhecimento facial. Também é aplicável a qualquer situação em que seria muito difícil para os indivíduos estarem cientes de que estão sendo observados e que os dados referentes à observação estão sendo criados." (tradução livre). Segue trecho original: "***Engaged*** *observed data includes data that originates from online cookies, loyalty cards, and other instances in which the individual is made aware of the observation at some point in time. While the individual may forget that the data is being created, there is a general awareness that it is taking place. In some cases, the individual can object to or abort the creation. For example, a person may disable the Wi-Fi on their mobile device if they don't want to be observed. Regulation and industry practice have implications on which sub-classification a type of data might fit. For example, cookies are included in engaged because various regulations and industry codes have made transparency a growing norm.* ***Not anticipated*** *data creation are instances in which individuals are aware that there are sensors but have little sense that the sensors are creating data that may pertain to the individual. For example, a person may be aware that there are sensors in the tires on the car and in the oil pan in the engine, but the person might not be aware that the manner in which he or she maintains the car is a data element that might pertain to them. This sub-classification would be appropriate for many of the applications related to the Internet of Things. Typical individuals would have limited awareness of this type of data.* ***Passive*** *The last sub-category is passively created observational data. An example is CCTV in public places when combined with facial recognition. It is also applicable to any situation in which it would be very difficult for individuals to be aware that they are being observed and data pertaining to the observation is being created".* (Grifo nosso). ABRAMS, Martin. *The Origins of Personal Data and...Op. cit.* Disponível em: <http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf>. Acesso em: 04.11.2017.

(*credit ratios*). A indústria de marketing direto começou com o processo simples de usar dados de transações para derivar segmentos de mercado com base em semelhanças e preferências. Além disso, uma vez que os analistas começaram a buscar as semelhanças entre os consumidores, eles começaram a realizar cálculos aritméticos simples para melhorar as comparações. Por exemplo, a rátio da dívida hipotecária para a dívida do consumidor demonstraria algo interessante? Os produtos desses cálculos simples são dados derivados de dados reais.

A indústria de seguros tem buscado, durante centenas de anos, o nascimento, a morte, a profissão, o endereço, o estilo de vida e as tabelas atuariais utilizadas para a assinatura do seguro de vida. Em suma, dessas tabelas de comparações simples que resulta o dado derivado.

Embora esses dados derivados se baseiam em dados provenientes de interações e transações que envolvem o indivíduo, a recíproca não é verdadeira, na medida em que o indivíduo não participa tampouco cria os dados derivados.[122]

Na concepção de Martin, os dados derivados são dados simplesmente retirados, de forma bastante mecanica, de outros dados e que se tornam um novo dado relacionado ao individuo. [123]

Os dados derivados são divididos em duas categorias: os dados derivados de computação e os dados notáveis. O primeiro são os dados que foram criados por novos elementos de dados que passaram por um processo aritmético executado por elementos numéricos existentes. O segundo são os dados que derivam de novos dados criados através da classificação de indivíduos como sendo parte de um grupo com atributos comuns que serão notados em outro grupo. [124]

---

[122] *Idem, ibidem*, p. 106-107.

[123] O autor assim explica: "Os dados derivados são dados que são simplesmente derivados de um modo razoavelmente mecânico de outros dados e se tornam um novo elemento de dados relacionado ao indivíduo. Por exemplo, taxas simples calculadas a partir de outros dados são derivadas. Os clusters de marketing (grupo ou publico alvo) também são um exemplo de dados derivados *" (tradução livre).* Segue trecho original*: "Derived data is data that is simply derived in a fairly mechanical fashion from other data and becomes a new data elemento related it the individual. For example, simple ratios calculated from other data is derived. Marketing clusters are also an example of derived data*". Idem, ibidem, p. 108.

[124] Portanto, o autor esclarece que: "**Dados derivados computacionalmente (dados derivados da computação)** são a criação de um novo elemento de dados através de um processo aritmético executado em elementos numéricos existentes. Por exemplo, um credor pode criar um dado computacional calculando a relação entre a dívida hipotecária e a dívida total do consumidor, um comerciante on-line pode calcular o gasto médio por visita ou um comerciante pode calcular a porcentagem de itens devolvidos para itens comprados. Cada um dos novos produtos computacionais é um elemento de dados que pode ser usado por uma organização para entender melhor o comportamento ou tomar decisões relativas ao indivíduo. O indivíduo normalmente não estaria ciente da criação do novo elemento de dados. Os **dados derivados da condição (dados notáveis)** são novos elementos de dados criados pela classificação de indivíduos como parte de um grupo com base em atributos comuns mostrados pelos membros do grupo. Por exemplo, um

2.4.4. Inferido

Os dados inferidos são aqueles em que há a possibilidade de dedução, com probabilidade significativa, de um atributo a partir de um conjunto de atributos da pessoa. Após certo tempo, especificamente na década passada, cientistas aprenderam como usar um dado pessoal fornecido e observado não estruturado para análise de modelos que podem prever um comportamento futuro.

Os dados inferidos são o produto da probabilidade baseada em processos analíticos mais sofisticados. Pontuações de créditos e de identidade são exemplos das inferências advindas de outros dados proporcionados pela ferramenta *Big Data*.[125]

Enfim, os dados inferidos são subclassificados em de estatística e de análise avançada. Os dados inferidos por estatísticas são um produto de caracterização de um processo estatístico. Por sua vez, os dados de análise avançada são criados por um específico processo de análise de dados em massa como aquele produzido pelo já mencionado *Big Data*.[126]

---

profissional de marketing pode perceber que seus clientes têm seis atributos comuns e procurar os mesmos atributos em um grupo de clientes em potencial." (tradução livre). Segue trecho original: "***Computationally*** *derived data is the creation of new data element through an arithmetic process executed on existing numeric elements. For example, a lender might create a computational data by calculating the ratio of mortgage debt to total consumer debt, an online merchant might calculate average spend per visit, or a merchant might calculate the percentage of returned items to items bought. Each of the new computational products is a data element that might be used by an organization to better understand behavior or make decisions pertaining to the individual. The individual would not typically be aware of the creation of the new data element.* ***Notionally*** *derived data are new data elements created by classifying individuals as being part of a group based on common attributes shown by members of the group. For example, a marketer might notice its customers have six common attributes and look for the same attributes in a group of potential customers*". (Grifo nosso) ABRAMS, Martin. *The Origins of Personal Data and...Op. cit.* Disponível em: <http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf>. Acesso em: 04.11.2017.

[125] Nesse sentido se dá a definição de: "**Dados inferidos** são o produto de um processo analítico baseado em probabilidades. As pontuações de crédito e identidade são exemplos, assim como muitas das inferências que vêm da análise de big data" (tradução livre). Segue trecho original: "*Inferred data is the product of a probability-based analytic process. Credit and identity scores are examples, as are many of the inferences that come from big data analysis". Idem, ibidem*, p. 108.

[126] É o que se extrai de: "**Estatística:** Dados estatisticamente inferidos são o produto da caracterização baseada em um processo estatístico. Os exemplos incluem pontuações de risco de crédito, a maioria das pontuações de fraude, pontuações de resposta e pontuações de lucratividade. O indivíduo não está tipicamente envolvido no desenvolvimento dessas pontuações. Os **dados analíticos avançados** são o produto de processos analíticos avançados, como os encontrados em big data. Esses elementos de dados são geralmente o produto da análise em conjuntos de dados maiores e mais diversos, e os elementos são baseados em análises que dependem mais da correlação do que da causação. Os primeiros exemplos de tais elementos de dados são pontuações de identidade que predizem a probabilidade de uma identidade ser real. Embora as

2.4.5. Análise da taxonomia baseada na origem dos dados

Abaixo segue a tabela que classifica a categoria de dados pela origem inspirada na tabela desenvolvida por Martin Abrams com maiores detalhes e alguns exemplos. [127]

A primeira coluna está a classificação maior que se destina em como os dados são originados, se são fornecidos, observados, derivados ou inferidos.

A segunda coluna apresenta uma subclassificação que analisa de forma mais detida como esses dados foram coletados.

A terceira coluna consta os exemplos para auxiliar o leitor para relacionar a categoria com os dados e o que acontece no mundo.

A quarta coluna proporciona uma simples classificação fundamentada no nível individual de alerta e proteção em se estabelecer quanto consciente do processamento de seus dados o indivíduo está, perceptível na distância de identificação e do modo que o dado é originado.

---

pontuações de crédito dependessem da análise de falhas de crédito anteriores e do que correlacionou e impactou essas falhas, as pontuações de identidade basearam-se em anomalias na maneira como as identidades eram estruturadas. Isso exigiu um novo tipo de análise que não era possível no passado. No campo da medicina, o Big Data está começando a gerar insights sobre a probabilidade de futuros resultados de saúde. O indivíduo não estaria ciente da criação desses novos dados que são o produto das inferências que vêm da análise". (tradução livre). Segue trecho original: "**Statistical:** Statistically inferred data is the product of characterization based on a statistical process. Examples include credit risk scores, most fraud scores, response scores, and profitability scores. The individual is not typically involved in the development of these scores. **Advanced Analytical** data are the product of advanced analytical processes such as those found in big data. These data elements are typically the product of analysis on larger and more diverse data sets, and the elements are based on analysis that is more dependent on correlation rather causation. Early examples of such data elements are identity scores that predict the likelihood that an identity is real. While credit scores were dependent on looking at past credit failures and what correlated to and impacted those failures, identity scores were based on anomalies in the manner in which identities were structured. This required a new type of analysis that had not been possible in the past. In the medical field, Big Data is beginning to generate insights into the likelihood of future health outcomes. The individual would not be aware of the creation of these new data that are the product of the inferences that come from analysis". ABRAMS, Martin. *The Origins of Personal Data and...Op. cit.* Disponível em: <http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf>. Acesso em: 04.11.2017.

[127] Idem, ibidem, p. 109-110.

Figura 1. Tabela das categorias dos dados pessoais classificados pela origem:

CATEGORIA	SUBCATEGORIA	EXEMPLOS	NIVEL DE CONSCIÊNCIA INDIVIDUAL
Fornecido	**Iniciados**	• Cadastros • Dados públicos Arquivos Licença	Alta
	Transacionados	• Contas pagas • Inquéritos respondidos • Registros públicos Saúde educação tribunais • Pesquisas	Alta
	Postados	• Discursos em lugares públicos • Postagens nas redes sociais • Fotos e vídeos postados;	Alta
Observado	**Acionados**	• Cookies dos sites • Cartão de fidelidade • Sensores de localização ativados em dispositivos pessoais	Médio
	Não previstos	• O tempo de pausa que o indivíduo leve na frente da tela do *tablete*	Baixo
	Passivos	• Sistema de câmeras das ruas	Baixo
Derivado	**Computacional**	• Compra média por visita	Médio para baixo
	Notável	• Classificação baseada nos atributos comuns dos compradores	Médio para baixo
Inferido	**Estatístico**	• Pontuação de crédito • Pontuação de fraudes	Baixo
	Análise avançada	• Risco de desenvolver uma doença, baseado nos diversos fatores analíticos;	Baixo

Dessa forma, como exemplo, o histórico médico fornecido pelo usuário é classificado como um dado fornecido pela sua iniciativa e que apresenta um alto nível de alerta e conscientização do indivíduo que aceita o seu tratamento. O mesmo valerá para as contas pagas e pesquisas realizadas, sendo eles considerados dados fornecidos transacionados e as fotos, vídeos e opiniões promovidas pelos usuários na internet seriam dados fornecidos postados.

Como dados observados teríamos a captura de dados por meio de cookies e sensores de localização em objetos pessoais que seriam dados observados acionados ou notificados, cujo nível de conscientização é médio. Os dados do tempo que uma pessoa pausa sobre a tela do computador seria um dado observado não previsto, cujo nível de conscientização é baixo.

Para os dados derivados computacionais, alguns dos exemplos apontados são de dados de frequência de visitações no site e o risco de se desenvolver uma doença baseado em uma única variação genética. Já como dado derivado notável, há o exemplo dos atributos comuns de alguns consumidores que podem ser utilizados para notar outro grupo potencial de consumidores, isto é, consumidores que fumam cigarro geralmente ingerem bebidas alcoólicas, assim o incentivo do consumo do cigarro pelos outros usuários, poderá vir a aumentar a venda de bebidas em determinado bar.

Como dados inferidos, há basicamente duas subcategorias que seria de estatística e de análise avançada de dados. Por exemplo, como dado inferido estatístico, cita-se o sistema de pontuação de crédito utilizado por agências financeiras para medir o risco em se conceder um empréstimo para determinada pessoa, baseada no seu histórico financeiro. Além disso, com o uso do *big data*, através de dados fornecidos ou observados, um perfil do usuário pode ser traçado para deduzir algum comportamento futuro, por exemplo, se uma criança de 9 (nove) anos terá sucesso na faculdade.

Da análise detida, verifica-se que a grande quantidade de dados pessoais fornecidos e observados na internet possibilita a criação de novos dados que podem identificar uma pessoa. Diante da inovação tecnológica, a quantidade de dados inferidos levará a extinção dos dados derivados.

Infere-se que a maioria das leis sobre proteção de dados são transcrições das orientações da OECD e das Diretivas Europeias de proteção de dados pessoais, as quais

colocam o indivíduo e o seu consentimento como algo de extrema relevância para o exercício de direitos como o acesso, a oposição, o cancelamento ou a retificação.

Ocorre que não há campo de atuação do titular de dados pessoais para que os dados observados (não previstos e passivos), os dados derivados e, principalmente, os dados inferidos sejam criados. Portanto, nessa perspectiva, o consentimento não é a solução viável para que o usuário controle os dados que o identificam ou podem vir a identifica-lo.

Embora o consentimento mereça continuar sendo um mecanismo necessário para a proteção de dados pessoais, no caso dos dados observados, derivados e inferidos, ele se mostra pouco efetivo. Para tanto, sugere-se identificar que talvez uma política pública de proteção de dados pessoais e uma autoridade administrativa fiscalizadora seja uma alternativa para complementação da proteção. A política pública seria viável ao estabelecer quais interesses seriam legítimos para que o responsável pudesse efetuar o tratamento de dados pessoais que independem da anuência do usuário e, ao mesmo tempo, obter a proteção e segurança necessária.

Por último, pretendeu-se apenas apresentar neste trabalho uma taxonomia para a proteção de dados pessoais, sem desmerecer outras e nem adotar tal classificação como algo incontestável. A finalidade de demonstrar a visão pessoal do autor Martin se deu com o único proposito de induzir reflexões a respeito dos diversos exemplos de coleta e criação de dados pessoais que fogem daquilo que o individuo conhece sobre o tratamento desses dados. Observa-se, através do estudo proposto, que o nível de consciência que os indivíduos têm ou deveriam ter sobre os tipos de dados armazenados, criados, modificados, transmitidos e comercializados é baixo. Conquanto os dados derivados e inferidos não estejam explicitamente corroborados na maioria das legislações de proteção, a aglomeração desses dados pode vir a identificar uma pessoa, o que, em tese, abrangeria o amplo conceito de dados pessoais, ao passo que uma legislação efetiva e com extrema proteção é o caminho central que deve ser percorrido.

2.5. Origem e evolução do direito à proteção dos dados pessoais

A proteção dos dados pessoais é uma preocupação que se tornou uma tendência mundial, pois diversos países incluíram esse direito fundamental em seus ordenamentos

jurídicos[128], inclusive, com expressa previsão nas Consituições da Espanha[129], Portugal[130], Russia[131], entre outros.

Ocorre que houve uma evolução nas próprias leis de proteção de dados até se consagrar certa autonomia, pois as legislações incluíam tal proteção como um desmembramento da privacidade. [132]

[128] DONEDA, Danilo. O Direito Fundamental à Proteção de Dados Pessoais. In: MAGALHÃES, Guilherme (coord.). *Direito Privado e Internet*. São Paulo: Atlas, 2014, p. 66.

[129] Segundo artigo 18 da Constituição Espanhola, em seu parágrafo 4, disciplina a proteção de dados pessoais enquanto o parágrafo 1 cuida da privacidade: "Artigo 18. 1. O direito à honra, à privacidade pessoal e familiar e à própria imagem é garantido. 2. O endereço é inviolável. Nenhuma inscrição ou registro poderá ser feito sem o consentimento do proprietário ou resolução judicial, exceto em caso de flagrante delito. 3. O sigilo das comunicações e, em particular, dos cartões postais, telégrafos e telefones é garantido, salvo decisão judicial. 4. A lei limitará o uso da tecnologia da informação para garantir a honra e a privacidade pessoal e familiar dos cidadãos e o pleno exercício de seus direitos." (tradução livre). Segue trecho original: "*Articulo 18. 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 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*". (Grifo nosso) ESPANHA. Cosntitucion Española de 1978. Disponível em: http://www.congreso.es/docu/constituciones/1978/1978_cd.pdf. Acessado em: 31.11.2017.

[130]Conforme artigo 35º da Constituição Portuguesa, o qual prevê: "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 protecção 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 protecção idêntica à prevista nos números anteriores, nos termos da lei". (Grifo nosso) PORTUGAL. Constituição da República Portuguesa de 1976. Disponível em: https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx. Acesso em: 31.11.2017.

[131] É o que dispõe o artigo 24 da Constituição Russa: "A coleta, conservação, uso e disseminação de informações sobre a vida privada de uma pessoa não serão permitidos sem seu consentimento. 2. Os órgãos da autoridade estatal e o governo autónomo local, os seus funcionários devem assegurar a todos a possibilidade de conhecer os documentos e materiais que afetem diretamente os seus direitos e liberdades, salvo disposição em contrário prevista na lei. "(tradução livre). Segue trecho original, traduzida do russo para o inglês: "1. *The collection, keeping, use and dissemination of information about the private life of a person do shall not be allowed without his or her consent. 2. The bodies of state authority and local self-government, their officials shall ensure for everyone the possibility of acquainting with the documents and materials directly affecting his or her rights and freedoms, unless otherwise provided for by law*". RUSSIA. Constituição Russa de 1993. Disponível em: http://www.constitution.ru/en/10003000-01.htm. Acesso em: 31.11.2017.

[132] Doneda explica que: "Essa evolução reflete tanto a busca de uma tutela mais eficaz como a constatação de que a proteção da pessoa na Sociedade da Informação passava, cada vez mais, a depender diretamente do controle destas sobre seus próprios dados pessoais, o que acabou vinculando a matéria aos direitos fundamentais". DONEDA, Danilo. O Direito Fundamental à Proteção de Dados Pessoais...*Op.cit.* p. 67.

As primeiras legislações que tratavam de dados pessoais foram a Lei do Land alemão de Hesse, de 1970, seguida pela Lei Sueca de 1973 nomeada como "*Data Legen 289*" ou "*DataLag*" que cuidava dos bancos de dados e a *Privacy Act* do sistema norte-americano de 1974[133], conhecido por estabelecer um "*Code of Fair Information Pratice*"[134] que se destinava a regular a coleta, manutenção, uso e disseminação de informações pessoais sobre os particulares que eram conservados pelo setor público. [135] Até então, as legislações tinham como foco em obrigar que os bancos de dados fossem transparentes e em estabelecer a responsabilidade de seus operadores.

Além disso, também em solo norte-americano, o primeiro estudo que ganhou certa notoriedade sobre a relação entre a privacidade e o tratamento de dados pessoais veio com o "*Records, computers and the rights of citizens*" de 1973[136], efetuado por uma comissão de especialistas para a "*Secretary for health, education and welfare"* que alertou sobre a capacidade do sistema dos computadores em ser um instrumento poderoso que pode ser usado pelo governo e indústrias.[137] Esse primeiro passo foi fundamental e serviu de inspiração para outros países, principalmente, europeus, que pretendiam despertar a

---

[133] O Direito Fundamental à Proteção de Dados Pessoais...*Op.cit*. p. 67.

[134] CATE, Fred H. The failure of Fair Information Practice Principles. In: *Consumer Protection in the Age of the 'information economy' (Markets and the Law).* Hampshire: Ashgate Publish, 2006, p. 343-379.

[135] DONEDA, Danilo. O Direito Fundamental à Proteção de Dados Pessoais. In: MAGALHÃES, Guilherme (coord.). *Direito Privado e Internet*. São Paulo: Atlas, 2014, p. 66.

[136] EUA. *Records, computers and the rights of citizens*. Report of the Secretary's Advisory Committee on Automated Personal Data Systems. U.S. Department of Health, Education & Welfare. Julho de 1973. Disponível em: https://www.justice.gov/opcl/docs/rec-com-rights.pdf. Acesso: 05.11/2017.

[137] Segue um trecho do Relatório citado: "Computadores interligados por meio de redes de telecomunicações de alta velocidade estão destinados a se tornar o principal meio de produção, armazenamento e uso de registros sobre pessoas. As inovações agora em discussão no governo e na indústria privada reconhecem que o sistema de manutenção de registros baseado em computador, se usado adequadamente, pode ser uma poderosa ferramenta de gerenciamento. Sua capacidade de recuperação e análise em tempo hábil de corpos complexos de dados pode ser inestimável assistência a tomadores de decisão pressionados. Sua capacidade de lidar com grandes quantidades de transações individuais em minutos e horas, em vez de semanas ou meses, como era o caso anteriormente, possibilita programas de serviço para pessoas que seriam impensáveis na era manual de manutenção de registros. Medicar, por exemplo, seria impossível administrar sem computadores para assumir muitas funções administrativas de rotina. Os sistemas de pagamentos de assistência pública baseados em computador também estão ajudando os Estados e os condados a garantir que os pagamentos de assistência social vão para aqueles que realmente precisam e merecem". (tradução livre). Segue trecho original: "*Computers linked together through high-speed telecommunications networks are destined to become the principal medium for making, storing, and using records about people. Innovations now being discussed throughout government and private industry recognize that the computer-based record keeping system, if properly used, can be a powerful management tool. Its capacity for timely retrieval and analysis of complex bodies of data can be of invaluable assistance to hard-pressed decision makers. Its ability to handle masses of individual transactions in minutes and hours rather than in weeks or months, as was formerly the case, makes possible programs of service to people that would have been unthinkable in the manual record-keeping era. Medicare, for example, would be impossible to administer without computers to take over many routine clerical functions. Computer-based public assistance payments systems are also helping States and counties to assure that welfare payments go to those who truly need and deserve them*". Ibidem, p. 05.

necessária reflexão para os efeitos que a vinda dos computadores e técnicas modernas de armazenamento de dados poderia acarretar.

Com a finalidade de equilibrar interesses econômicos e a proteção de direitos e garantias fundamentais que surgiu a ideia em se criar as *Guidelines on The Protection of Privacy and Transborder Flows of Personal Data* em 1980[138], elaboradas pela OCDE que é uma organização internacional que tem como objetivo desenvolver políticas públicas que compatibilizem o desenvolvimento econômico e o bem estar das pessoas, visando à proteção dos dados pessoais e a sua transferência internacional. Essas *Guidelines* tratavam do tema de proteção de dados pessoais de forma bem ampla, porém devido ao rápido desenvolvimento tecnológico foram atualizadas em 2013, sem, todavia, alterar a essência do documento.

Seguindo essas diretrizes, no ano de 1981, o Conselho Europeu editou a Convenção de Estrasburgo para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais[139], verdadeiro marco teórico para a proteção dos dados pessoais no mundo uma vez que os seus artigos ainda são aplicados para embasar, fundamentalmente, o tema até os dias atuais. Segundo tal Convenção, em seu preâmbulo, a proteção de dados pessoais é vista como o protagonista a fim de proteger os direitos humanos e as liberdades fundamentais, de ampliar as garantias dos indivíduos, especialmente, o respeito à privacidade, perante o aumento do fluxo transfronteiriço de dados pessoais submetidos ao processamento automatizado, sem mencionar que a sua aplicação leva a união e unificação da lei entre seus membros.[140]

---

[138] Em 1978, perceberam que a falta de um quadro de proteção de dados pessoais poderia afetar todo o livre fluxo fronteiriço de dados entre os países. Logo, um juiz australiano chamado Michael Kirby presidiu o grupo que desenvolveu esse quadro de proteção a convite da OECD publicado em 1980. Disponível em: <http://www.oecd.org/sti/ieconomy/30yearsaftertheimpactoftheoecdprivacyguidelines.htm>. Acesso em: 02.11.2017.

[139] UNIÃO EUROPÉIA. *Convenção de Estrasburgo para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais*. 1981. Dsiponivel em: https://rm.coe.int/1680078b37. Acesso em: 02.11.2017.

[140] Assim, segue texto integral do preâmbulo: "Os Estados membros do Conselho da Europa, signatários da presente Convenção, Considerando que o objetivo do Conselho da Europa é alcançar maior unidade entre seus membros, com base, em particular, no respeito ao Estado de Direito, bem como aos direitos humanos e liberdades fundamentais; Considerando que é desejável alargar as salvaguardas aos direitos de todos e às liberdades fundamentais e, em particular, o direito ao respeito da privacidade, tendo em conta o crescente fluxo transfronteiriço de dados pessoais sujeitos a tratamento automático; Reafirmando ao mesmo tempo seu compromisso com a liberdade de informação independentemente das fronteiras; Reconhecendo que é necessário conciliar os valores fundamentais do respeito pela privacidade e o livre fluxo de informação entre os povos. Acordaram o seguinte: (...)". (tradução livre). Segue trecho original: "*The member States of the Council of Europe, signatory hereto, Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms; Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing*

A Convenção de Estrasburgo de 1981 é um tratado internacional que não se restringe aos países membros da União Européia. Veja-se pelo Uruguai que foi o primeiro país que não fazia parte do bloco econômico europeu a ratificar o acordo em 2013. Isso porque, essa abertura foi conferida com o objetivo de uniformizar um quadro de tutela de dados pessoais no mundo todo[141]. Por outro lado, a Convenção nº 108 deixou de distinguir o tratamento de dados pessoais nos setores público e privado, tampouco diferenciou a privacidade e os dados pessoais, sendo especialmente abrangente e principiológica.

Posteriormente, tais diretrizes inspiraram a "*Personal Data Protection*", isto é, a célebre Diretiva nº 95/46/CE sobre proteção dos dados pessoais na União Européia que reafirmou a posição da Convenção n. 108 ao sistematizar, de forma ampla, o que seria um tratamento adequado dos dados pessoais dos cidadãos europeus, ou melhor, dirigido às pessoas físicas.

Enfatiza-se a questão da abrangência das Diretivas no sentido de que coube a cada Estado-membro realizar a transposição dessas regras para a sua legislação interna. A Diretiva nº 95/46 estabelece um padrão mínimo a ser seguido. Assim, por exemplo, no tocante aos dados sensíveis, cada Estado poderá legislar de modo a não tolerar o tratamento de dados sensíveis, entretanto, o que não poderá fazê-lo seria permitir o tratamento irrestrito desses dados sem a anuência do titular e em qualquer hipótese. Em verdade, como já salientado, a Diretiva estabelece um parâmetro mínimo a ser seguido, mas não há vinculação no ordenamento jurídico dos Estados-membros europeus. Como se verá adiante neste presente trabalho, a abordagem da Diretiva 95/46/CE será de suma importância para tratar do caso da desindexação de dados pessoais, desenvolvido no Capítulo V.

Para socorrer aos anseios da informática e da globalização, outras diretivas foram criadas para complementar as disposições da Diretiva 95/46/CE pelo Parlamento e Conselho Europeu tais como a Diretiva 97/66/CE (relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações), a Diretiva 2002/58/CE (disciplina a proteção dos dados pessoais e a privacidade informativa no setor das

---

flow across frontiers of personal data undergoing automatic processing; Reaffirming at the same time their commitment to freedom of information regardless of frontiers; Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples. Have agreed as follows: (...)". UNIÃO EUROPÉIA. *Convenção de Estrasburgo para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais*. 1981. Dsiponivel em: https://rm.coe.int/1680078b37. Acesso em: 02.11.2017.

[141] LIMA, Cíntia Rosa Pereira. *A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil*. Tese de Livre Docência apresentada junto à Faculdade de Direito de Ribeirão Preto. Ribeirão Preto: USP, 2015, p. 146.

comunicações eletrônicas), Diretiva 2006/24/CE (relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE), entre outras.

Para o aprimoramento do tema, em novembro de 2010, a Comissão Europeia publicou uma "*Comprehensive Approach on Personal Data Protection in the European Union*" e concluiu que a União Européia necessita de uma política mais compreensiva e coerente para tutelar um direito fundamental à proteção dos dados pessoais. Em 2012, editou-se uma proposta para um nova Diretiva, intitulada de "*Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*"[142], a qual acolheria um direito que se convencionou nomear de direito ao esquecimento, o que será tratado em momento oportuno.

Após mais de quatro anos de negociações, pesquisas e consultas, em 27 de abril de 2016, foi aprovado o Regulamento nº 679/2016, conhecido como "Regulamento Geral de Proteção de Dados" ou "*General Data Protection Regulation* (GDPR)"[143], que entrou em vigor no dia 25 de maio de 2018, para tratar da proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Uma das novidades é que o Regulamento Geral se aplica a entidades que processam dados pessoais, mesmo quando o tratamento ocorre fora do território da União Europeia, desde que bens ou serviços sejam oferecidos a titulares de dados que se encontram em algum país da comunidade europeia ou na hipótese de vigilância e monitoramento do comportamento dos titulares de dados localizados na União Europeia. Assim, a compreensão da proteção dos dados pessoais do modelo europeu é de extrema importância, inclusive, em âmbito global, tanto para os titulares de dados quanto para as empresas estrangeiras que realizam o seu tratamento e ofertem seus serviços e produtos.

---

[142] UNIÃO EUROPEIA. *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*. Disponível em: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52012PC0010. Acesso em: 04.11.2017.

[143] UNIÃO EUROPÉIA. *General Data Protection Regulation*. Disponivel em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 04.11.2017.

Embora o Regulamento Geral de Proteção de Dados tenha revogado a Diretiva 95/46/CE, os seus princípios comuns continuam sendo basilares para tal regramento, conforme Considerando (9) do regulamento. [144]

Imperioso destacar que, no âmbito supranacional, há também a "Carta dos Direitos Fundamentais" da União Européia (*Charter of Fundamental Rights of the European Union*), de 07 de dezembro de 2000, no capítulo das liberdades consagrou o direito à proteção dos dados pessoais em seu artigo 8º[145], o qual prevê:

> 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 respetiva retificação.
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente. (Tradução livre)

Expressiva a importância da "Carta dos Direitos Fundamentais" que reconhece a autonomia do direito à proteção dos dados pessoais, porque é de se constatar que o artigo

[144] Nesse sentido, o Considerando (9) do GDPR esclarece que: "Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas a nível da União, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE". E, além disso, revela no Considerando (2) que "os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais. O presente regulamento tem como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares".

[145] É o que se extrai do texto original: "*Article 8 - Protection of personal data: 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority*". UNIÃO EUROPÉIA. *Charter of Fundamental Rights of the European Union*. 2000. Disponível em: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12016P/TXT. Acesso em: 03.112017.

7º[146] deste diploma regulamenta o direito à privacidade como sendo aquele em que "todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações". Por derradeira, cristalino afirmar então que se trata de dois direitos diversos, característicos e próprios, ao passo que a proteção de dados pessoais também apresenta seus princípios estruturantes e fundantes.

2.6. Os principais princípios de proteção dos dados pessoais

Com a base na autodeterminação informativa, o titular dos dados pessoais faz jus a concretização de determinados princípios que deverão nortear as atividades dos responsáveis pelo tratamento de dados pessoais, o comportamento dos indivíduos envolvidos e dos demais que relacionam-se nos meios virtuais.

Atualmente, o Brasil não conta com uma legislação própria do direito à proteção dos dados pessoais. No entanto, os três projetos de lei em tramite no Congresso Nacional foram inspirados no direito europeu italiano.[147]

Em razão das raízes com sistema romano-germânico e com um quadro avançado de tutela, optou-se por abordar o modelo europeu de proteção de dados pessoais ao tratar da questão principiológica. Em contrapartida, relevante destacar os princípios estampados na *Guidelines on The Protection of Privacy and Transborder Flows of Personal Data* da OCDE em 1980 e se tornaram um padrão para o modelo jurídico europeu e também foram replicados em alguns diplomas legais. Na OCDE são previstos o Princípio de Limitação da Coleta (*Collection Limitation Principle*), Principio de Qualidade dos Dados (*Data Quality Principle*), Princípio de Especificação dos Propósitos (*Purpose Specification Principle*), Princípio do Uso Limitado (*Use Limitation Principle*), Princípio da Garantia de Segurança (*Security Safeguards Principle*), Princípio da Transparência (*Openness Principle*), Princípio da Participação Individual (*Individual Participation Principle*) e Princípio da Responsabilidade (*Accountabilitu Principle*). Esses oito princípios basilares para a proteção de dados pessoais constituem o seguinte:

[146] O modelo europeu, portanto, assertivamente dispõe a privacidade como direito diverso da proteção dos dados pessoais. Segue trecho original: "*Article 7 - Respect for private and family life: Everyone has the right to respect for his or her private and family life, home and communications*". *Charter of Fundamental Rights of the European Union. 2000.*

[147] Os projetos de Lei em trâmite no Brasil são: PL 330/2013 proposto pelo Senado; PL 4060/2012 proposto pela Câmara; PL 5276/2016 proposto pelo Ministério da Justiça que contou com participação popular.

1. Princípio de limitação da coleta
A coleta de dados pessoais deveria ser limitada e qualquer desses dados deveria ser obtido através de meios legais e justos e, caso houver, informando e requerendo o consentimento do sujeito dos dados.
2. Princípio de qualidade dos dados
Os dados pessoais deveriam ser relacionados com as finalidades para os quais foram tratados e, na medida necessária, devem ser exatos, completos e permanecerem atualizados.
3. Princípio de Especificação dos Propósitos
Os propósitos da coleta de dados pessoais devem ser indicadas no momento da coleta de dados ao mais tardar e o uso subsequente limitado à realização destes objetivos ou de outros que não sejam incompatíveis e que sejam especificados cada vez que mudar o propósito.
4. Princípio do Uso Limitado
Dados pessoais não deveriam ser divulgados, comunicados ou utilizados com finalidades outras das que foram especificadas de acordo com o Parágrafo 9, salvo:
a) com o consentimento do sujeito dos dados; ou
b) por força de lei.
5. Princípio da Garantia de Segurança
Back-up de segurança regulares deveriam proteger os dados pessoais contra riscos tais como perda, ou acesso, destruição, uso, modificação ou divulgação desautorizados de dados.
6. Princípio da Transparência
Deveria haver uma política geral de abertura ou transparência a respeito do desenvolvimento, da prática e da política referentes a dados pessoais. Deveriam estar prontamente disponíveis meios de estabelecer a existência e natureza de dados pessoais, as finalidades principais de seu uso, bem como a identidade e residência habitual do controlador de dados.
7. Princípio da Participação Individual
Um indivíduo deveria ter o direito de:
I. obter do controlador de dados, ou por outro meio, a confirmação de que este possui ou não dados referentes a ele;
II. de que lhe sejam comunicados dados relacionados a ele:
a) dentro de um prazo razoável;
b) por um preço, caso houver, que não seja excessivo;
c) de maneira razoável; e
d) de modo prontamente compreensível para ele;
III. obter explicações caso for rejeitado um pedido feito conforme o disposto nos subparágrafos I e II, e ter meios de contestar tal recusa; e
IV. contestar dados relacionados a ele e, se a contestação for recebida, pedir que os dados sejam apagados, retificados, completados ou modificados.
8. Princípio da Responsabilidade
O controlador de dados (*data controller* ou responsável) terá de prestar contas pela observância das medidas que dão efeito aos princípios acima indicados. (Tradução livre)[148]

[148] De acordo com o texto original: *"**Collection Limitation Principle:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. **Data Quality Principle:**. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. **Purpose Specification Principle:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. **Use Limitation Principle:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law. **Security Safeguards Principle:** Personal data should be protected by reasonable security safeguards against such*

A partir desse documento, como referenciado anteriormente, criou-se a Convenção de Estrasburgo de 1981, conhecida também como Convênio nº 108 do Conselho da Europa que, do mesmo modo, elencou cinco princípios inspirados na citada *Guidelines*, quais sejam o da publicidade, da exatidão, da finalidade, do livre acesso e da segurança física e lógica[149], que apresentam certo consenso na matéria, razão pela qual merecem ser destacados.

2.6.1. Princípio da transparência ou da publicidade

O princípio da transparência dita que a existência de um banco de dados pessoais não pode ser acessado por uma minoria, muito pelo contrário, o público deverá ter conhecimento sobre ele com algumas prerrogativas como pedido de relatórios periódicos de atividades, exigência que o responsável pelo banco de dados obtenha uma autorização prévia de funcionamento e, na sua ausência ou infringência de norma, o interessado também poderá notificar a autoridade, seja um juiz, delegado ou autoridade garante para informar a respeito de eventual transgressão. [150]

Além disso, o princípio da transparência garante que o uso dos dados pessoais deve ser divulgado ao titular que deverá ter o conhecimento de que, em determinadas circunstancias, ao contratar um serviço pelo site da internet, o provedor de aplicações efetuará a coleta de seus dados enquanto utiliza o serviço fornecido.

---

risks as loss or unauthorised access, destruction, use, modification or disclosure of data. ***Openness Principle:*** *There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.* ***Individual Participation Principle:*** *An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.* ***Accountability Principle:*** *A data controller should be accountable for complying with measures which give effect to the principles stated above".* Disponível em: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part2>. Acesso em: 02.11.2017.

[149] Tais princípios estão respectivamente presentes nos artigos 5º, 7º e 8º da Convenção de Estrasburgo de 1981.

[150] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006, p. 216.

2.6.2. Princípio da exatidão

O princípio da exatidão garante exatamente a qualidade dos dados pessoais que devem ser transparentes, exatos, relevante e atuais ao contexto que foram coletados. Está previsto no artigo 5º da Convenção de Estrasburgo[151], porém o item "d" revela que os dados pessoais devem ser exatos e, se necessário, permanecerem atualizados. Ora, inegável que a atualização constante é necessária para que os dados pessoais sejam exatos, o que revela certo contrassenso para o sistema protetivo.

Assim, por tal princípio, assegura-se ao usuário a faculdade jurídica de atualização, de modificação, de retificação, de inclusão e de remoção de dados pessoais que não traduzam a realidade fática objetivamente. Além disso, o tratamento de dados não poderá ser excessivo, inadequado, impertinente em relação à finalidade declarada, podendo o usuário requerer a sua extidão. [152]

2.6.3. Princípio da finalidade

O princípio da finalidade também preocupa-se com a utilização dos dados pessoais, segundo o qual deve ser realizado de acordo com a finalidade para qual foi autorizado o seu tratamento. Logo, antes do dado ser coletado, o responsável deverá informar porquê, para quem, como e qual será o uso dos dados pessoais.

Segundo Doneda, considera-se que o princípio da finalidade deve ser tratado como princípio corolário de proteção de dados pessoais no sentido de que a informação vincula-se ao titular e deste nunca se afasta, ou seja, "antes de ser meramente abstrata e sujeita à livre disposição, esta informação, à medida que identifica alguma característica de uma pessoa, permanece sempre vinculada a ela, e sua utilização pode refletir diretamente para o

[151] Confere com original: "*Article 5 – Quality of data Personal data undergoing automatic processing shall be:* (...) *c adequate, relevant and not excessive in relation to the purposes for which they are stored;* d accurate and, where necessary, kept up to date;(...)".

[152] MENDES, LAURA Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 71/72.

seu titular". [153] Assim, é extremamente importante a conexão da informação, sua origem e os motivos de sua coleta.

Por meio deste princípio, proíbe-se a transferência de dados pessoais a terceiros sem a anuência do titular. Isto é, a vontade inicialmente manifestada de aceitação do tratamento de seus dados pessoais está vinculada a determinado propósito que deverá ser respeitado.

2.6.4. Princípio do livre acesso

O princípio do livre acesso garante que o usuário tenha acesso aos seus dados, independentemente do local que esteja armazenado, meio pelo qual poderá requisitar informações, cópias dos registros, corrigir informações e excluir outras. Em outras palavras, o banco de dados deverá estar sempre disponível para o titular de dados pessoais.[154]

Do livre acesso decorrem diversos direitos e garantias dos titulares de dados como o acesso, a retificação, a oposição e o cancelamento que será objeto de análise em tópico próprio.

É de extrema importância que o livre acesso não seja desobedecido já que seria uma afronta a um dos princípios corolários do sistema protetivo em voga, inerente para que um tratamento de dados pessoais seja realizado de maneira legítima e lícita.

2.6.5. Princípio da segurança dos dados pessoais

O princípio da segurança dos dados pessoais estabelece um comando para o responsável pelo seu tratamento que deverá garantir a segurança física e lógica contra a

[153] DONEDA, Danilo. Princípios de proteção de dados pessoais. In: LUCCA, Newton de. FILHO, Adalberto Simão. LIMA, Cíntia Rosa Pereira de. (coords.) *Direito & Internet III – Tomo I: Marco Civil da internet (Lei º 12.965/2014)*. São Paulo: Quartier Latin, 2015, p. 378.

[154] Desa forma, Sampaio entende que o livre acesso liga-se com a transparência: "o princípio da transparência pouco valeria se a ele não se associasse um outro: o princípio do livre acesso do individuo ao banco de dados, onde informações a ele pertinenetes estiverem armazenadas". SAMPAIO, José Adércio Leite. *Direito à intimidade e à vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte.* Belo Horizonte: Del Rey, 1998, p. 518.

adulteração, destruição, desvios, extravios e acesso indevido aos dados pessoais, inclusive, seja nos meios virtuais ou não.

Nesse sentido, Sampaio dita que "os dados de caráter pessoal devem ser correta e eficazmente protegidos contra riscos de extravio e de destruição, uso, modificação, transmissão ou acesso não autorizados". [155]

Asseguram-se, assim, as boas práticas e normas de *compliance* pelas empresas ou pessoas naturais que devem proteger tais dados contra invasões, bem como o seu uso ilícito.

2.7. O tratamento dos dados pessoais

Da criação do primeiro computador eletrônico digital ENIAC (*Eletronic Numerical Integrator and Calculator*) em 1946 até os computadores para uso da população em geral como o lançamento da empresa IBM em 1981, o tratamento automatizado de dados em grande escala passou a ser uma das consequências desse fenômeno. [156]

Os milhares computadores lançados detém uma enorme capacidade de transformar dados em informação valiosa. Os usuários da Web são notificados para fornecerem os seus dados pessoais e assim o fazem sem notar que a venda de dados é um "negócio lucrativo". [157]

[155] SAMPAIO, José Adércio Leite. *Direito à intimidade e à vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte.* Belo Horizonte: Del Rey, 1998, p. 518.

[156] Para curiosidade sobre como surgiu a ideia do computador pessoal, entre outros aspectos tecnológicos, sugere-se MANEY, Kelvin. et. al. *Tornando um mundo melhor*. New Jersey: IBM Press, 2011. Disponível em: <ftp://public.dhe.ibm.com/la/documents/imc/br/news/events/book_centennial/2011_09_14_0516_Tornando_O_Mundo_Melhor_PDF.pdf.>. Acesso em: 30.09.2017.

[157] Conforme o trecho: "Todos os dias somos solicitados a divulgar dados sobre nós mesmos. Na maioria das vezes, o fazemos sem pensar duas vezes. Aceitamos a solicitação como necessária, e, mais importante, os dados serão usados apenas para a finalidade para a qual foram fornecidos. O que não conseguimos perceber é que, atualmente, mais do que nunca, nossos dados estão sendo processados e compartilhados, muitos deles sem a nossa permissão ou conhecimento. As empresas descobriram que a venda de dados é um negócio lucrativo. Infelizmente, os dados que elas vendem são nossos. Dados demográficos, sobre tendências de compras e preferências pessoais tornaram-se valiosos para as organizações que tentam vender seus produtos em um mercado altamente competitivo. Por esta razão, a indústria de dados é muito lucrativa". STAIR, Ralph M. *Princípios de Sistemas de Informação: uma abordagem gerencial*. Trad. Maria Lúcia Iecker Vieria e Dalton Conde de Alencar. 2 ed. Rio de janeiro: LTC Editora, 1998, p.112.

Para tanto, a figura do banco de dados surgiu como "um conjunto de informações organizadas segundo uma determinada lógica" [158], cuja serventia seria o armazenamento para posterior uso conforme determinado fim.

Ocorre um processo quantitativo e qualitativo dos dados que são processados e o que se obtérm são as referencias da própria pessoa. Atualmente, diversas técnicas foram criadas para que o tratamento de dados gere informações. Dessa forma, explica Doneda:

> O mero fato da informação ser processada por computadores representa, por si, uma mudança nos efeitos de seu tratamento. Alguns desses efeitos são mensurados quantativamente, isto é, são decorrência do maior volume de informação que pode ser processado. Não é somente a quantidade de informação que diferencia o tratamento informatizado, mas também novos métodos, algoritmos e técnicas podem ser utilizados para este fim, operando igualmente uma mudança qualitativa no escopo do tratamento. [159]

A enorme quantidade de informação sobre as pessoas são obtidas por essas diversas técnicas automatizadas, cuja estrutura de rede aberta de computadores possibilita a sua transmissão e armazenamento na internet.

O tratamento de dados pessoais para ser considerado legal deve preencher algumas regras que, geralmente, não apresentam dissonância nas leis sobre o assunto, para qual se adota o conceito proposto na Diretiva 95/46/CE e no Regulamento 2016/679 da União Européia que muito se assemelham.

A Diretiva 95/46/CE compreende o tratamento em seu artigo 2º:

> b) «Tratamento de dados pessoais» («tratamento»), qualquer operação ou conjunto de operações efectuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, 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, apagamento ou destruição;.

O Regulamento Geral de Proteção de Dados Pessoais que entrará em vigor, no seu artigo 4º, (2), define o tratamento como:

> «Tratamento», 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

[158] DONEDA, Danilo. *Da privacidade...Op.cit.* p.158.
[159] Ibidem, p. 172.

> disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;.

Logo se verifica que toda operação realizada sobre dados pessoais ou um conjunto de dados pessoais ou um conjunto de operações, independente do meio ser ou não automatizado, caracteriza um tratamento de dados pessoais. Nesse ponto o Regulamento 2016/679 amplia o tratamento para abranger "um conjunto de operações efetuadas sobre conjuntos de dados pessoais", o que revela certa preocupação com as novas técnicas de aglomeração de dados proporcionada pelo uso do *Big Data*.

A coleta de dados pessoais caracteriza-se pelo ato de uma ou mais pessoas, físicas ou jurídicas, que recolhe, registra ou detém os dados fragmentados ou não de um individuo, podendo ter sido fornecidos ou observados pelo uso de ferramentas automatizadas.

Independente de o sujeito sofrer limitação cognitiva, estar inconsciente ou ser coagido, os dados fornecidos por ele caracterizam o ato de coleta e, por consequência, configura o tratamento de dados pessoais.

A coleta de dados pessoais poderá, em um segundo momento, ser processada para que então os provedores de aplicações consigam utilizar esses dados pessoais para o fim de serem contratados para anunciar publicidade dirigida para o usuário. É o que diz Reinaldo Filho sobre "a publicidade *on-line* emprega métodos e *softwares* especializados em mineração de dados (*data mining*), que permitem aos anunciantes definir o público-alvo de seus anúncios e quais informações ele visualiza". [160] Em outras palavras, a coleta de dados fornecidos e observados pode constituir-se em verdadeira *commodity*[161] para o responsável que lucra com o fluxo informacional.

Após a coleta dos dados, o seu processamento que antecede a etapa da utilização que, por sua vez, analisa e classifica os dados pessoais criando perfis (*profiling*) dos seus

[160] REINALDO FILHO, Demócrito. As "histórias patrocinadas do Facebook": os limites da utilização de dados pessoais no *marketing on-line*". *Revista Síntese Direito Empresarial*. São Paulo, ano 7, nº 38, p. 195, maio/jun. 2014.

[161] Alexander Galvão assim explica: "A nova classificação de um setor informacional no qual a informação é tida, essencialmente, como commodity corrobora a impressão de que a emergência de uma sociedade da informação, baseada em uma economia da informação, não parece confirmar-se na produção de semicondutores de silício, computadores e similares. O 'pós-industrial' parece, desta forma, afirmar-se em uma economia da informação na qual parte significativa do valor econômico não repousará nos chips ou nas redes telemáticas, mas sim nos grandes fluxos de informações (notícias, entretenimento, educação e conhecimento em códigos digitais) proporcionados pela ligação dos microcircuitos (encapsulados em diversos produtos materiais) com as redes de telecomunicações com capacidades de tráfego e ubiqüidade crescentes." GALVÃO, Alexander Patêz. A informação como *commodity*: mensurando o setor de informações em uma nova economia. *Ciência da Informação*. V. 28, n. 1, Brasília: IBICT, 1999. Disponível em: http://revista.ibict.br/ciinf/article/view/861/895. Acesso em: 01.10.2017.

usuários. Cada vez que se armazena um dado relativo ao individuo, *dossies* digitais são montados. [162]

A disseminação de dados pessoais nada mais é que a sua transmissão seja por difusão ou qualquer outra forma de disponibilização, isto é, notadamente, a "comercialização" de dados pessoais.

Certo que uma das problemáticas que envolvem a disseminação de informações é a sua tutela justamente em razão da transferência transfronteiriça de dados pessoais, ou seja, a sua circulação entre governos, corporações e indivíduos que estejam em países diferentes.

2.8. Garantias e direitos subjetivos do titular dos dados pessoais

O poder de controle da coleta, processamento, transmissão, uso, armazenamento e conservação dos dados pessoais, entre outras operações, requer que sejam atribuídos certos direitos ou faculdades como pressupostos do exercício regular de direito pelo seu titular em face dos responsáveis perante as autoridades judiciais e administrativas.

Em realidade os direitos e garantias são um reflexo dos princípios que os responsáveis deverão acolher e diligenciar para o seu fiel cumprimento. Dessa forma, foram eleitos quatro principais direitos que os usuários possuem que apresentam certo consenso nas legislações europeias e também no Marco Civil da Internet no Brasil (Lei nº 12.965/2014).

2.8.1. De consentimento

O sujeito tem o direito de exigir que o seu consentimento seja fornecido para o tratamento dos seus dados, salvo exceções de interesse legítimo e interesse público. Elementar que o consentimento é pedra central para a proteção de dados pessoais[163].

[162] Nesse sentido, Alessandro Hirata assevera: "criam-se verdadeiros arquivos de informações de cada usuário, com os mais diferentes dados sobre o seu comportamento social, econômico e pessoal: tais informações podem ser utilizadas para os meios diversos fins". HIRATA, Alessandro. O *Facebook* e o direito à privacidade. *Revista de Informação Legislativa*, Brasília, v. 51, n. ja/mar. 2014, p. 17-27, 2014, p.20.

Quando não seja possível obter o consentimento para o tratamento de dados pessoais que são inferidos ou derivados em clara acepção de "dados extraídos de outros dados", outros mecanismos limitadores como uma política pública deverá delimitar a fronteira do que seria um interesse legítimo ou interesse público.

Até mesmo o consentimento para fins de tutela de dados fornecidos pelo titular e observados (por *cookies e* programas *espiões)* pode não ser suficiente perante as clausulas contratuais e políticas de privacidade colossais que demandariam grande tempo de leitura e que se mostram incompatíveis com a boa-fé objetiva dos internautas. Nesse sentido, Cintia Rosa Pereira de Lima alerta:

> O impasse é que, justamente pela complexidade na redação destes contratos, o usuário vê-se desestimulado a ler todos os termos e cláusulas contratuais, vendo-se "forçado" a concordar em bloco clicando numa declaração formulada pelo próprio fornecedor de que ele leu, entendeu e concorda com todos os termos da licença ou com todas as cláusulas do contrato. [164]

Ocorre que corriqueiras são as situações em que o titular efetivamente lê o que está aceitando. Por isso, as diretrizes de uso e finalidade de coleta de dados deve ser clara e destacada das clausulas contratuais, disposições que já eram obrigatórias no Brasil com o Código de Defesa do Consumidor e na Europa com a Diretiva 95/46/CE. Até o novo Regulamento Geral de Proteção de Dados Pessoais Europeu manteve tal disposição, porém modificou o que se entendia por consentimento. Não basta que o consentimento seja "inequívoco" (proposta da Diretiva 95/46/CE)[165], deverá ser "expresso" como uma forma dar uma maior certeza e probabilidade de que o titular efetivamente saiba com o que está

---

[163] Cintia Rosa assim defende: " (...) o consentimento é visto como elemento central da proteção de dados pessoais. Mas, para que sirva realmente ao seu propósito, o titular deve estar apto a tomar uma decisão plenamente consciente dos seus efeitos. O questionamento que se faz é de que maneira esse consentimento é coletado?" LIMA, Cíntia Rosa Pereira. *A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil*. Tese de Livre Docência apresentada junto à Faculdade de Direito de Ribeirão Preto. Ribeirão Preto: USP, 2015, p. 247-248.

[164] LIMA, Cíntia Rosa Pereira. O ônus de ler o contrato no contexto da "ditadura" dos contratos de adesão eletrônicos. In: *Direito e novas tecnologias*. Florianópolis: CONPEDI, 2014, p. 443-465. Disponivel em: http://publicadireito.com.br/artigos/?cod=981322808aba8a03. Acesso em: 01.10.2017.

[165] Verifica-se que a Diretiva 95/46 não tratava do consentimento expresso em sua definição: Art. 2º. "(...) h) «Consentimento da pessoa em causa», qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objecto de tratamento".

concordando. No Considerando 32 do novo Regulamento 2016/679 europeu assim esclarece:

> O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio *web* na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrónica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido. [166]

Ora, consentimento inequívoco poderia ser preenchido com o simples click na barra de rolamento (à direita) do arquivo no site. Apesar da vulnerabilidade do usuário, caminhou bem o modelo europeu com a necessidade do consentimento expresso como um direito que poderá ser exercido e reclamado perante a *Autoridade Garante*, órgão fiscalizador (âmbito administrativo), e o Poder Judiciário.

2.8.2. De acesso

O direito de acesso decorre do Princípio do Livre Acesso que garante não somente o acesso aos seus dados, mas ser informado da finalidade do seu uso e mantê-los no banco

[166] Na definição do citado Regulamento, artigo 4, (11): "«Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;" (grifo nosso). Regulamento nº 2016/679. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 31.09.2017.

de dados com objetividade e de fácil compreensão para que outros direitos sejam exercidos como o de retificação, oposição e cancelamento.

É o direito de se informar, ser informado e a autodeterminação informativa que assegura o controle da circulação de seus dados pessoais.

2.8.3. De retificação, oposição e cancelamento

Os direitos de retificação, oposição e cancelamento decorrem do direito do acesso, como outrora mencionado, no entanto, cada qual tem a sua particularidade. O direito de retificação assegura a correção dos dados pessoais quando forem estes incompletos, incorretos ou desatualizados. O direito de oposição se relaciona ao interessado se opor ao tratamento ilícito ou ilegal de seus dados pessoais, isto é, impedir que seja realizado. Por fim, o direito de cancelamento no sentido de revogação do consentimento outorgado ou da exclusão dos dados pessoais que foram indevidamente tratados. [167]

2.9. A proteção dos dados pessoais no Brasil e o Projeto de Lei nº 5.276/2016

A propósito de uma regulamentação específica para o direito à proteção de dados pessoais, o Brasil encontra-se atrasado na análise com o avançado modelo europeu já que não há uma lei semelhante positivada. A ausência de uma lei especial que tutele somente os dados pessoais, processados de forma automatizada ou não, provoca uma liberdade das empresas, governos e terceiros interessados de se valerem dos dados pessoais dos brasileiros, sem a garantia de um tratamento adequado, para obter proveito, principalmente, econômico com a sua utilização.

Em que pese isso, atualmente, existem leis esparsas que tutelam de certo modo a proteção de dados pessoais seguindo critérios e situações distintas como a Lei do Cadastro

[167] LIMA, Cíntia Rosa Pereira. *A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil*. Tese de Livre Docência apresentada junto à Faculdade de Direito de Ribeirão Preto. Ribeirão Preto: USP, 2015, p. 24253-254.

Positivo (Lei n 12.414/2011)[168], a Lei de Acesso à Informação (Lei n 12.527/2011)[169], o Código de Defesa do Consumidor (Lei nº 8.078/1990), o Marco Civil da Internet (Lei nº 12.965/2014) e seu Decreto Regulamentador (Decreto nº 8.771/2016).

Ao que interessa esse trabalho, abordar-se-ão o Código de Defesa do Consumidor e o Marco Civil da Internet já que se relacionam com o tema proposto.

Veja que, dificilmente, o usuário que navega na Web não se enquadrará na definição de consumidor uma vez que existe uma remuneração ainda que indireta, dos provedores de aplicação na internet. Os dados pessoais são assim utilizados como própria "moeda de troca" pelo serviço fornecido, como demonstrado no Capítulo I.

Igualmente, o contexto em que se transpõe a discussão do direito ao esquecimento, o direito à desindexação e à desvinculação de dados pessoais ocorre também a internet, o que justifica a consulta ao Marco Civil de Internet.

O Código de Defesa do Consumidor[170] inovou ao disciplinar os parâmetros legais em que os bancos de dados e cadastros dos consumidores podem funcionar no ordenamento jurídico brasileiro. Tal proeza está estipulada em seu artigo 43, o qual prevê o direito de livre "acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes". Além disso, observa-se o direito de correção, derivado do princípio da exatidão, do consumidor que poderá exigi-lo imediatamente do fornecedor. A obrigação de transparência dos fornecedores também está explicita no artigo na medida em que estes deverão manter os cadastros atualizados com dados objetivos, claros, verdadeiros e em linguagem de fácil compreensão, sem mencionar que as informações negativas só poderão ser mantidas pelo prazo máximo de 05 (cinco) anos. Por fim, o fornecedor deverá notificar de forma escrita o consumidor sobre o cadastro, exceto quando solicitado pelo próprio. [171]

---

[168] A Lei do Cadastro Positivo: "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". BRASIL. Lei n 12.414/2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12414.htm. Acesso em: 02.10.2017.

[169] A Lei de Acesso à Informação: "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; (...) e dá outras providências. BRASIL. Lei n 12.527/2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 02.10.2017.

[170] BRASIL. Lei nº 8.078/1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8078.htm. Acessado em: 02.10.2017.

[171] Conforme, previsão expressa do CDC: "Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3°

Conquanto a proteção dos dados pessoais estabelecida no Código de Defesa do Consumidor seja de grande valia, os direitos de correção, direito de livre acesso e de notificação ali previstos são limitados à relação entre consumidor e fornecedor, isto é, o individuo deverá se enquadrar na definição legal de consumidor e o responsável pela coleta na de fornecedor para a incidência dessas normas protetivas.

Ademais, o Código Consumerista não define tampouco limita o que venha a ser um dado pessoal, o que enfraquece a lógica de tutela do próprio consumidor, pois o fornecedor não possui o discernimento para compreender o que deve ou não armazenar, além daqueles dados básicos objetivos de identificação como, por exemplo, o nome, endereço, número de CPF.

O Marco Civil da Internet (MCI)[172] que estabelece os princípios, as garantias, os direitos e os deveres para o uso da internet no Brasil caminhou para suprir essa deficiência de conceituação dos dados pessoais, o que foi concretizada com o seu decreto regulamentador.

O artigo 14 do Decreto nº 8.771/2016[173] define que dado pessoal é um "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa", sendo o seu 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". [174] Assim sendo, qualquer desses atos que tenha ocorrido no contexto da internet, dentro do território nacional, caracteriza o

---

O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores".

[172] BRASIL. Lei nº 12.965/2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 02.10.2017.

[173] O Decreto nº 8.771/2016 regulamenta o MCI para tratar ainda das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

[174] BRASIL. Decreto nº 8.771/2016. Disponivel em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm. Acesso em: 02.10.2017.

tratamento de dados pessoais e justifica a aplicação do MCI, independentemente da sede da empresa, isto é, do provedor de aplicações ter estabelecimento no Brasil ou não.

O Marco Civil da Internet (MCI) foi além ao fixar a privacidade e a proteção de dados pessoais como um dos pilares de sustentação que deve se harmonizar com o valor da liberdade de expressão.

O fato é que a proteção de dados pessoais pode ser encontrada em quantidade expressiva de dispositivos do MCI como, por exemplo, o princípio da proteção de dados pessoais[175], os direitos e garantias dos usuários[176], a retenção de dados e guarda obrigatória de registros de conexão e de acesso[177] pelos provedores, entre outros.

Merece destaque a previsão do direito à exclusão no inciso X do artigo 7º do MCI que dividiu debates sobre este se tratar do direito ao esquecimento na internet ou uma de suas facetas, especificamente, no Brasil, o qual dispõe que é assegurada a "exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei" (grifo nosso), o que, desde já, adianta-se ao afirmar que este seria um direito mais relacionado com a seara contratual e com a proteção de dados pessoais do que com a privacidade e identidade da pessoa humana. Importante

[175] Segundo o artigo 3º do MCI: "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: (...) II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; (...)".

[176] Conforme, o artigo 7º do MCI que prevê o consentimento expresso sobre o tratamento de dados pessoais, entre outros direitos que se destaca: "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - *inviolabilidade e sigilo de suas comunicações privadas armazenadas*, salvo por ordem judicial; IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização; V - manutenção da qualidade contratada da conexão à internet; VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade; VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet; XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet". (Grifo nosso)

[177] Tal garantia está previstas em diversos artigos estão inseridos no Capítulo III do MCI.

esclarecer que atingida a finalidade do uso do dado pessoal, os provedores deverão excluí-los de seus bancos de dados.

Pois bem, registre-se que o consentimento expresso sobre o tratamento de dados pessoais é também eleito como um dos mecanismos de tutela do usuário da internet no Brasil. De igual modo, a transmissão dos dados para terceiros deverá ocorrer mediante prévia notificação e previsão contratual destacada feita pelo provedor de aplicação ao titular dos dados.

O Marco Civil da Internet também prevê sanções como advertência, multa de até 10% (dez por cento) do faturamento do grupo econômico no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção, suspensão temporária das atividades que envolvam tratamento de dados e proibição de exercê-lo[178], para o caso de descumprimento da norma a fim de torná-la efetiva.

Importante ressaltar que o próprio MCI, em seu artigo 2º, inciso III, dispõe que "a proteção de dados pessoais deve se dar nos termos da lei", mencionando a necessidade da existência de uma legislação geral de proteção de dados pessoais que não circunscreva somente aos contornos da internet.

Quanto às iniciativas legislativas no país, ao menos, três projetos de lei que buscam sistematizar a matéria a fim de estabelecer um microssistema de proteção de dados pessoais que seja abalizado na autodeterminação informativa, na dignidade da pessoa humana e no desenvolvimento de sua personalidade. São eles: PL nº 330/2013 proposto pelo Senado; PL nº 4060/2012 proposto pela Câmara; PL nº 5276/2016 proposto pelo Ministério da Justiça que contou com participação popular. [179]

[178] É o que se transcreve do art. 12 do MCI: "Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção; III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11. Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o **caput** sua filial, sucursal, escritório ou estabelecimento situado no País".

[179] Para maior aprofundamento, sugere-se: BIONI, Bruno. *Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil*. Grupo de Estudos em Políticas Públicas em Acesso à Informação da USP – GPOPAI. 2015. Disponível em: http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf. Acesso em: 02.10.2017.

Dentre eles, destaca-se o Projeto de Lei nº 5276/2016 como o mais completo do ponto de vista acadêmico ao passo que elenca as definições de dados pessoais e seu tratamento para demonstrar em quais situações essa lei de proteção será aplicável.

Além disso, é fruto de alto debate em todos os setores e ainda nota-se que se inspirou nas diversas disposições do modelo de proteção de dados europeu.

As definições de dados pessoais e de tratamento de dados propostas pelo citado Projeto de Lei são as mesmas dispostas pelo Decreto Regulamentador do Marco Civil da Internet. No entanto, o referido Projeto de Lei incluiu a definição do que são dados sensíveis e aprovou o seu tratamento com certas restrições.

Cumpre ressalvar, porém, que em alguns dispositivos o mencionado projeto confunde proteção de dados pessoais com a privacidade, o que pode ser observado pela expressa previsão no art. 2º que elenca a privacidade como fundamento da proteção de dados pessoais, o que não se sustenta pelo o que foi exposto neste Capítulo. [180]

O Projeto de Lei nº 5.276/2016 incide nas operações de tratamento de dados realizadas no território nacional, até no tratamento de dados com o escopo de fornecer bens ou serviços ou tratamento de dados de indivíduos localizados no território nacional; por fim, nos dados pessoais objeto de coleta no território nacional. [181] Nota-se certa redundância no texto já que a coleta de que diz respeito à terceira hipótese está incluída na definição de tratamento de dados da primeira hipótese por definição legal.

Todavia, não se aplica em: a) tratamentos realizados por pessoa natural para fins exclusivamente pessoais; b) tratamentos para fins exclusivamente jornalísticos, artísticos, literários ou acadêmicos; c) tratamentos para fins exclusivos de segurança pública, defesa nacional, segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais. [182]

Por fim, prevê a atuação de um órgão fiscalizador para combater os desvios legais, sedimentar as orientações sobre a interação entre a Tecnologia e o Direito, autorizar códigos de boa conduta e julgar ainda os apelos dos interessados em proteger os seus dados

[180] Interessante as argumentações desenvolvidas pela professora Cíntia Pereira de Lima que participou de audiência na Câmara dos Deputados para proferir a sua visão sobre o PL nº 4.060 de 2012. Além disso, destacou que o PL 5276/2016 é o mais completo, porém também verificou algumas inconsistências, das quais se compartilha, principalmente, a confusão técnica entre privacidade e proteção dos dados pessoais. Ver: LIMA, Cíntia Rosa Pereira. *Parecer técnico encaminhado para a Comissão Especial destinada a proferir Parecer ao Projeto de Lei nº 4.060 de 2012, do Deputado Milton Monti, que dispõe sobre o tratamento de dados pessoais e dá outras providências*. Disponível em: http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/dra-cintia-rosa-pereira-de-lima-usp. Acesso em: 06.12. 2017.

[181] Conforme transcrição do art. 3º do PL nº 5276/2016.

[182] Conforme transcrição dos incisos do art. 4º do PL nº 5276/2016.

pessoais, o que, como entidade administrativa, não afastará de modo algum o controle do poder jurisdicional. Essas entre outras tantas competências, o projeto se refere ao "órgão competente" fiscalizador e o "Conselho Nacional de Proteção de Dados e da Privacidade" para implementar políticas públicas, sugerir estudos e debates. Fato é que ambos os órgãos deverão zelar pelos princípios e sistema protetivo dos dados pessoais.

CAPÍTULO III – O FUNCIONAMENTO E A ATIVIDADE DOS MOTORES DE BUSCA

3.1. Internet: do passado ao futuro

A internet permite a comunicação em escala global ao passo que depara-se com um novo mundo, a Galáxia da Internet[183], justamente pelo o seu uso de forma crescente e veloz no final da década de 90 que transformou o planeta Terra e superou barreiras para ser o alicerce tecnológico da sociedade em rede e informacional.

O primeiro ano da utilização aberta da *World Wide Web*, um dos recursos que a internet oferece, que se deu em 1995, havia cerca de 16 milhões de usuários da rede de computadores no mundo. Tal número cresceu para 400 milhões em 2001. Desde então, após catorze anos, contamos com aproximadamente 3,2 bilhões de usuários mundialmente. [184]

Caracterizou-se quase que uma onipresença da internet, o que jamais foi previsto quando de sua criação. De início, os pesquisadores foram contratados para criar a internet como instrumento para fins militares e não para a pesquisa, comunicação e compartilhamento de informações entre particulares, empresas e Estados.

Em 1969 deu-se a constituição da internet com a Arpanet, uma rede de computadores montada pelo *Advanced Research Projects Agency* (conhecido pela sigla ARPA) formado pelo Departamento de Defesa dos Estados Unidos. O objetivo do ARPA era angariar recursos de pesquisa, especialmente, das universidades e indústrias, para que os Estados Unidos se tornasse uma potência tecnológica militar em resposta ao lançamento do primeiro Sputinik[185] ocorrido no dia 04 de outubro de 1975 pela União Soviética.

A construção da internet se tornou possível por causa do visionário J.C.R. Licklider, professor de psicologia experimental do Instituto de Tecnologia de Massachutes

[183] A referência à "Galáxia da Internet", expressão alcunhada por Manuel Castells, foi inspirada no termo criado por Macluhan conhecido de "Galáxia de Gutenberg" em homenagem ao criador da máquina impressora no Ocidente. CASTELLS, Manuel. A galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade. Traduzido por Maria Luiza X. de A. Borges; revisão Paulo Vaz. Rio de Janeiro: Zahar, 2003, p. 8.

[184] Segundo dados estatísticos do ITU (Internacional Telecommunication Union), órgão da ONU especializado no estudo das tecnologias da informação e da comunicação. Disponível em: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf. Acesso em: 06.07.2016.

[185] Primeiro satélite artificial que orbitou a Terra por seis meses.

(MIT) que se dedicava ao estudo entre os seres humanos e as inovações tecnológicas. Foi Licklider que teve a ideia de uma rede sem fio interligando computadores através de sistema de comunicação.

Da psicologia para a engenharia da computação, Licklider tornou-se o primeiro Diretor do Departamento de Técnicas em Processamento de Informação do ARPA (IPTO – *Information Processing Techniques Office*), cujo ARPANET era um de seus programas.

O Departamento de Técnicas em Processamento de Informação do ARPA (IPTO) tinha como objetivo estudar a computação interativa que se concretizou pelo uso de uma tecnologia revolucionária de transmissão de telecomunicações chamada de comutação por pacote de dados, desenvolvida na *Rand Corporation*. A ideia principal era que a rede de computadores descentralizada e flexível, por meio do uso dos pacotes de dados, pudesse evitar que as comunicações militares fossem interrompidas e perdidas em razão de ataques nucleares. O funcionamento se dava por mensagens fracionadas assim como pequenos pacotes, cada um com seu caminho, empregando-se de variados meios físicos, como por exemplo, as linhas telefônicas, cabos óticos, sinais de radio, micro-ondas e satélites, para chegar ao destinatário final, onde esses pacotes seriam remontados como se fosse um quebra-cabeça.

A mesma tecnologia de transporte de informações por meio de pacotes de dados foi utilizada no projeto Arpanet que conectou quatro computadores: três no Estado da Califórnia (nas Universidades de Stanford, Berkeley e na UCLA) e um na Universidade de Utah.

Além disso, após o projeto Arpanet continuou a ser executado em colaboração com outros centros de pesquisa e redes de computadores. Para que a comunicação entre as redes de computadores ocorresse, o uso de protocolos de comunicação padronizados foi a solução dada por Vint Cerf, Gerard Lelann (do grupo de pesquisa francês) e Robert Metcalfe (do Xerox PARC) que idealizaram o protocolo de controle de transmissão, mais conhecido como TCP – *Transmission Control Protocol*, em 1973, durante a apresentação de um seminário em Stanford.

Em seguida, em 1978, pelos esforços do grupo Network Working Group, Vint Cerf, Postel e Crocker, criaram um protocolo intrarrede (IP) e o acrescentaram ao TCP, tendo sido o código padrão conhecido até hoje, o TCP/IP.

A National Science Foundation (NSF), órgão do governo americano, por volta de 1974, montou sua própria rede de comunicações entre computadores denominada de NSFNET e começou a gerenciar a Arpanet como seu *backbone* ou infraestrutura.

Em fevereiro de 1990 terminou o programa da Arpanet, pois se apresentava obsoleto. Por outro lado, no mesmo ano, o físico Tim Berners-Lee[186] desenvolveu a *World Wide Web*, mais conhecida como Web, como consequência de sua pesquisa no *European Particle Physics Laboratory* (CERN), situado na Genebra, que nada mais é que um conjunto de protocolos que permite a criação, na Internet, de *home pages*, com texto, som, imagens, vídeos, cuja leitura é feita em camadas por meio de *hyperlinks*. Em síntese, Tim criou o protocolo HTTP (*Hipertext Transfer Protocol*) usado para transferir arquivos na Web.

Relevante destacar que existem diferenças entre a Web e a Internet:

> A World Wide Web (www) – uma teia de aranha mundial – é conhecida como a área onde se colocam páginas com informação, texto, gráficos, clipes de som e vídeo. As páginas ligam-se entre si por 'hyperlinks' (hppl), o que proporciona a possibilidade de 'navegação' pelos conteúdos das mesmas. [...] A World Wide Web, ao permitir essa simples e intuitiva navegação pelos 'sitios' da Internet, através de uma interface amigável, expandiu-se espetacularmente na década de 90 e tornou-se na mais importante componente da Internet, como meio de comunicação e interação entre as pessoas, bem como de transmissão de informação sem que a localização geográfica tenha qualquer influência.[187]

A expansão do uso da internet apenas se deu em decorrência da criação do recurso *World Wide Web*, cuja interface corrobora para o acesso e tráfego de informações. [188]

Na verdade, tal desenvolvimento ainda ocorreu pelo acesso livre e aberto aos documentos básicos e sua infraestrutura, especialmente às especificações de seus protocolos. [189]

Da mesma maneira como a internet, a Web evoluiu com o passar dos anos, sendo possível se verificar duas fases ou estágios distintos. Na década de 90, a primeira fase da

---

[186] Conforme descrito por Manuel: "O que permitiu à Internet abarcar o mundo todo foi o desenvolvimento da www. Esta é uma aplicação de compartilhamento de informação desenvolvida em 1990 por um programador inglês, Tim Berners-Lee, que trabalhava no CERN, o Laboratório Europeu para Física de Partículas baseado em Genebra". CASTELLS, Manuel. A galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade. Traduzido por Maria Luiza X. de A. Borges; revisão Paulo Vaz. Rio de Janeiro: Zahar, 2003, p. 17.

[187] MARQUES, Garcia; LOURENÇO, Martins. *Direito da informática*. Coimbra: Almedina, 2000, p. 52.

[188] Não somente como mero expectador, o internauta, ou melhor, "qualquer pessoa, munida de um 'software' apropriado e com acesso a um computador 'hospedeiro', pode compor a suas páginas, o seu 'site' com informação facultável aos outros utentes da rede, através de um endereço próprio". MARQUES, Garcia; LOURENÇO, Martins. *Direito da informática*. Coimbra: Almedina, 2000, p. 52.

[189] MARQUES, Garcia; LOURENÇO, Martins. *Direito da informática*. Coimbra: Almedina, 2000, p. 53.

Web 1.0 caracterizava-se por ser "*the mostly read-only web*", ou seja, os usuários utilizavam a rede mundial de computadores exclusivamente para leitura online. Na sua segunda fase, Web 2.0, aprimorada de 2006 em diante, acrescentaram-se outros mecanismos como as aplicações que comportavam a criação de conteúdo de maneira colaborativa. [190]

A web 2.0 permite que, por exemplo, em sites como o Wikipédia de publicação coletiva, os usuários possam escrever e alterar os artigos; em blogs hospedados por sites como o WordPress e o Blogspot em que as pessoas escrevem sobre a sua vida e experiências, outros navegadores podem localizar os mais variados conteúdos, comentar e curtir, até receber sugestões de produtos e serviços feitas pelos blogueiros e que, nesses casos, são recompensados financeiramente ou com "presentes", tornou-se uma verdadeira indústria de publicidade e propaganda.

As redes sociais como o *Facebook* representam uma intensa troca de mensagens em tempo real, publicações ("posts") de opiniões, fotos e "check-ins", com a criação de perfis eletrônicos, onde preferencias musicais, interesses, histórico acadêmico e profissional, entre outros dados são disponibilizados à sua "lista de amigos", formando uma rede, a qual a privacidade pode ser limitada ou não.

Infinitas são as vantagens da rede colaborativa com a inserção de conteúdo e interação entre os navegadores da Web.

Bem verdade também que o uso de dispositivos móveis tais como os celulares, smartphones, *personal assistance* (PDAs), *notebooks*, *tablets*, com melhores configurações e organizações de seu conteúdo (softwares mais eficientes) corroboraram para o sucesso da Web ao apostar no acesso mais direto e facilitado aos aplicativos e recursos da rede.

Por isso, no início do século XXI, a internet se tornou um meio de comunicação em massa e que locomove também a economia.

A respeito do futuro da internet é necessário sempre apostar em novas ideias como Larry Page que com a *Google Inc* investe, no Projeto Loon, anunciado em junho de 2013, consistente no plano de usar balões de hélio para levar internet de banda larga a cinco

[190] Como bem explicitado pela Cíntia Rosa Pereira de Lima: "Em outras palavras, na primeira fase da web (1.0), a internet era utilizada basicamente como fonte de informação e como meio de comunicação (e-mails). Na fase seguinte, web 2.0, a internet é utilizada, além das maneiras antes citadas, como ferramenta potente de gerar conteúdo de maneira colaborativa e divulga-lo, permitindo inclusive que outras pessoas continuem a trabalhar com a ideia, curtindo, compartilhando, blogando, retwitando etc". LIMA, Cíntia Rosa Pereira. O conceito de tratamento de dados após o caso Google Spain e sua influência na sociedade brasileira. In: *III Encontro de Internacionalização do CONPEDI*. Madrid : Ediciones Laborum, 2015. V. 9., p. 120. Disponível também em: http://www.conpedi.org.br/wp-content/uploads/2016/03/Vol.-9-Madrid.pdf. Acesso em: 02.02.2016.

milhões de pessoas que ainda não tem acesso.[191] No entanto, decerto que o interesse da empresa não é apenas solidário e da inclusão digital. Quanto maior o número de usuários na Internet, maiores serão os dados trafegados e, consequentemente, maior será o seu lucro. Pois então, não se pode perder de vista a tutela dos usuários da Internet, o tratamento de seus dados de maneira consentida ou lícita perante uma internet neutra, democrática e regulamentada.

3.2.Funcionamento da internet e as ferramentas de busca

A internet[192] pode ser definida como uma rede global de computadores conectados entre si, cujo funcionamento se dá pelo sistema TCP/IP, o qual torna possível a comunicação entre diferentes computadores.

O protocolo de controle de transmissão (TCP) divide os dados em pacotes e, após a sua transmissão, reúne-os para formar novamente os dados originariamente transmitidos. O protocolo de internet (IP) adiciona a cada pacote de dados o endereço do destinatário para que alcancem o destino correto. Cada computador ou roteador participante do processo de transmissão de dados se vale do endereço constante nos pacotes para saber para onde encaminhar a mensagem. [193]

Existem diversas rotas que a transmissão de dados pode ocorrer de forma automática, mas no fim todos os dados chegam até o seu destino.

Os pacotes de dados contêm os endereços IP do remetente e do destinatário. Um endereço IP identifica certa conexão à internet em um determinado momento. Toda vez que um usuário se conecta a rede, seu computador recebe automaticamente de seu provedor de acesso um endereço de IP que é único durante aquela conexão e imprescindível para que o pacote de dados transmitidos chegue ao destinatário. Atualmente

[191] SCHMIDT, Eric. ROSENBERG, Jonathan. EAGLE, Alan. *Como o Google funciona*. Trad. André Gordirro. Rio de Janeiro: Intrinseca, 2015, p. 242.

[192] Pelo dicionário, a internet é definida como: "Qualquer conjunto de redes de computadores ligados entre si por roteadores e gateways, como, p. ex., aquela de âmbito mundial, descentralizada e de acesso público, cujos principais serviços oferecidos são o correio eletrônico (q.v.), o chat (q.v.) e a Web (q.v.), e que é constituída por um conjunto de redes de computadores interconectados por roteadores que utilizam o protocolo de transmissão TCP/IP." FERREIRA, Aurélio Buarque de Holanda. *Dicionário Aurélio da Lingua Portuguesa.* 5 ed. Curitiba: Editora Positivo, 2010, p.1175.

[193] LEONARDI, Marcel. Internet: elementos fundamentais. In: SILVA, Regina Beatriz Tavares da. (coord.) Et al. *Responsabilidade Civil na Internet e nos demais meios de comunicação.* 2 ed. São Paulo: Saraiva, 2012, p. 80 – 81.

as principais formas de transmissão são a *world wide web*, o correio eletrônico e o *chat*, entre outros.

Dessa forma, cotidianamente, o que se intensificou foi o uso da *world wide web* que se dá mediante a digitação do endereço eletrônico na rede, propiciando o acesso a determinado site[194] ou conteúdo na web, representado pelo nome de domínio.

O usuário, todavia, nem sempre tem à sua disposição o endereço eletrônico ou a relação deles para localizar a informação, texto, imagem, produto, vídeo, entre outros, que procura na rede. Para facilitar o acesso e impulsionar o uso da web é que existem as ferramentas de busca, as quais merecem destaque os dois tipos que são mais utilizados: os diretórios e os motores de busca.

Compreender as características dos motores de busca é de extrema importância para se analisar no que consiste o direito ao esquecimento na sociedade informacional, sobre a remoção de informações pessoais ou apenas a sua desvinculação ao nome da pessoa (também conhecido como desindexação) dos resultados de pesquisa.

A diferenciação entre motores de busca e diretórios deve ser contemplada a fim de que se delimite melhor quais são os buscadores da web e suas características, cujos usuários podem se insurgir e invocar o clamado direito ao esquecimento, a desindexação e desvinculação de dados pessoais.

3.2.1. Diretórios

Os diretórios precederam os motores de busca e foram criados quando o conteúdo da web ainda era pequeno e, por isso, a coleta de dados não era automática e tampouco o tráfego de informações era tão expressivo.

Em verdade, a função dos diretórios era organizar os sites da web que compõe a sua base de dados em categorias e subcategorias. Dessa forma, cabeçalhos dos assuntos são distribuídos na página e os usuários acessam um vocabulário controlado. [195]

[194] Website é um conjunto de páginas da web que e cada página possui no seu conteúdo documento composto por hipertexto e através deste que ligações são efetuadas na rede.

[195] Para se compreender melhor sobre as diferenças entre diretórios e motores de busca, vale consultar o artigo da Beatriz Valadares Cédon intitulado de *Ferramentas de Busca da Web*. In: Revista C. Informática. Brasília, v. 30. n.1. Jan./Abr. 2001, p. 39-49. Disponível em: http://www.scielo.br/pdf/ci/v30n1/a06v30n1. Acesso em: 25.05.2016.

Os sites coletados e armazenados no banco de dados dos diretórios são, geralmente, selecionados por pessoas, editores que tomam conhecimento de novos sites seja por anúncios de pesquisa na Internet, por sugestões dos próprios usuários ou por robôs que coletam os endereços eletrônicos. Em outras palavras, ocorre uma escolha determinada por certos critérios que atribuem a relevância ao site ou documento realizada pelos editores.

Importa mencionar que em novembro de 1992 foi lançado o primeiro diretório chamado de *The World Wide Web Virtual* (http://vlib.org/)[196] também criado por Tim Berners-Lee no CERN, em Genebra, que funciona até os dias atuais com a ajuda de especialistas e de um conselho consultivo. Todavia, este não ficou tão conhecido quanto o Yahoo Directory[197], outro diretório de pesquisa que se encerrou em 2014, mas que apresentava os resultados de forma hierárquica e em pastas. Outros exemplos de diretórios que subsistem são o *Open Directory Project* (https://www.dmoz.org/) e o *Best of The Web* (https://botw.org/).

Os diretórios prezam pela qualidade dos sites que anunciam e, muitas vezes não dirigem propagandas e podem se associar á bibliotecas, instituições de ensino ou profissionais da tecnologia da informação. Podem ser avaliativos e temáticos como é o caso do *Civil Rights Litigation Clearing House* (http://www.clearinghouse.net/), ligado à Universidade de Direito de Michigan, que coleta documentos e informações sobre processos judiciais civis nos Estados Unidos e os distribui em categorias para a pesquisa do usuário. O *Clearing House* ainda avalia os conteúdos e possui uma política de transparência sobre quais sites são selecionados por seus editores, especialistas.

Devido ao crescente número de usuários da web e que, cada vez mais, valem-se da internet para adquirir conhecimento, deixando de lado livros impressos para navegar nos *e-books* (livros eletrônicos), procurar por informações, notícias em páginas de sites, que

[196] No site da livraria virtual é possível conhecer a sua história e origem, como podemos ver: "*The WWW Virtual Library (VL) is the oldest catalogue of the Web, started by Tim Berners-Lee, the creator of HTML and of the Web itself, in 1991 at CERN in Geneva. Unlike commercial catalogues, it is run by a loose confederation of volunteers, who compile pages of key links for particular areas in which they are expert; even though it isn't the biggest index of the Web, the VL pages are widely recognised as being amongst the highest-quality guides to particular sections of the Web.*" Disponível em: http://vlib.org/admin/AboutVL. Acesso em: 08.06.2016.

[197] O site do Yahoo Directory, antes de se tornar o motor de busca que é hoje (Yahoo Search), era um diretório de outros sites criado em 1994, por dois estudantes da Universidade de Stanford, Jerry Yang e David Filo, que, de início, chamavam o seu site de "*Jerry and David's Guide to the World Wide Web*". Depois de um ano de funcionamento, o site recebeu mais de um milhão de acessos, o que ficou claro que ali havia um interesse de muitas pessoas. Entretanto, com a vinda de motores de busca como o Google, o número de usuários teve uma queda gradativa, sendo que, no dia 31 de dezembro de 2014, foi oficialmente desativado. ZECHMAN, Ashley. *So long, Farewell, Auf Wiedersehen* Yahoo Directory. Disponível em: https://searchenginewatch.com/sew/news/2373344/so-long-farewell-auf-wiedersehen-yahoo-directory. Acesso em: 08.06.2016.

novos diretórios foram criados, quais sejam os diretórios de ferramentas de busca. Assim, o usuário adequa ao seu interesse à ferramenta de busca que atenda às suas expectativas para encontrar informações, de forma fácil e rápida, ao invés de ficar refém apenas daquela ferramenta que detém o maior poder econômico e pode dirigir as informações intencionalmente.

3.2.2. Motores de Busca

O funcionamento dos motores de busca ocorre mediante o uso de metadados, descritores, *metatags*,[198] que são referências dos sites utilizadas para localizar para o usuário a URL (*Universal Resource Locator*) onde se encontra o documento (conteúdo) ou site que ele deseja localizar. Essas referências são coletadas por meio de programas buscadores de páginas denominados de *crawlers* ou *spiders* que, em verdade, são robôs automatizados que vasculham toda a web e fazem uma seleção dos sites, arquivos como PDF, imagens e vídeos do Youtube, por exemplo. Os mecanismos de busca mais utilizados ultimamente são o Google, o Yahoo e o Bing.

Por outro lado, interessante notar que atualmente existem motores de busca também temáticos e bem específicos como o PIPL[199], cujo objetivo é encontrar informações pessoais e profissionais na rede de determinada pessoa, basta colocar o nome, e-mail, apelido ou telefone que todas as ocorrências serão fornecidas, inclusive, os perfis nas redes sociais, histórias, notícias e localizações geográficas, idade e sexo. Tal ferramenta ainda sinaliza o orgulho de facilitar o fornecimento dos dados para empresas como Sansung, Thomson Reuters, Aviva, entre outras. [200]

---

[198] Sobre o uso de *metatags*: "As *metatags* são uma ótima maneira para os webmasters fornecerem informações sobre seus sites a mecanismos da pesquisa. *Metatags* podem ser usadas para fornecer informações a todos os tipos de clientes. Cada sistema processa somente as metatags que entende e ignora o resto. Metatags são adicionadas à seção `<head>` de sua página HTML (...)". Para maiores esclarecimentos, o webmaster é o profissional que sabe operar as tarefas entre o computador e a internet, geralmente, é aquele responsável pelo site. *Metatags que o Google entende*. Disponível em: https://support.google.com/webmasters/answer/79812?hl=pt-BR. Acesso em: 09.06.2016.

[199] O slogan do motor de busca é: *"Pipl makes it easy to get contact, social and professional information about people. Learn about using Pipl for your business or application or to enhance your customer list"*. Disponível em: https://pipl.com/. Acesso em: 09.06.2016.

[200] A utilização de motores de busca de pessoas revela sensível questão para sua identidade e proteção de dados pessoais, o que merece uma reflexão maior sobre o consentimento do particular na divulgação dos dados pessoais que expõe atributos da personalidade perante terceiros que exploram economicamente as informações e facilitam o seu acesso para qualquer pessoa no mundo.

O funcionamento dos motores de busca que será explicado com maiores detalhes e em etapas a seguir não se confunde com o diretório de pesquisa que também é uma ferramenta de busca.

Em verdade, os motores de busca executam quatro funções básicas, quais sejam o rastreamento do conteúdo dos sites, a indexação desses dados, o armazenamento no banco de dados e a busca.

3.2.2.1. Rastreamento

O rastreamento ocorre por intermédio de robôs que vasculham a rede da Web a fim de localizar os sites eletrônicos, documentos, enfim, aquilo que o usuário solicitou e quer encontrar.

Os robôs são conhecidos por *Crawlers* (rastejadores) ou *Spiders* (aranhas) que são programas ou *softwares* lançados pelo computador do motor de busca na tentativa de obter resultados requeridos. Os robôs podem se locomover por meio de links existentes nas páginas da web ou qualquer outra estratégia que esteja programado.

A localização dos arquivos e sites ocorre por palavras extraídas de títulos, cabeçalhos, resumo ou campos especiais dispostos como *metatags* situadas nas páginas HTML. Assim, quanto melhor determinado os descritores ou *metatags* pelos websites, o rastreamento dos robôs será mais acessível e eficaz.

Os documentos localizados pelos robôs são encaminhados aos indexadores.

3.2.2.2. Indexação

Por sua vez, a indexação sobrevém quando se extrai a informação das páginas da Web e as armazena em seguida no banco de dados dos motores de busca.

Pela indexação, toda a informação proveniente dos robôs é extraída, copiada e organizada, cuja seleção advém pelos algoritmos. Os engenheiros da computação instituem

os algoritmos de acordo com critérios propostos de forma prévia e observando as políticas e diretrizes da empresa detentora do motor de busca.

Os usuários também podem colaborar com a indexação dos endereços de websites ao sugerir a inclusão de alguns deles no índice de busca. Em razão dos critérios de seleção dos conteúdos da Web que serão exibidos, como o próprio nome denota "sugestão", o pedido não significa que a indexação ocorrerá, mas é uma possibilidade.

Em contrapartida, por exemplo, alguns provedores de informação podem não apresentar o interesse de que as suas páginas, arquivos, documentos e endereço eletrônico estejam disponíveis para a captação pelos robôs e, sucessiva, indexação. Nesse caso, há um *metatag* que pode ser representado pela seguinte fórmula "*<Meta name = "Robots" contente = "noindex">*", ou seja, "*noindex*" que ao ser adicionado no marcador do cabeçalho do endereço impede o rastreamento e indexação.

3.2.2.3. Armazenamento

As informações coletadas são armazenadas no banco de dados para uso em pesquisas futuras. Dessa maneira, a base de dados comporta URLs, endereços eletrônicos das páginas HTML, títulos, resumos, o tamanho e as palavras contidas nos documentos coletados.

Tal armazenamento pode se diferenciar de um motor de busca em relação a outro como é o caso do Google que possui o sistema de memória "cache"[201] que se trata de um repositório de páginas da web temporário. Como podemos notar:

[201] Em termos técnicos, os principais motores de busca se valem do mecanismo de cache para o grande volume de acessos: "Como os mecanismos de busca precisam ser rápidos, sempre que possível, a maioria das tarefas deve ser conduzida na memória principal. Como conseqüência, o cache é altamente recomendado e usado extensivamente. O armazenamento em cache é uma técnica útil para sistemas da Web que são acessados por um grande número de usuários. Ele permite um tempo de resposta curto, reduz significativamente a carga de trabalho nos servidores *back-end* e diminui a quantidade total de largura de banda utilizada." (tradução livre). Segue trecho original: "*As search engines need to be fast, whenever possible, most tasks should be conducted in main memory. As a consequence, caching is highly recommended and extensively used. Caching is a useful technique for Web systems that are accessed by a large number of users. It enables a shorter average response time, significantly reduces workload on back-end servers, and decreases the overall amount of bandwidth utilized*." YATES, Ricardi Baeza. NETO, Berthier Ribeito. *Modern Information Retrieval: the concepts and technology behind search*. 2 ed. New York: Addison-Wesley Publishing Company, 2011, p. 465.

> O que é o *Cache* do Google? Para poder calcular e exibir em décimos de segundo os resultados de busca, o Google utiliza-se de uma cópia das páginas de *sites* na internet rastreadas por seu robô Googlebot, armazenadas em seus servidores. Essas páginas são chamadas de *cache* Google e juntas compõem o índice do Google. Assim, os resultados que vemos na tela de resultados dos *sites* de busca foram calculados com base nessa cópia das páginas. A cada nova passagem do Googlebot pela página, o Google verifica se houve alguma alteração em seu conteúdo. Em caso positivo, são recalculados os diversos fatores que influenciam o posicionamento da página nas buscas (densidade de palavras-chave, negritos, nome de imagens, dentre muitos outros) e essas alterações serão eventualmente refletidas num melhor ou pior posicionamento nos resultados de busca. [202]

Justamente pela passagem do *Googlebot* (*crawler*) mais de uma vez nas páginas da web que o banco de dados ou repositório da Google é temporário.

3.2.2.4. Busca

O usuário quando digita ou discursa a palavra-chave do que almeja localizar na Web pelo mecanismo do motor de busca, em segundos visualiza um índice, ou melhor, uma lista com informações organizadas. Isso porque, a consulta formulada pelo usuário é recebida e transmitida para o software de busca que localiza, entre milhões de itens copiados na base de dados, aqueles que devem ou deveriam constituir a resposta pretendida.

O índice do motor de busca revela a extração de arquivos e websites da Web feita pelos *softwares* robôs que prezam pela relevância das informações que são determinadas pelos algoritmos, cálculos baseados em fórmulas complexas.

O usuário do mecanismo de busca satisfeito é aquele que encontra respostas que tenham relação com a palavra-chave que foi pesquisada ainda que ela seja equívoca e possa apresentar diferentes sentidos.

Como o índice criado ou a lista revela cópias das páginas da web que foram feitas em momento anterior à pesquisa, pode ser que quando o usuário acessa (“dá um click”) no link, aquele não esteja mais disponível seja pela mudança de endereço ou a sua remoção.

[202] *Sobre o sistema cache da Google*. Disponível em: http://www.seomarketing.com.br/cache-Google.php. Acesso em: 15.06.2016.

Esse episódio é descrito por técnicos como "*LinkRot*", ou seja, a perda de links em documentos da internet. [203]

Consequentemente, o contrário também ocorre, isto é, a desindexação de um resultado da lista de busca não denota necessariamente que o conteúdo do site também será removido ou bloqueado.

A compreensão da desindexação dos resultados de busca se mostra relevante para a construção do direito ao esquecimento na sociedade informacional uma vez que reconhecem alguns doutrinadores que apenas este é o solo fértil de tal direito e outros já entendem que a terminologia não é adequada, pois se trataria mais de um direito à desindexação ou *right to not be find*, questões que serão objeto de estudo no decorrer desta dissertação.

Voltando ao sistema de busca da Google, o ranking[204] seria a principal ferramenta do motor de busca, pois a partir dela que se dá a qualidade e relevância da busca. Nesse sentido, especificamente o PageRank simula a navegação do usuário na Web, calculando a probabilidade do acessos aos sites e aos seus links.[205] Além disso, para obter um resultado de qualidade, geralmente os motores de busca se valem tanto do que, diga-se de passagem "o homem médio" julgaria como relevante, bem como dos "clicks" dos próprios usuários que indicam quais resultados são importantes para uma determinada consulta.[206]

Para o *Google Inc* o aumento de acesso ao seu motor de busca significa o aumento do número de anúncios e, por conseguinte, o aumento na sua receita anual.

---

[203]História sobre os sites de busca. *Como funciona os sites de busca*. Disponível em: https://sites.google.com/site/historiasobreossitesdebusca/como-funciona-os-sites-de-busca. Acesso em: 15.06.2016

[204] Sobre o ranking: "*Ranking is the hardest and most important function search engines have to execute. A first challenge is to devise an adequate evaluation process that allows judging the efficacy of a ranking, in terms of its relevance to the users. Without such evaluation process it is close to impossible to fine tune the ranking function, which basically prevents achieving high quality results*." YATES, Ricardi Baeza. NETO, Berthier Ribeito. *Modern Information Retrieval: the concepts and technology behind search*. 2 ed. New York: Addison-Wesley Publishing Company, 2011, p. 471.

[205] Nesse sentido, tecnicamente: "*The best known link-based weight is PageRank, which is part of the ranking algorithm originally used by Google [263]. PageRank simulates a user navigating randomly on the Web, as follows. Consider that our user is currently at page a. Following, she moves to one of the pages pointed by page a by randomly selecting one of the hyperlinks present in a. Next, she repeats the process for the page she moved to, and so on. After a large number of such moves, we can compute the probability with which our user visited each page. This probability is a property of the graph, which was referred to as PageRank in the context of the Web.*(..)"Idem, ibidem, p. 474.

[206] É o que se infere do trecho original: "*To be able to evaluate quality, Web search engines typically use human judgements that indicate which results are relevant for a given query, or some approximation of a "ground truth" inferred from user's clicks, or finally a combination of both, as follows*." Idem, ibidem, , p. 474.

Diante do grande número de websites, páginas da web e usuários, o tráfego de dados na Web é intenso uma vez que atrai constantemente grandes corporações interessadas em obter lucro tanto com a venda de produtos e serviços, seja de maneira direta ou indireta, quanto com a captação de dados pessoais que foi objeto de análise nos Capítulos 1 e 2.

CAPÍTULO IV – O DIREITO AO ESQUECIMENTO

4.1. Esquecimento: sentido

A noção que portamos de esquecimento ou de ser esquecido não é de todo recente já que pode ser identificada em outras épocas e sociedades. Todavia, com o advento da sociedade informacional e o grande fluxo de informações, passou-se a notar a necessidade de se tutelar um novo direito que assumiu as suas atuais feições muito recentemente, sendo uma construção que se inicia no final do século XIX e absorve nova roupagem nos dias atuais.

Trata-se do famoso direito ao esquecimento que almeja o seu explicito reconhecimento na sociedade informacional. Destarte, no direito estrangeiro, diversas expressões surgiram para representá-lo como na língua inglesa *right to be forgotten* (direito de ser esquecido), *right to forget* (direito de esquecer), aos que consideram como parte da tutela da privacidade o chamam de *right to be let alone* (direito de ser deixado em paz), há outros que o encontram como um desdobramento da proteção dos dados pessoais e o chamam de *right to erasure* (direito ao apagamento), *right to delete* (direito de apagar).

A expressão que melhor define é *right to oblivion* (direito ao esquecimento) que remete a palavra *oblivion* que provém do grego *Lethe*, "que designa uma deusa, filha da discórdia, que fluía como um rio no submundo infernal" [207]. O mito descrevia que a pessoa conduzida ao inferno depois de sua morte era obrigada a beber a água desse rio Lethe, para que as memórias da sua vida pregressa fossem apagadas[208], ou melhor, destruídas.

O sentido que se busca empregar ao que se convencionou chamar de "direito ao esquecimento" seria basicamente uma oportunidade para que fatos pretéritos desagradáveis ou constrangedores não fiquem assombrando as pessoas a cada momento de suas vidas.

---

[207] PARENTONI, Leonardo. O direito ao esquecimento (*right to oblivion*). In: DE LUCCA, Newton. (coord.). *Direito e Internet III*: Marco Civil da Internet (Lei n. 12.965/2014). Tomo I. São Paulo: Quartier Latin, 2015, p 546.

[208] É o que se extrai do trecho: "*According to ancient Greek mythology, Lethe (...), better Known as Oblivion, was a river deity, the daughter of Ungratefulness, who flowed in the underworld Hades. People believed that when the dead reached Hades they were forced to drink Lethe's water to erase any memory of their previous life*". XANTHOULIS, Napoleon. Conceptualising a Right to Oblvion in the Digital World: a human rights-based approach. *University College London Research Papers*. p. 01-38, maio/2012. Para aprofundamento da história: WEINRICH, Harald. *Lete:* arte e crítica do esquecimento. Tradução de Lya Luft. Rio de Janeiro: Civilização Brasileira, 2001, p. 24-25.

Isso porque, a relação estabelecida entre a memória e o esquecimento preserva uma importante função que é a de moldar o futuro das pessoas. [209]

Além disso, informações pessoais que são divulgadas e republicadas fora do contexto impedem o desenvolvimento da pessoa de maneira digna, obstaculizando o exercício livre de sua identidade pessoal. Ora, de fato "(...) não se pode deixar de considerar que a vida é um permanente recomeçar que precisa, portanto, que muitos dos seus capítulos, efetivamente se encerrem para que outros se iniciem". [210]

A perpetuidade de informações e lembranças pode vir a causar um estigma social, uma marca que acompanhará a pessoa para uma vida inteira, o que poderá gerar prejuízos e até a perda de uma chance. Em suma, a permanência da circulação de informações pessoais verídicas, porém descontextualizadas, poderá arruinar as possibilidades de um recomeço.

4.2. Embate entre a conservação da memória coletiva e o esquecimento pessoal

Há certa dualidade na memória humana: Esquecer ou lembrar? Existe algum valor no esquecimento?

De acordo com Pablo Dominguez, existe um certo valor e funcionalidade no ato de esquecer que seria tão necessário quanto o de lembrar. Nesse sentido, demonstra que:

> Esquecer é tão importante quanto lembrar, pois possibilita que o ser humano selecione as informações ininterruptamente recebidas pelo cérebro, preservando somente aquelas memórias que o indivíduo considerar como úteis, necessárias ou significativas. Não existe contradição entre lembrar e esquecer, pois os dois atos fazem parte do mesmo processo e, em realidade, são fenômenos complementares, pois é no processo de formulação de novas memórias em que se observa o constante e necessário esquecimento de outras.[211]

Pode-se afirmar que a memória individual seria seletiva, pois escolhe o que é útil lembrar e o que não é. No entanto, a convivência, a troca de informações e experiências

[209] Paul Riccoeur enfatiza que "para abraçar o futuro, é preciso esquecer o passado num gesto de inauguração, de início, de recomeço, como nos ritos de iniciação". RICOEUR, Paul. A memória, a história, o esquecimento. Tradução de Alan François et. Al. Campinas: Editora UNICAMP, 2007, p. 510.

[210] CONSALTER, Zilda Mara. *Para além do rio lete: o direito ao esquecimento como aporte teórico para a proteção efetiva da intimidade na era virtual.* Tese de doutorado apresentada no Programa de Pós Graduação da Faculdade de Direito da Universidade de São Paulo. Orientador Dr. Álvaro Villaça Azevedo. São Paulo, 2016, p. 189.

[211] MARTINEZ, Pablo Dominguez. *Direito ao esquecimento: a proteção da memória individual na sociedade da informação*. Rio de Janeiro: Editora Lumen Juris, 2014, p. 62.

pessoais em um grupo pode vir a criar o que Maurice Halbwach ousou denominar de memória coletiva.[212]

A resistência em se admitir um direito ao esquecimento encontra-se na confusão com a possibilidade de "apagar" eventos históricos até aqueles violentos e contra os direitos humanos. Também há o receio de que o exercício deste direito acarrete na manipulação da informação, a qual foi traço distintivo dos regimes totalitários.[213]

Com base nessas premissas, o advogado Pablo Martinez desenvolve a ideia de que existe um aspecto público e privado do direito ao esquecimento. O aspecto público pretende a valorização de eventos históricos com a punição de atividades ilícitas, o que abrange a memória social. Já o aspecto privado, fundamentado "na dignidade da pessoa humana, busca proteger o indivíduo em face da divulgação de informações privadas que, fora de contexto, sem utilidade pública, sem contemporaneidade, mesmo verídicas, ferem ou podem ferir um indivíduo".[214]

O direito ao esquecimento não seria propriamente o direito que um sujeito detém de obrigar que terceiros esqueçam os fatos de sua vida pretérita tampouco a possibilidade de mudar o passado ou realizar um ato de censura. Pelo contrário, a adoção pelo termo de "esquecimento" se justifica na medida em que proporciona a não rememoração daquele fato que o indivíduo deseja manter para si. Além de proporcionar um esquecimento coletivo que representaria a oportunidade de enfraquecer essa lembrança no grupo do qual aquele indivíduo faz parte.

4.3. Conceito, função e natureza jurídica do direito a ser esquecido: complexidade

A facilidade proporcionada pelas novas tecnologias acarreta em um cenário de perenidade e conservação constante das informações, onde se modificou a regra e a

[212] HALBWACHS, Maurice. *La memoria colectiva*. Tradução de Inés Sancho-Arroyo. Zaragoza: Prensas Universitarias de Zaragoza, 2004.
[213] MARTINEZ, Pablo Dominguez. *Direito ao esquecimento: a proteção da memória individual na sociedade da informação*. Rio de Janeiro: Editora Lumen Juris, 2014, p. 69-70.
[214] MARTINEZ, Pablo Dominguez. *Direito ao esquecimento: a proteção da memória individual na sociedade da informação*. Rio de Janeiro: Editora Lumen Juris, 2014, p. 71.

exceção. O esquecimento que sempre foi a regra, porém nos contornos atuais tornou-se a exceção.[215]

A expressão "direito ao esquecimento" tem sido utilizada pelo menos em três acepções[216]: i) uma tradicional; ii) a segunda no âmbito da internet; iii) a terceira criada com base no modelo de proteção dos dados pessoais europeu.

O direito ao esquecimento como foi tradicionalmente conhecido é aquele direito do sujeito em não ver a republicação de alguma notícia sobre um evento, que já tinha sido legitimamente publicada, em razão do demasiado transcurso de tempo.[217]

Essa concepção tradicional surgiu em época que antecede a utilização dos mecanismos da Internet como meio de comunicação e transmissão de dados em massa. Cita-se a sua gênese no Caso *Lebach*[218], julgado pelo Tribunal Constitucional Alemão em 1973 em razão de ter se tornado um julgamento paradigmático pelo embate dos direitos da personalidade e a liberdade de imprensa e de informação. [219]

Nessa senda, no ano de 1969, um homem, na condição de partícipe, cometeu um crime de latrocínio que chamou a atenção do público, com a ampla cobertura pela imprensa e televisões locais que ficou conhecido como o "Assassinato de soldados de Lebach". No fatídico episódio, o roubo de armas e munições das forças armadas alemãs levou ao homicídio de quatro soldados e um quinto foi ferido. Em agosto de 1970, os dois principais réus foram condenados à prisão perpétua. Já o partícipe foi condenado a seis anos de reclusão, porque ajudou na preparação criminosa.

A ZDF (*Zweites Deutsches Fernsehen* – Segundo Canal Alemão) produziu um documentário em detalhes sobre todo o ocorrido e os envolvidos no crime cometido na província de *Lebach.* No documentário, o homem que participou do roubo era apresentado com nome e seu retrato, todavia atores foram contratados para expor de modo

---

[215] MAYER-*SCHÖNBERGER*, Viktor. *Delete: the virtue of forgetting in the digital age.* Princeton: Princeton University Press, 2009, p 52 e 95.

[216] Essas três acepções foram apontadas pela autora Giusella Finocchiaro, professora da Universidade de Bolonha na Itália. FINOCCHIARO, Giusella. Il diritto all'oblio nel quaro dei diritti dela personalità. In: *Il Diritto Dell'informazione e dell'informatica*. Rivista Promossa Dalla Fondazione Centro di Iniziativa Giuridica Piero Calamandrei. 2014, p. 591 – 604.

[217] É a concepção da professora Giusella: "*Com il diritto all'oblio si è fato tradizionalmente riferimento al diritto di un soggetto a non vedere pubblicate alcune notizie relative a vicende, già legitimamente pubblicate, rispetto all'accadimento dele quali è trascorso um notevole lasso di tempo.*" Ibid. p. 592.

[218] Esse era o nome de um lugarejo localizado a oeste da República Federal da Alemanha.

[219] Todas as informações do caso foram retiradas da tradução da decisão da Corte Alemã. MARTINS, Leonardo. *Introdução à jurisprudência do Tribunal Constitucional Alemão*. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Organização e introdução: Leornado Martins. Trad. Beatriz Henning et al. Prefácio: Jan Woischnik. Montevidéu: Fundação Konrad Adenauer, 2005, p. 486-494.

particularizado todo a ação na noite do crime, a perseguição policial e sua prisão, inclusive, expondo o seu envolvimento e ligação homossexual. Pretendia-se transmitir o documentário na sexta-feira, poucas horas anteriores da sua soltura.

Indignado, o homem propôs uma ação com pedido liminar em face da emissora para que ela se abstivesse em exibir o documentário, porque o conteúdo violaria os seus direitos de personalidade. Ocorre que tanto o Tribunal Estadual de Mainz quanto o Superior Tribunal Estadual de Koblenz julgaram a medida liminar improcedente.

Por sua vez, em recurso dirigido ao Tribunal Constitucional Alemão, o apelo do condenado foi atendido. O Tribunal Constitucional Alemão julgou procedente a Reclamação Constitucional "por vislumbrar uma infração perpetrada pelos tribunais do direito de desenvolvimento da personalidade (Art. 2 I GG)". Considerou que, no caso concreto, deveria haver "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)". O Tribunal Constitucional Alemão, portanto, modificou as decisões dos tribunais civis e proibiu o citado canal alemão de transmitir o documentário até a decisão final da ação principal pelos tribunais ordinários competentes. Nesse sentido, o acordão frisou que não há preferência entre direitos fundamentais ao passo que uma ponderação de interesses seria necessária para julgar o caso concreto, valorando-se a posição da pessoa humana:

> O conceito de pessoa humana (Menschenbild) da Grundgesetz e a configuração a ele correspondente da comunidade estatal exigem tanto o reconhecimento da independência da personalidade individual como a garantia de um clima de liberdade que não é imaginável atualmente sem comunicação livre. Ambos 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. Certamente, podem decorrer da liberdade de radiodifusão efeitos limitadores para as pretensões jurídicas derivadas do direito [fundamental] da personalidade; porém, o dano causado à "personalidade" por uma apresentação pública não pode ser desproporcional ao significado da divulgação para a comunicação livre (cf. Adolf Arndt, op. cit.). Além disso, desse valor de referência decorre que a ponderação necessária por um lado deve considerar a intensidade da intervenção no âmbito da personalidade por um programa de tipo questionável e, por outro lado, está o interesse concreto a cuja satisfação o programa serve e é adequado a servir, para avaliar e examinar se e como esse interesse pode ser satisfeito [de preferência] sem um prejuízo – ou sem um prejuízo tão grande – da proteção à personalidade. [220]

[220] *Ibidem*, p. 491/492.

Por essa visão, o direito ao esquecimento relaciona-se com a privacidade do indivíduo e o desenvolvimento de sua personalidade que, especificamente, no caso *Lebach*, considerou-se a ressocialização do condenado em processo criminal.

No Brasil, a configuração da possibilidade de "esquecer" os crimes cometidos no passado apresenta-se como fundamento o princípio constitucional da proibição de pena de caráter perpétuo, o qual o condenado não deve sofrer os efeitos da pena pelo resto de sua vida. [221]

Em razão disso, os delitos não devem constar da folha corrida do condenado, exceto na hipótese de prática de nova infração penal e outros casos previstos em lei[222]. Os crimes cometidos pelo indivíduo deverão ainda serem sigilosos para que a sua reinserção na sociedade se efetive. [223][224]

Atrelar o direito ao esquecimento somente às situações de reabilitação criminal seria demasiadamente restritivo, pois as outras pessoas que não foram condenadas criminalmente e que reclamam a mesma pretensão jurídica seriam prejudicadas. Os condenados teriam uma vantagem sobre os demais, infringindo a igualdade jurídica.

Além da possibilidade da reabilitação social, compreende-se nessa tradicional acepção, de maneira um pouco mais ampla, que o direito ao esquecimento vincular-se-ia a questão subjetiva do ser humano em não ser relembrado de fatos que almeja esquecer por meio da republicação da informação legítima e verídica que se distanciou do debate

[221] Cf. Artigo 5º da CF/88: "Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...)III - ninguém será submetido a tortura nem a tratamento desumano ou degradante; (...)XLVII - não haverá penas: b) de caráter perpétuo;". BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 06.12.2017.

[222] Cf. Artigo 202 da Lei nº 7.210/1984: "Cumprida ou extinta a pena, não constarão da folha corrida, atestados ou certidões fornecidas por autoridade policial ou por auxiliares da Justiça, qualquer notícia ou referência à condenação, salvo para instruir processo pela prática de nova infração penal ou outros casos expressos em lei". BRASIL. Lei nº 7.210/1984. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L7210.htm. Acesso em: 06.12.2017.

[223] Cf. Artigo 93 do Código Penal: "A reabilitação alcança quaisquer penas aplicadas em sentença definitiva, assegurando ao condenado o sigilo dos registros sobre o seu processo e condenação. Parágrafo único - A reabilitação poderá, também, atingir os efeitos da condenação, previstos no art. 92 deste Código, vedada reintegração na situação anterior, nos casos dos incisos I e II do mesmo artigo." BRASIL. Código Penal. Decreto-Lei nº 2.848 de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 06.12.2017.

[224] Cf. Artigo 748: "Art. 748. A condenação ou condenações anteriores não serão mencionadas na folha de antecedentes do reabilitado, nem em certidão extraída dos livros do juízo, salvo quando requisitadas por juiz criminal". BRASIL. Código de Processo Penal. Decreto-Lei nº 3689 de 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689Compilado.htm. Acesso em: 06.12.2017.

público pelo transcurso do tempo. Nesse caso, relaciona-se mais com o direito à privacidade do indivíduo que pretende ser deixado em paz e controlar a divulgação de suas informações relativas à sua esfera privada.

A segunda acepção compreende que o direito ao esquecimento não se trata apenas ou necessariamente de uma republicação da informação, mas da sua própria permanência na rede de internet. De maneira que não se considera o tempo transcorrido entre a publicação da informação e a sua republicação, mas o tempo que decorreu desde a publicação original[225].

Nota-se que o risco do conteúdo da informação pessoal verídica e constrangedora manter-se acessível aos demais tende a ser infinita perante a capacidade de coleta, armazenamento e difusão de dados pessoais na internet.

Além disso, anteriormente, o sujeito que buscasse ser esquecido e também esquecer-se de determinado fato que lhe causasse constrangimento ou desgosto poderia simplesmente mudar-se de cidade, até mesmo de país, para que um recomeço fosse concretizado.

O autor Viktor Mayer-Schönberger, em sua obra "*Delete: the virtue of forgetting in the digital age*" trata de vários exemplos, nos quais a perenização de informações na Internet pode ocasionar consequências alarmantes para os indivíduos. Ele afirma que, antigamente, se a pessoa não tinha o poder de controle de suas informações pessoais e que lhe causavam transtornos, ela poderia simplesmente partir. Ora, "durante séculos, o deslocamento de uma comunidade para outra permitiu que as pessoas reiniciassem suas vidas sem máculas, à medida que as informações sobre elas permaneciam locais", porque atravessar o Atlântico da Europa para os Estados Unidos, nos séculos 18 e 19, concedia a oportunidade de as pessoas começarem do "zero", não apenas com vistas a conseguir um emprego, ganhar dinheiro, mas notadamente em termos de controlar as informações que os outros obtinham delas. [226] Com a vinda da internet, as informações perseguirão a pessoa por onde ela for.

---

[225]Nesse sentido, explica a professora Giusella que "*In altri termini, non si trata solo o necessariamente di uma ripubblicazione dell'informazione, ma piuttosto di uma permanenza dela stessa nella Rete. (...)Il tempo da considerare non è più quello trascorso tra la pubblicazione dell'informazione e la ripubblicazione, ma quello trascorso dal tempo dela pubblicazione che perdura*" (...) *Non si tratta del diritto a dimenticare, ma del diritto a contestualizzare.*". *ibidem.*, p. 593.

[226] Lê-se o original: "*If all else fail to control information, people have had another, albeit much more costly option: exit. For centuries, moving from one community to another permitted people to restart their lives with a clean slate, as information about them stayed local. Crossing the Atlantic from Europe to newly founded United States, or into the great Western frontier of eighteenth and nineteenth centuries let people start drom scratch, not just in economic terms, but more importantly in terms of knowledge others had of*

Em contrapartida, é notável a diferença dessa segunda concepção para a primeira, justamente pelo potencial de difusão da informação. A republicação da informação em televisões, rádios e jornais costumeiramente acontece de forma momentânea e pontual enquanto na internet não é necessário que um ato de "republicação" seja realizado para que a informação ali permaneça.

É o nítido exemplo das empresas jornalísticas que digitalizam todo o seu acervo e o disponibilizam na internet. Embora, naquela época, o interesse público que impulsionou a divulgação da notícia pessoal teria sido legitimamente preenchido, o ato de inseri-la no site poderá levar a uma confusão entre o que a pessoa foi e o que ela é.

A permanência da informação na internet certamente levará, em algum momento, a sua descontextualização entre o momento de sua produção e a realidade atual. Isso porque, a pessoa tem o direito de mudar a si mesma.

A terceira acepção de direito ao esquecimento é aquela que se refere ao direito à proteção dos dados pessoais. Traduz-se na faculdade jurídica de apagar, cancelar e se opor ao tratamento de dados pessoais[227] nos termos do modelo de proteção europeu, especificamente, na Diretiva nº 95/46/CE e também no novo Regulamento Geral de Proteção de Dados Pessoais, do Parlamento e Conselho Europeu, que apresenta os mesmos direitos.

O que inspirou essa terceira acepção foi justamente o julgamento do Caso *Mario Costeja* em face do motor de busca *Google* em que se determinou, em maio de 2014, que os resultados de pesquisa fossem desindexados da lista de busca para minimizar a propagação do conteúdo da informação sem, contudo, removê-la de sua fonte original, o que será objeto de enfrentamento no próximo Capítulo.

Ora, a terceira acepção não se trata de um direito ao esquecimento, mas do exercício do direito à proteção dos dados pessoais, evidenciado pelo cancelamento ou apagamento dos dados que foram considerados irrelevantes, inadequados e excessivos, conforme o princípio da qualidade dos dados e o princípio da finalidade.

---

them". MAYER-SCHÖNBERGER, Viktor. *Delete: the virtue of forgetting in the digital age.* Princeton: Princeton University Press, 2009, p. 103.

[227] Por último, a terceira acepção seria o que ficou decidido no caso Costeja e os motores de busca que será objeto de análise no próximo capítulo. Nessa esteira, a professora Giusella esclarece: "*uma terza accezione del diritto all'oblio è quella che si riferisce al diritto ala cancelazione, al bloco, al congelamento dei dati 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 'relativa ala tutela dele persone fisiche com riguardo al tratamento dei dati personali, nonché ala libera circolazione di tali dati*'". Ibidem. p. 594.

A complexidade que o fenômeno do direito ao esquecimento apresenta impulsiona a construção de diversas conceituações e agrupamento de situações que não revelam pertinência lógica entre si para estarem atracadas sob o "mesmo barco".

Prontamente, a partir da descrição das três acepções, diversas propostas conceituais para o direito ao esquecimento são localizadas entre os doutrinadores que estudam o tema.

Há quem diga que o direito ao esquecimento define-se pelo direito de que "ninguém pode ser eternamente lembrado ou cobrado por atos praticados no passado"[228].

No mesmo sentido, o artigo "*Oblivion the Right to Be Different*", em que Norberto Nuno Gomes de Andrade cita a conceituação de Giogio Pino como sendo "*The right to silence on past events in life that are no longer occuring*"[229], o que traduz uma conceituação bastante abrangente para o tema, pois ignora a possível interferência de outros interesses em jogo.

Há quem entenda que o direito ao esquecimento visa tutelar a vida privada, especialmente, a intimidade da pessoa humana como a definição proposta pela autora Zilda Consalter:

> [...] pode-se delinear o direito ao esquecimento como um direito subjetivo, de titularidade individual e não absoluto, resultante do desdobramento do direito fundamental à intimidade, mediante o qual o interessado, no exercício de sua liberdade, autonomia e determinação individual, controla se fatos pertencentes ao seu passado podem ou não ser retomados no presente, como forma de salvaguardar a sua integridade emocional, psíquica, profissional e social, além de resguardar, eficazmente, a sua vida intima.[230]

O conceito de direito ao esquecimento proposto pela autora Zilda não tende a satisfazer ao que se compreende do fenômeno do esquecimento. Em verdade, confunde-se a autora ao se referir à intimidade como privacidade informativa, isto é, a possibilidade de controle de suas informações privadas, além do mais, em linhas gerais, a violação da intimidade pressupõe a ocorrência de um ato ilícito que fere diretamente tal bem jurídico.

---

[228] DA SILVA, Roberto da Silva Baptista Dias. PASSOS, Ana Beatriz Guimarães. Entre lembrança e olvido: uma análise das decisões do STJ sobre o direito ao esquecimento. *Revista Jurídica da Presidência*. Vol. 16, nº 109, jun./set.. Brasília: 2014, p. 397.

[229] PINO, Giogio apud ANDRADE, Noberto Nuno Gomes de. *Oblivion: The Right to Be Different ... from Oneself Reproposing the Right to Be Forgotten*. Revista de Internet, Direito e Política. Universitat Oberta de Catalunya. February/2012.

[230] CONSALTER, Zilda Mara. *Para além do rio lete: o direito ao esquecimento como aporte teórico para a proteção efetiva da intimidade na era virtual.* Tese de doutorado apresentada no Programa de Pós Graduação da Faculdade de Direito da Universidade de São Paulo. Orientador Dr. Álvaro Villaça Azevedo. São Paulo, 2016, p. 204.

O direito que se pretende delimitar sobre esquecer fatos passados, de não reacender tais fatos levando ao público e de perenizar informações que dificultam o esquecimento poderá não infringir o íntimo da pessoa, a esfera mais interior da vida privada. Bastaria que, por exemplo, uma mulher que no passado trabalhou como prostituta e, após um decurso de tempo, constituiu família e largou a profissão, deseja não rememorar tal fato pretérito e que seus vizinhos não fiquem sabendo do seu passado, pois lhe causa certo constrangimento. Todavia, isso não quer dizer que essa mulher esforça-se em esconder esse fato e que a possível divulgação deste violaria a sua intimidade. É o típico caso de direito ao esquecimento que mescla a parcela do conceito de privacidade nos contornos atuais com o controle da sua vida privada com o direito à identidade de ser quem se é hoje e transparecer isso, tais argumentos que serão revisitados no tópico da sua autonomia.

Com base na relação consumerista, Laura Shertel Mendes, ao comentar o art. 43 daquele Código, tratou o direito ao esquecimento como "um limite temporal para o armazenamento de dados pessoais"[231], o que se relaciona mais com o direito à proteção de dados pessoais e seus princípios tais como a finalidade e adequação.

De igual modo, Mario Hernández Ramos assevera que o direito ao esquecimento constitui "parte essencial do direito à proteção de dados pessoais", enfatizando para o direito de controle e disposição. [232]

Já para Pere Simon Castellano, nessa mesma perspectiva, o direito ao esquecimento se concretizaria na pretensão legitima de se opor, excluir ou cancelar os dados pessoais que circulam na rede ou que sejam difundidos sem consentimento prévio ou quando este tiver sido revogado, ou quando os dados deixaram de ser úteis para a finalidade com que foram coletados e publicados na *Web.*[233]

Vislumbra-se que o direito ao esquecimento ainda que sob a feição da internet não se reduz ao direito à proteção de dados pessoais. Os dados estão em constante circulação, processamento, utilização e armazenamento, o que justifica a sua tutela ser dinâmica.

---

[231] MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo***.** Faculdade de Direito. Universidade de Brasília, Brasília: 2008, p. 131.

[232] RAMOS, Mário Hernandez. El derecho al olvido em la web 2.0. 2013, p. 131-136.

[233] Segue trecho original: "*El derecho al olvido digital se erige como respuesta a un nuevo reto social -la perennidad de la información- que plantea Internet. Tal derecho se concreta en la pretensión legítima de oponerse, borrar o cancelar aquellos datos personales que circulan en la red, ya sean difundidos sin consentimiento previo o con el mismo revocado, o cuando los datos han dejado de ser útiles para la finalidad con la que se recabaron y hicieron públicos en la web."* CASTELLANO, Pere Simon. El régimen constitucional del derecho al olvido en Internet. Neutralidad de la red y otros retos para el futuro de Internet. Actas del VII Congreso Internacional Internet, Derecho y Política Universitat Oberta de Catalunya Barcelona: Huygens Editoral, 11-12 de julho de 2011, p. 405. Disponível em: file:///C:/Users/user/Downloads/El regimen constitucional del derecho al%20(1).pdf. Acessado em: 06.06.2016.

Atrelar o direito ao esquecimento com os direitos e garantias próprios da proteção dos dados pessoais certamente acarretará em uma discriminação entre "dados pretéritos"[234] e "dados atuais", mas a proteção ocorre para toda e qualquer espécie de dados, sendo mais dura para os dados sensíveis, bastando que o dado seja qualificado com a adjetivação de "pessoal" para que se enquadre nos modelos de legislação de proteção de dados pessoais.

Considerando o direito ao esquecimento na seara digital está o conceito proposto pela professora Cíntia Rosa Pereira de Lima que com base na legislação europeia de proteção de dados pessoais assim o define como:

> um direito autônomo de personalidade através do qual o indivíduo pode excluir ou deletar as informações a seu respeito quando tenha passado um período de tempo desde a sua coleta e utilização e desde que não tenham mais utilidade ou não interfiram no direito de liberdade de expressão, científica, artística, literária e jornalística [235].

Com a devida vênia, o direito à proteção dos dados pessoais assegura o exercício de excluir ou deletar as informações pessoais, sendo a remoção de conteúdo *online* apenas uma das formas que asseguram e efetivam a tutela do direito ao esquecimento.

No mesmo sentido, Leonardo Parentoni inclui o direito ao esquecimento ao tratamento informatizado de dados pessoais:

> É a faculdade de obstar o processamento informatizado, a transferência ou publicação de dados pessoais, além de exigir que sejam apagados, sempre que a sua preservação esteja causando constrangimento ao sujeito envolvido, desde que não exista razão de interesse público que justifique a preservação.[236]

Observa-se por esse conceito que além de compreender o direito ao esquecimento como objeto tutelado os dados pessoais, ainda restringe-o para a seara da "informatização", porém, averiguou-se que, em ampla maioria, o sistema protetivo dos dados pessoais garante a tutela para dados automatizados ou não. Nesse sentido, tal definição restringe a

[234] Referir-se ao dado em si como pretérito poderá resultar certa confusão com o tempo ou momento em que ele foi disponibilizado na rede e o transcurso do tempo de produção da informação que se pretende esquecer. Em outras palavras, tratar de um "dado pretérito" não seria o melhor termo a se empregar.
[235] LIMA. Cíntia Rosa Pereira de. Op. cit., p. 93.
[236] PARENTONI, Leonardo. O direito ao esquecimento (*right to oblivion*). In: DE LUCCA, Newton. (coord.). *Direito e Internet III*: Marco Civil da Internet (Lei n. 12.965/2014). Tomo I. São Paulo: Quartier Latin, 2015, p. 577

uma faceta do direito à proteção dos dados pessoais que é autônomo em relação ao direito ao esquecimento.

Próximo do sentido empregado pela primeira e pela segunda acepções assinaladas, isto é, do direito ao esquecimento dentro ou fora do âmbito da internet, encontra-se René Ariel Dotti que compreende o direito ao esquecimento no sentido de uma:

> [...] faculdade de a pessoa não ser molestada por atos ou fatos do passado que não tenham legítimo interesse público. Trata-se do reconhecimento jurídico à proteção da vida pretérita, proibindo-se a revelação do nome, da imagem e de outros dados referentes à personalidade. [237]

Bem a verdade que o nome, a imagem e outros dados referentes à personalidade são representativos do direito à identidade pessoal, porém com este não se confunde, o que será esclarecido no próximo item.

Por outro lado, o professor Anderson Schreiber estipula uma nova abordagem ao direito ao esquecimento e não o define como um direito de "reescrever a história", de alterar os fatos ou suprimir conteúdos porventura veiculados na Internet, mas sim como um direito de "não ser perseguido por certos fatos", evitando-se uma identificação inadequada da pessoa humana que violaria, em último caso, seu direito à identidade pessoal. [238] É o que ele definiu como:

> (...) o direito ao esquecimento não atribui a ninguém o direito de apagar fatos ou reescrever a História (ainda que se trate tão somente da sua própria história). O que o direito ao esquecimento assegura é a possibilidade de se discutir o uso que é dado aos fatos pretéritos, mais especificamente o modo e a finalidade com que são lembrados.[239]

Com fundamento na identidade pessoal, Anderson ainda explica que o direito ao esquecimento seria melhor abordado pela "desidentificação" da vítima do conteúdo veiculado pelo terceiro, pela indexação adequada desse conteúdo em relação ao nome da vítima nos motores de busca e a contextualização do conteúdo veiculado pelo terceiro.[240]

---

[237] DOTTI, René Ariel. O direito ao esquecimento e a proteção do habeas data. In: WAMBIER, Teresa Arruda Alvim (Coord.). *Habeas Data*. São Paulo: Revista dos Tribunais, 1998, p. 300.
[238] SCHREIBER, Anderson. Marco Civil da Internet: Avanço ou Retrocesso? A responsabilidade Civil por Dano Derivado do Conteúdo Gerado por Terceiro. In: DE LUCCA, Newton. (coord.). *Direito e Internet III: Marco Civil da Internet (Lei n. 12.965/2014).* Tomo II. São Paulo: Quartier Latin, 2015, p. 299 – 301..
[239] SCHREIBER, Anderson. *Direitos da Personalidade.* 3 ed. São Paulo: Atlas, 2014, p. 174.
[240] SCHREIBER, Anderson. *Op. cit.* , 2015, p. 299 – 301..

Apropriado em partes, o conceito proposto por Anderson no sentido de não ser perseguido por certos fatos está adequada, porém a desindexação, a desidentificação e a contextualização podem ser aliados para o combate do direito ao esquecimento, mas não o tutelam propriamente em si.

Os casos de desindexação, desidentificação e contextualização são fenômenos que não requerem a supressão do conteúdo veiculada na internet e, por tanto, estão sob o cinjo do direito à proteção dos dados pessoais. A desindexação é uma faculdade do usuário de se opor ao tratamento de seus dados pessoais realizado pelos motores de busca, sem que isso afete a informação que se encontra no site (fonte primária). A desidentificação seria a retirada dos desígnios identificativos da pessoa de determinado conteúdo, por exemplo, a retirada do nome e da imagem da pessoa retratada na notícia veiculada, ou aquele amigo da rede social como o *Facebook* que realiza a sua marcação (*tag*) do seu perfil a foto postada. A contextualização não seria a supressão de conteúdo, mas a sua correção e adequação, isto é, elementos são adicionados para o fim de corrigir aquela informação. Os três mecanismos são tutelados pelo direito de oposição, cancelamento, apagamento (ou melhor, nesse caso remoção do link da lista de resultados) referente aos dados pessoais.

Daí se extrai a relação entre a proteção de dados pessoais e o direito ao esquecimento uma vez que as faculdades previstas na Diretiva 95/46/CE, no Regulamento Geral Europeu e, especificamente, no caso brasileiro do Marco Civil da Internet, conforme direitos e garantias de consentimento expresso, exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e a remoção de conteúdo infringente, dedicam-se a auxiliar a tutela do direito ao esquecimento, mas de nada se assemelham com o seu objeto.

O objeto do direito ao esquecimento é o livre desenvolvimento da pessoa humana, posto na cláusula geral da dignidade que se busca manter os fatos pretéritos no passado, permitindo proteger tanto o contemporâneo conceito de privacidade quanto a identidade da pessoal.

Viviane Nóbrega Maldonado entende o direito ao esquecimento como: “a possibilidade de alijar-se do conhecimento de terceiros uma específica informação que,

muito embora seja verdadeira e que, preteritamente, fosse considerada relevante, não mais ostenta interesse público em razão de anacronismo".[241]

Assim, o direito ao esquecimento trata de informações verdadeiras que, apesar da existência de um interesse público no passado, não mais assumem essa condição, causando consequências para a sua esfera privada e para si.

Imperioso delimitar que os fatos inverídicos, presentes ou pretéritos, não se enquadram no conceito e objeto do direito ao esquecimento, cuja remoção se dá justamente pela inverdade da informação.[242]

Não há que se controverter sobre a natureza jurídica do direito ao esquecimento na medida que como diz respeito à pessoa, tal direito nasce com ela, sendo um direito subjetivo, uma espécie dos direitos da personalidade.

O direito ao esquecimento apresenta uma faceta positiva (obrigação de fazer) quanto negativa (abstenção). Positiva, porque permite ao titular exercer a sua pretensão contra terceiros, exigindo que removam o conteúdo infringente deste direito seja nos meios de comunicação tradicionais ou na internet. Negativa, porque impõe que a esses terceiros se abstenham de processar, publicar, republicar e conservar tal informação pessoal.[243]

[241] MALDONADO, Viviane Nóbrega. *O direito ao esquecimento.* Barueri,SP: Novo Século Editora, 2017, p. 97.
[242] MALDONADO, Viviane Nóbrega. *O direito ao esquecimento.* Barueri,SP: Novo Século Editora, 2017, p.96.
[243] PARENTONI, Leonardo. O direito ao esquecimento (*right to oblivion*). In: DE LUCCA, Newton. (coord.). *Direito e Internet III*: Marco Civil da Internet (Lei n. 12.965/2014). Tomo I. São Paulo: Quartier Latin, 2015, p. 581.

4.4. Da autonomia ou não do direito ao esquecimento

O pragmatismo auxilia no campo jurídico para delimitar os valores a serem protegidos e o que se pode considerar como um direito. Quais fatos são relevantes para a ciência do Direito e quais não são. Acontece que aglutinar todos os casos que "transparecem" tratar de pretensões de exclusão de informações pretéritas, desatualizadas e irrelevantes como sendo um direito ao esquecimento não é a melhor saída.

Não se pode tomar casos envolvendo direito de imagem e intimidade sobre os contornos da internet e nomeá-los hoje de direito ao esquecimento. Também a opção de elencar a desindexação de resultados dos motores de busca como direito ao esquecimento não representa a exegese deste direito.

Tais reflexões, demonstram que várias das tentativas já feitas para definir ou delimitar o conteúdo do direito ao esquecimento soam parciais ou falsas proposições do problema. Por isso que se deve ter em mente que o direito ao esquecimento tem um contorno diverso dos outros direitos reconhecidos, bem como da indexação e vinculação de dados pessoais nos motores de busca.

Todavia, pode-se dizer que o tema ainda está sendo extremamente ventilado entre os doutrinadores e magistrados que ainda procuram entender esse direito, o seu verdadeiro fundamento e possível autonomia.

O direito ao esquecimento apresenta características próprias que o difere de qualquer outro direito, quais sejam que: a) a divulgação, republicação e circulação de informações verdadeiras; b) informações sobre fato que tenha ocorrido em tempo remoto; c) que cause certo constrangimento para o titular e d) não contraste com o interesse público.

Como parâmetro para avaliar a procedência ou não do pedido do direito ao esquecimento, há a necessária ponderação de interesses entre a liberdade de expressão, de informação e o desenvolvimento livre da pessoa humana, baseada na cláusula geral da dignidade da pessoa humana.

Com a aplicação do direito ao esquecimento, protege-se, ainda que indiretamente, a proteção de todos aqueles outros direitos da personalidades explícitos (nome, imagem, privacidade, honra) e implícitos (identidade) já que dizem respeito a pessoa humana. Logo, apesar dos objetos jurídicos distintos e diferenciados, "misturam-se e confundem-se em

razão do caráter de essencialidade", pois o ser humano "não pode ser cindido de nenhum modo". [244]

Dessa forma, a despeito de entendimentos contrários, o direito ao esquecimento possui dois fundamentos, quais sejam a privacidade e a identidade pessoal. Em síntese, aborda-se o entendimento de Massimiliano Mezzanotte[245] que configura o direito ao esquecimento como sendo uma "situação jurídica subjetiva com *corpus* de um direito à identidade pessoal; mas *animus* de direito à privacidade". Em outras palavras, um situação jurídica subjetiva que possui uma matéria do direito à identidade pessoal e o espírito de direito à privacidade.

O direito ao esquecimento é um direito de personalidade autônomo porque não se resume exclusivamente na tutela da privacidade nem no direito à identidade pessoal.

Em outras palavras, o indivíduo que alega o direito ao esquecimento pretende resguardar determinado acontecimento que tenha participado e, portanto, que este fato de sua vida privada seja resguardado ou, pelo menos, não perenizado diante das novas tecnologias que aumentaram e baratearam a coleta, o armazenamento e o tratamento dos dados.

Por outro lado, o indivíduo não quer ser estigmatizado por um fato ocorrido no passado, geralmente, por um erro cometido em tempo remoto e passar a ser julgado como se fosse esta mesma pessoa que praticaria tal erro novamente. Assim, exerce seu direito à identidade pessoal, para que sua personalidade seja a real e não a estigmatizada.

O direito ao esquecimento não se confunde com o direito à proteção de dados pessoais que busca tutelar a dinâmica do tratamento de dados pessoais, sendo estes um prolongamento da pessoa humana que a identifica ou pode vir a identifica-la. O exercício das faculdades de correção, cancelamento ou apagamento de informações pessoais não leva em consideração o conteúdo da informação sobre o aspecto de sua esfera privada. Conforme se demonstrou no Capítulo 2, o direito à proteção de dados pessoais, independe, do seu conteúdo infringir ou constranger a esfera privada do titular de dados, o que diferencia do direito ao esquecimento que se volta a tutelar dados pretéritos que causam constrangimento.

Importante destacar que o constrangimento que aqui se apresenta não significa violência física ou moral tampouco que a pessoa deverá se sentir ofendida em sua honra,

[244] MARTINEZ, Pablo Dominguez. *Direito ao esquecimento: a proteção da memória individual na sociedade da informação*. Rio de Janeiro: Editora Lumen Juris, 2014, p. 82-83.
[245] MEZZANOTTE, M. *Il diritto all'oblio:* contributo allo studio della privacy storica. Napoli: Edizioni Scientifiche Italiane, 2009. p. 81.

direito autônomo considerado como a dignidade pessoal (subjetiva) e reputação (objetiva). O ato de constranger se dá no sentido de intimidação, inibição. Ora, a divulgação de certo fato pretérito e verídico que cause certa inibição[246] na pessoa que deseja controlá-los, mantê-los para si e, ao mesmo tempo, resguardar o direito que tem de ser a si mesmo.

Em verdade, como já referido, o direito ao esquecimento se enquadra na definição dos direitos da personalidade que estão previstos na Constituição Federal e no Código Civil de 2002 e que não traduzem um rol taxativo, estanque, apenas são direitos especiais diante da cláusula geral da proteção dos direitos da personalidade.

De acordo com Gustavo Tepedino:

> Deverá o interprete romper com a ótica tipificadora seguida pelo Código Civil, ampliando a tutela da pessoa não apenas no sentido de admitir um aumento das hipóteses de ressarcimento, mas, de maneira muito ampla, no intuito de promover a tutela da personalidade mesmo fora do rol de direitos subjetivos previstos pelo legislador codificador.[247]

Segundo Capelo de Sousa[248], o direito geral da personalidade "é um insofismável direito subjetivo privado" com uma tutela civil mais reforçada do que dos demais direitos subjetivos. Nessa seara que se desenvolve a sua teoria como um direito de personalidade.

4.5. O Direito ao esquecimento no Brasil

No direito brasileiro, pode-se afirmar que o direito ao esquecimento decorre do princípio da dignidade da pessoa humana (art. 1º, inc. III CF/88), porque é essencial para o

[246] A inibição como sinônimo de constrangimento seria tratado como "condição mental ou emocional que dificulta iniciar ou dar prosseguimento a uma ação", ou seja, a inibição limita o exercício de atividade livre e voluntária do sujeito que reclama pelo direito ao esquecimento que não quer que fatos pretéritos, inclusive, o modo e a finalidade com que são lembrados, continuem a repercutir efeitos na sua vida atual. HOUAISS, Antonio. VILLAR, Mauro de Salles. *Minidicionário da Língua Portuguesa*. Rio de Janiro: Objetiva, 2004, p. 417..

[247] TEPEDINO, Gustavo. Cidadania e os direitos da personalidade. In: Revista da Escola Superior da Magistratura de Sergipe. Aracaju, n. 3, 2002, p.4.

[248] DE SOUSA, Rabindranath V. A. Capelo, *O Direito Geral de Personalidade*. Coimbra: Coimbra Editora, 1995, p. 614-615.

pleno desenvolvimento da sua personalidade que fatos pretéritos e desprovidos de interesse público sejam constantemente relembrados no âmbito individual e coletivo.

O indivíduo deve poder se apresentar como é, a si mesmo, independente do meio de comunicação de propagação da informação pretérita, bem como controlar as informações que dizem respeito à sua vida privada. Por tal razão, o direito ao esquecimento é uma figura autônoma que tutela simultaneamente dois bens jurídicos: a identidade e a privacidade do indivíduo.

Decorre do direito geral da personalidade e da sua proteção civil-constitucional, especificamente, do artigo 11 do Código Civil. Esse é o entendimento exarado no Enunciado 531 do CCJ que dita: "A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento". A justificativa merece ser evidenciada:

> Os danos provocados pelas novas tecnologias de informação vêm-se acumulando nos dias atuais. O direito ao esquecimento tem sua origem histórica no campo das condenações criminais. Surge como parcela importante do direito do ex-detento à ressocialização. 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 [249]

Além disso, o direito ao esquecimento na sociedade informacional foi reconhecido em duas situações famosas pelo STJ, caso "Aída Curi" (REsp 1.335.153- RJ) e o da "Chacina da Candelária" (REsp nº 1.334.097), ambos de Relatoria do Min. Luis Felipe Salomão, processos intentados contra o mesmo veículo televisivo, sem que, no entanto, se estabelecesse requisitos objetivos para a sua aplicação.

O caso da "Chacina da Candelária", ocorrido no Rio de Janeiro em 1993, que ganhou repercussão nacional, teve um dos participantes considerado inocente. Ocorre que, anos após a sua absolvição, uma emissora de televisão produziu programa sobre o episódio, destacando novamente o seu nome como uma das pessoas que haviam participado do crime. Com a finalidade de não ver o seu passado remexido, o individuo ingressou com uma ação de responsabilidade civil, argumentando que sua exposição no programa, para milhões de telespectadores, em rede nacional, reacenderia a imagem do

[249] Enunciado 531 do CCJ. Disponível em: http://www.migalhas.com.br/arquivo_artigo/art20130607-02.pdf. Acesso em: 16.12.2017.

fato que passou, violando seu direito à paz, anonimato, privacidade pessoal e seu direito ao esquecimento. Na época dos fatos, foi obrigado a mudar da comunidade em que morava para preservar sua segurança e a de seus familiares.

No caso Ainda Curi foi realizado um pedido de direito ao esquecimento para os familiares da vítima, que, na época foi violentada sexualmente e morta em 1958 por um grupo de jovens. Após o transcurso de anos, a mesma emissora de televisão produziu um programa chamado "Linha Direta" e divulgou o nome e imagem da vítima, até com detalhes do crime.

Para os familiares de Aida Curi, não havia mais a necessidade de se resgatar aquela história que ocorreu há tempos atrás, saindo do debate público, cuja retransmissão traria de volta lembranças e sofrimento do episódio, razão pela qual moveram ação contra a emissora de televisão, também com o pleito de receber indenização por danos morais, materiais e à imagem.

Em ambos os casos, foram sopesados os valores constitucionais, porém no caso Ainda Curi[250] o direito ao esquecimento foi negado uma vez que o fato ganhou cunho histórico e que seria impossível informar a história do caso sem remeter ao nome da vítima.

Por derradeira, observável que o viés do direito ao esquecimento nesses casos enfrentado pelos Tribunais Superiores se traduz mais com a acepção tradicional do direito proposto, coadunando-se com a proteção da privacidade do individuo e do desejo em deixar o passado no passado.

[250] O caso Ainda Curi ainda está em discussão no STJ, ao passo que em junho de 2016 foi realizada uma audiência pública, ao qual teve a participação de juristas e especialistas na matéria, da qual se destaca a professora Cíntia Rosa Pereira de Lima que participou e exarou a pesquisa vasta, bem como a sua tese da existência e autonomia do direito ao esquecimento.

4.6. Legitimidade ativa e passiva de seu exercício

Como direito da personalidade, a legitimidade ativa de seu exercício é, em princípio, do titular de direito, qual seja a pessoa natural, principal atingida com a propagação dos fatos passados.

O pleito sobre o direito ao esquecimento poderá ser exercido também pelos sucessores, isto é, o cônjuge ou qualquer parente até o quarto grau, estando implícito na definição legal, os companheiros e companheiras conviventes em união estável, sem qualquer discriminação, de acordo com a transcrição do art. 12º do Código Civil brasileiro:

> Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei. Parágrafo único. Em se tratando de morto, terá legitimação para requerer a medida prevista neste artigo o cônjuge sobrevivente, ou qualquer parente em linha reta, ou colateral até o quarto grau.

Seguindo a definição proposta pelo professor Antonio Carlos Morato, os direitos da personalidade são "os direitos que versam sobre a própria pessoa e seus reflexos e que são *reconhecidos* à pessoa humana e *atribuídos* à pessoa jurídica", no que couber[251].

Adeptos da teoria de que a pessoa jurídica é também titular de direitos da personalidade estão Carlos Alberto Bittar[252], Rubens Limongi França[253], Antônio Chaves[254], Elimar Szaniawski[255] e Silmara Juny de Abreu[256] que encontram ainda aporte legal no fundamento do artigo 52 do Código Civil que expressamente estabelece: "aplica-se às pessoas jurídicas, no que couber, a proteção dos direitos da personalidade", tendo ainda na seara jurisprudencial a Súmula 227 do Superior Tribunal de Justiça a seu favor.[257]

---

[251] MORATO, Antonio Carlos. *Quadro geral dos direitos da personalidade***.** Revista da Faculdade de Direito (USP), v. 106-107, p. 124.
[252] BITTAR, Carlos Alberto. Os direitos da personalidade. Rio de Janeiro: Forense Universitária, 1989.
[253] FRANÇA, Rubens Limongi. Direitos da personalidade coordenadas fundamentais. Revista do Advogado, São Paulo, n. 38, p. 5-13, dez. 1992.
[254] CHAVES, Antonio. Lições de direito civil: parte geral 3. São Paulo: Bushatsky – Edusp, 1972.
[255] SZANIAWSKI, Elimar. Direitos da Personalidade e sua Tutela. São Paulo: Revista dos Tribunais , 1993.
[256] CHINELLATO, Silmara Juny de Abreu. Comentários à parte geral – artigos 1º a 21 do Código Civil. In: MACHADO, Antonio Cláudio da Costa. (Org.). CHINELLATO, Silmara Juny (Coord.). Código civil interpretado: artigo por artigo, parágrafo por parágrafo. 5. ed. Barueri: Manole, 2012. p. 30-51.
[257]Cf. Súmula n. 227 do STJ: "A pessoa jurídica pode sofrer dano moral".

A expressão "no que couber" é utilizada justamente, porque não há que se falar em direito à vida e direito à integridade física das pessoas jurídicas por causa de impossibilidade fática, Sabe-se que as pessoas jurídicas são uma criação fictícia ou construção artificial. Entre os direitos da personalidade que são admitidos para esse titular de direito estão o direito ao nome e à honra objetiva (reputação).[258]

Não se vislumbra, por hora, a possibilidade do direito ao esquecimento ser invocado pelas pessoas jurídicas. Em analogia com a honra subjetiva[259], verifica-se que faltaria o elemento psíquico apto a formar a consciência do que a pessoa jurídica se desejaria relembrar e esquecer. Soma-se a tal argumento a imprescindibilidade da clausula da dignidade da pessoa humana, inerente para o reconhecimento do direito ao esquecimento, que destina-se somente às pessoas físicas, segundo concepção Kantiana.[260]

A legitimidade passiva será do sujeito que tem o controle sobre a informação e que pode ser "qualquer pessoa física, jurídica ou ente despersonificado, público ou privado, nacional ou estrangeiro, inclusive grupos econômicos"[261] que processa, divulga, publica e republica, ou qualquer outra ação que importe na rememoração do conteúdo passado e constrangedor.

---

[258] Apesar da classificação conhecida entre "imagem-retrato" (representação física) e "imagem-atributo" (reputação, "boa imagem"), adota-se o entendimento do professor Morato para quem essa classificação é ociosa, pois esta pode ser suprimida pelo conceito de honra em seu sentido objetivo. MORATO, Antonio Carlos. Dano à imagem. In: RODRIGUES JUNIOR, Otávio Luiz. et al. (coord.) *Responsabilidade civil contemporânea:* em homenagem a Silvio de Salvo Venosa. São Paulo, Atlas, 2011, p. 566.

[259] GARCIA, Enéas. *Responsabilidade civil dos meios de comunicação.* São Paulo: Juarez de Oliveira, 2002, p. 93.

[260] Atribui-se a Immanuel Kant a elaboração da noção de dignidade da pessoa humana, conceito moderno, o qual sustenta que a pessoa natural possui "um fim em si mesma", pois "no reino dos fins, tudo tem ou um preço ou uma dignidade. Quando uma coisa tem preço, pode ser substituída por algo equivalente; por outo lado, a coisa que se acha acima de todo preço, e por isso não admite qualquer equivalência, compreende uma dignidade". KANT, Immanuel. *Fundamentação da metafísica dos costumes e outros escritos*. Tradução de Leopoldo Holzbach. São Paulo: Martin Claret, 2004, p. 64.

[261] Apesar de indicar os motores de busca como sujeito passivo, o que se discorda, empresta-se a definição de Parentoni sobre os possíveis *data controllers*. PARENTONI, Leonardo. O direito ao esquecimento (*right to oblivion*). In: DE LUCCA, Newton. (coord.). *Direito e Internet III*: Marco Civil da Internet (Lei n. 12.965/2014). Tomo I. São Paulo: Quartier Latin, 2015, p. 582.

4.7. Limitações à aplicação do direto ao esquecimento

Como nenhum direito de personalidade é absoluto, o direito ao esquecimento também comporta suas limitações, seja no interesse público ou nas liberdades de informação, expressão e de imprensa.

O interesse público guarda grande dificuldade de conceituação, porém pode-se citar Celso Antônio Bandeira de Mello, para quem "deve ser conceituado como o interesse resultante do conjunto dos interesses que os indivíduos pessoalmente têm quando considerados em sua qualidade de membros da Sociedade e pelo simples fato de serem"[262], o que não se confunde com o interesse do Estado.

Ora, a presença do interesse público afasta qualquer pretensão ao direito ao esquecimento, porém este não pode ser observado como mera curiosidade. Assim tem entendido a jurisprudência, como nos casos brasileiros da Chacina da Candelária e Caso Aída Curi. Também é o que adota Viviane Maldonado: "o interesse público não se confunde com o interesse do público, este, no mais das vezes, entendido como aquele que se exaure em aspectos de mera satisfação pessoal em termos de curiosidade". [263]

Bem é verdade que a ponderação de interesses deverá ser verificada no caso concreto. Assim, compreende Anderson:

> E não raro o exercício do direito de 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 os riscos trazidos pela recordação do fato à pessoa envolvida. [264]

Assim, exige-se a compatibilização dos direitos em conflito para que a proteção da personalidade aconteça, "sem que isto se traduza em censura ou inviabilização do direito de expressão e informação legítima". [265]

---

[262] MELLO, Celso Antonio Bandeira de. Curso de direito administrativo. 26 ed. São Paulo: Malheiros, 2009, p. 61.

[263] MALDONADO, Viviane Nóbrega. *O direito ao esquecimento.* Barueri,SP: Novo Século Editora, 2017, p. 115.

[264] SCHREIBER, Anderson. *Direitos da Personalidade.* 3 ed. São Paulo: Atlas, 2014, p. 174

[265] MARTINEZ, Pablo Dominguez. *Op. cit.* p. 180.

A liberdade de expressão, informação e imprensa não podem ser colocadas em um pedestal. Não há prevalência de interesses constitucionalmente consagrados. Dessa forma, merece atenção a real utilidade da informação que se distancia da curiosidade pública. [266]

Nenhum direito é absoluto tampouco o direito ao esquecimento, pois o interesse efetivo público e a utilidade da informação são um parâmetro a ser utilizado para que a informação potencialmente danosa seja rememorada em razão de publicação ou republicação do fato constrangedor depois do transcurso do tempo.

Valendo-se dos critérios bem analisados na obra de Pablo Martinez sobre "Direito ao esquecimento: a proteção da memória individual na sociedade da informação", adota-se o entendimento de que a importância da informação seja analisada também pela sua atualidade e pelo lapso temporal decorrido entre o fato e sua republicação, isto é, valendo-se dos prazos prescricionais no momento de julgar o caso concreto.

A utilização dos prazos prescricionais é uma forma de analisar o tempo de vida útil da informação pessoal pretérita e potencialmente danosa, objeto do direito ao esquecimento.

Como não há ainda norma específica que tutele o direito ao esquecimento[267], por hora, adotam-se os prazos prescricionais estipulados no Código de Defesa do Consumidor para fatos comuns no Código Penal para os fatos criminosos no âmbito brasileiro. [268]

No âmbito do criminal, valendo-se da regra da reincidência, sugere-se a adoção do prazo de cinco anos contados a partir da data do cumprimento da pena ou da sua extinção, para que um fato criminoso seja publicado, republicado ou permaneça disponível de acesso na internet, neste ultimo particular, caso tenha manifestação do interessado para a sua remoção após o prazo indicado. [269]

---

[266] *Idem, ibidem.*

[267] Atualmente, em pesquisa, foi encontrada a tramitação de oito projetos de lei que visam conceituar e tutelar o direito ao esquecimento no Brasil. São eles: PL 1589/2015, de proposição da deputada Soraya Santos; PL 215/2015, de proposição do Deputado Hildo Rocha; PL 1547/2015 de proposição do Deputado Expedito Neto; PL 7881/2014, de proposição do Deputado Eduardo Cunha; PL 1676, de proposição do Deputado Vital do rêgo; PL 2712/2015, de proposição do Deputado Jefferson Campos; PL 8443/2017, de proposição do Deputado Luiz Lauro Filho; PL 10087/2018, de proposição do Deputado Francisco Floriano. Analisou-se que todas as propostas legislativas restringem ou ampliam muito o direito ao esquecimento, confundindo-o com outros direitos de personalidade tais como a privacidade, o nome, a imagem e a proteção dos dados pessoais, sem adotar regras claras e precisas, com critérios ou parâmetros que auxiliem na sua aplicação.

[268] Compartilha-se da mesma ressalva do autor Martinez no sentido de que não se pretende estabelecer prazos inalteráveis como regras de conduta a serem obrigatórias de aplicação: "Não se pretende aqui determinar prazos fixos e imutáveis, já que tal poder só caberia à lei, que, em razão de seu império, definiria marcos e prazos, tornando a superação de tais limites atividade ilegal, transformando o lícito em ilícito". MARTINEZ, Pablo Dominguez. *Op. cit*., p.194.

[269] É o que dispõe o artigo 64 do Código Penal para fins de verificação da reincidência: "Art. 64 - Para efeito de reincidência: I - não prevalece a condenação anterior, se entre a data do cumprimento ou extinção da pena

Cediço que fatos relativos à matéria criminal envolvem questões de interesse público, mas que pode desaparecer em razão do tempo. É o que compreendeu o Ministro Luís Felipe Salomão, no julgamento do caso da Aída Curi:

> O interesse público que orbita o fenômeno criminal tende a desaparecer na medida em que também se esgota a resposta penal conferida ao fato criminoso, a qual, certamente, encontra seu último suspiro, com a extinção da pena ou com a absolvição, ambas irreversivelmente consumadas. E é nesse interregno temporal que se perfaz também a vida útil da informação criminal, ou seja, enquanto durar a causa que legitimava. Após essa vida útil da informação, seu uso só pode ambicionar, ou um interesse histórico, ou uma pretensão subalterna, estigmatizante, tendente a perpetuar no tempo as misérias e vicissitudes humanas. Não se pode, pois, nestes casos, permitir a eternização da informação. [270]

A opção pela regra do prazo da reincidência como parâmetro de divulgação de fatos criminosos, contados da data do cumprimento da pena ou de sua extinção, revela-se mais adequado do que simplesmente a contagem de prazo prescricional antes e depois do trânsito em julgado da sentença, do *ius puniendi* estatal.[271] Esse severo posicionamento exposto nesta dissertação se dá por causa dos efeitos da conduta lesiva a um bem jurídico compreendido como fundamental na sociedade, razão pela qual merece um regramento mais rigoroso.

Ora, após o cumprimento da pena, o transcurso do prazo prescricional e do prazo para aferição da reincidência, não há razão para a divulgação de fato criminoso que impeça a reinserção da pessoa do réu na sociedade. Para o professor Claudio Luiz Godoy, o direito ao esquecimento:

> Cuida-se inclusive de garantir ou facilitar a interação e reintegração do indivíduo à sociedade, quando em liberdade, cujos direitos da personalidade não podem, por evento passado e expirado, ser diminuídos. Isso encerra até corolário da admissão, já antes externada, de que fatos passados, em geral, já não mais despertam interesse coletivo. Assim também com relação ao crime, que acaba

---

e a infração posterior tiver decorrido período de tempo superior a 5 (cinco) anos, computado o período de prova da suspensão ou do livramento condicional, se não ocorrer revogação (...)". BRASIL. Código Penal. Decreto-lei nº 2.848, de 07 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm. Acesso em: 01.06.2018.

[270] BRASIL STJ, Resp nº 1.335-153-RJ, Rel. Min. Luís Feipe Salomão, 4ª turma, j. 28/05/2013, p. 35.

[271] O autor Martinez estabelece como parâmetro para a divulgação ou republicação dos fatos criminosos os artigos 109 e 110 do Código Penal, o que, como esclarecido acima, revela-se ainda uma posição mais branda do que aquela que foi adotada nesta dissertação. MARTINEZ, Pablo Dominguez. *Op. cit*. p 197-199.

> perdendo, com o tempo, aquele interesse público que avultava no momento de seu cometimento ou mesmo de seu julgamento. É claro que essa consideração não se aplica àqueles crimes históricos, que passam enfim para a história, aos grandes genocídios, como é exemplo nazista, citado por Costa Andrade. Aliás, pelo contrário, esses são casos que não devem ser esquecidos. [272]

Como bem explicado, em outras palavras, fatos criminosos que ganharam contornos históricos não serão objeto do direito ao esquecimento. O indivíduo interessado não poderá se valer do direito ao esquecimento a fim de obstar a circulação, a manutenção e o acesso a essas informações históricas, pois se revestem de interesse público. É necessário também se conhecer o passado, a história, para que, muitas vezes, se consiga compreender e aplicar o direito no presente, fazendo o uso do método da hermenêutica jurídica de interpretação histórica.

Já os fatos comuns ou não criminosos, de conteúdo pessoal, despidos de valor histórico, merecem um maior abrandamento, ou seja, a aplicação de prazos prescricionais menores, pois não se deve colocar em pés de igualdade os efeitos da punição do Estado, a repressão criminal, e a divulgação de acontecimentos ordinários.

A divulgação de fatos comuns que envolvem dados pessoais, tais como, fotos, vídeos, notícias, postagens em redes sociais, entre outros, também deve ter um prazo que se encerrará a sua utilização e acesso pelo público.

Diante da ausência de regulamentação, optou-se pela prescrição do Código de Defesa do Consumidor que estipula o prazo de cinco anos para que informações negativas sobre o consumidor fiquem disponíveis nos cadastros, fichas e registros. [273] Aplica-se o diploma consumerista brasileiro ao invés da prescrição de dez anos do Código Civil[274], principalmente, quando a informação encontra-se na internet, local em que, como já salientado nos capítulos 1 e 2, existe uma remuneração indireta dos provedores de aplicação pelo uso dos dados pessoais. Portanto, espera-se que o prazo de cinco anos contados da ocorrência do fato seja razoável para a circulação dessas informações pessoais

[272] GODOY, Claudio Luiz Bueno de. *A liberdade de imprensa e os direitos a personalidade*. São Paulo: atlas, 2001, p. 89-90.

[273] Conforme art. 43 do Código de Defesa do Consumidor: "O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. (...)"

[274] Regra do artigo 205 do Código Civil: "A prescrição ocorre em dez anos, quando a lei não lhe haja fixado prazo menor.".

que não apresentem qualquer interesse público na sua manutenção e divulgação nos meios de comunicação em massa.

Notável que não se intende estabelecer critérios obrigatórios e distantes do caso concreto. Caberá ao aplicador do direito, o julgador, realizar o cotejo entre os direitos fundamentais da liberdade de expressão, de informação e de imprensa e o direito ao esquecimento para deferir a remoção de fatos pretéritos e que causam certo constrangimento pessoal aos legitimados ativos.

A ordem constitucional que irá conduzir igualmente o debate é também a clausula geral da dignidade da pessoa humana que encontra o seu fundamento Kantiano em "ser um fim em si mesmo". [275]

A permanência da informação passada não pode prevalecer sobre a dignidade da pessoa humana, pois esta objetiva "um complexo de direitos e deveres fundamentais que asseguram a pessoa tanto contra todo e qualquer ato de cunho degradante e desumano, como venham a lhe garantir as condições existenciais mínimas para uma vida saudável". [276]

[275] KANT, Immanuel. *Fundamentação da metafísica dos costumes e outros escritos*. Tradução de Leopoldo Holzbach. São Paulo: Martin Claret, 2004.
[276] SARLET, Ingo Wolfgang. *Dignidade da pessoa humana e Direito Fundamentais na Constituição Federal de 1988.* Porto Alegre: Livraria do Advogado, 2007, p. 62.

CAPÍTULO V – A DESINDEXAÇÃO DE DADOS PESSOAIS

5.1. Desindexação: sentido

Conforme já mencionado no Capítulo 2, no âmbito do modelo europeu, vislumbrou-se a necessidade de harmonização em relação a diversos aspectos legais, dentre eles a questão da proteção de dados pessoais e da privacidade perante os desafios que a internet e seus desdobramentos trouxeram.

Esforços foram envidados para a atualização da Diretiva 95/46/CE, cujo estudo "*A Comprehensive Approach on Personal Data Protection in the European Union*" em 2010, revelou, entre outras preocupações, o que se convencionou chamar de "*The Right to Be forgotten*", especificamente, o item 2.1.3 ("*Enhancing control over one's own data*") chegou a defini-lo como o direito dos indivíduos de não terem os seus dados pessoais processados e apagados quando eles não forem mais necessários para os propósitos legítimos para qual foram coletados. [277] [278]

[277] Já nesse parecer do ano de 2010, constatou-se que o usuário não tem um livre acesso aos seus dados pessoais que estão sob o poder de terceiros (controladores de dados). Como exemplo, cita a questão das redes sociais que, na época, proporcionavam poucos meios para que tal acesso fosse efetivo: " O exemplo das redes sociais on-line é particularmente relevante aqui, pois apresenta desafios significativos ao controle efetivo do indivíduo sobre seus dados pessoais. A Comissão recebeu várias perguntas de indivíduos que nem sempre conseguiram obter dados pessoais de fornecedores de serviços online, como as suas imagens, e que, por conseguinte, foram impedidos de exercer os seus direitos de acesso, retificação e eliminação". (tradução livre). Segue trecho original: "*The example of online social networking is particularly relevant here, as it presents significant challenges to the individual's effective control over his/her personal data. The Commission has received various queries from individuals who have not always been able to retrieve personal data from online service providers, such as their pictures, and who have therefore been impeded in exercising their rights of access, rectification and deletion*". Além disso, outra preocupação ocorria em relação aos limites de processamento de dados conforme o seu propósito (princípio da minimização de dados). Nesse sentido que a desindexação se aplicaria para limitar a utilização dos dados: "a limitação do processamento dos controladores de dados em relação aos seus propósitos (princípio de minimização de dados)"(tradução livre). Segue trecho original: "*the limitation of the data controllers' processing in relation to its purposes (principle of data minimisation*)". Disponível em: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf. Acesso em: 15.12.2017.

[278] O estudo delimita e exemplifica uma hipótese do exercício do direito a proteção de dados pessoais, tratando-o como o direito ao esquecimento: "esclarecer o chamado "direito ao esquecimento", ou seja, o direito dos indivíduos de terem seus dados não mais processados e excluídos quando não forem mais necessários para fins legítimos. Esse é o caso, por exemplo, quando o processamento é baseado no consentimento da pessoa e quando ele retira o consentimento ou quando o período de armazenamento expirou". (tradução livre). Segue trecho original: "*clarifying the so-called 'right to be forgotten', i.e. the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes. This is the case, for example, when processing is based on the person's consent and when he or she withdraws consent or when the storage period has expired*;".*idem, Ibidem*, p. 8.

O parecer alertou para um dos desafios no ambiente online, qual seja a retenção de dados pelos responsáveis sem que a pessoa em questão esteja informada ou que tenha concedido o seu consentimento ou que o tempo de permanência do dado se expirou. Os usuários devem sempre poder acessar, corrigir, excluir e suspender o tratamento de seus dados pessoais, salvo razões legítimas autorizadas pela lei.

Esses direitos já existiam no quadro jurídico europeu, conforme Diretiva 95/46/CE. No entanto, a forma pela qual esses direitos poderiam ser exercidos apresentavam divergências entre a legislação de cada Estado-membro. Por isso, a atualização da diretiva era demanda indispensável para uma harmonização das regras de proteção de dados pessoais. [279]

Em outra ocasião, no dia 22 de janeiro de 2012, a comissária Viviane Reding apresentou uma proposta de atualização da Diretiva 95/46/CE que assim previa o direito ao esquecimento (apagamento de dados) como: "Se um indivíduo não quiser mais que seus dados pessoais sejam processados ou armazenados por um controlador de dados, e se não houver uma razão legítima para mantê-los, os dados deverão ser removidos do sistema". [280]

O Regulamento Geral nº 2016/679, aprovado no dia 27 de abril de 2016, pelo Parlamento e Conselho, trouxe em seu artigo 17, no Capítulo III "Direitos do titular dos dados", Secção 3ª "Retificação e apagamento", do Regulamento Geral Europeu 2016/679, o direito a ser esquecido:

Artigo 17.o Direito ao apagamento dos dados («direito a ser esquecido»)

[279] É o que se extrai do trecho do citado Parecer: "Os indivíduos devem sempre poder acessar, retificar, excluir ou bloquear seus dados, a menos que haja motivos legítimos, previstos por lei, para impedir isso. Esses direitos já existem no atual marco legal. No entanto, a forma como estes direitos podem ser exercidos não é harmonizada e, portanto, o seu exercício é, na verdade, mais fácil em alguns Estados-Membros do que noutros. Além disso, isto se tornou particularmente desafiante no ambiente online, onde os dados são frequentemente mantidos sem que a pessoa em causa seja informada e /ou tenha dado o seu consentimento a ela.". (tradução livre). Segue trecho original: "*Individuals should always be able to access, rectify, delete or block their data, unless there are legitimate reasons, provided by law, for preventing this. These rights already exist in the current legal framework. However, the way in which these rights can be exercised is not harmonised, and therefore exercising them is actually easier in some Member States than in others. Moreover, this has become particularly challenging in the online environment, where data are often retained without the person concerned being informed and/or having given his or her agreement to it*.", ibidem, p. 07.

[280] Segue trecho original: "*If an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system.*" REDING, Viviane. *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital* Age 5 (Jan. 22, 2012). Disponível em: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF. Acesso em: 15.12.2017.

1.O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes 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.o, n.o 1, alínea a), ou do artigo 9.o, n.o 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.o, n.o 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.o, n.o 2;

d) Os dados pessoais foram tratados ilicitamente;

e) Os dados pessoais têm de ser apagados 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.o, n.o 1. 2.Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.o 1, 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.

3.Os n.os 1 e 2 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.o, n.o 2, alíneas h) e i), bem como do artigo 9.o, n.o 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.o, n.o 1, na medida em que o direito referido no n.o 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.

Como é possível observar, o "direito a ser esquecido", para o novo regulamento, tratar-se-ia de um direito ao "apagamento", ou seja, a supressão dos dados pessoais, sem demora injustificada, seguindo os motivos legais.

Dentre os motivos legais, destaca-se o princípio da finalidade em que o fim para qual se motivou o tratamento de dados pessoais ocorreu deixa de existir, o exercício da garantia de oposição e do consentimento que é revogado, bem como o tratamento dado de forma ilícita.

Ocorre que, como se analisou no Capítulo anterior, o direito ao esquecimento não se confunde com o direito à proteção de dados pessoais. A proteção dos dados pessoais é autônoma e poderá auxiliar no exercício do direito ao esquecimento por meio da remoção do conteúdo de informações verídicas e constrangedoras que devem permanecer no passado.

Para o exercício do direito à proteção de dados pessoais no que se refere a faculdade de remoção ou supressão, o próprio Regulamento estipula os limites legais para tanto, quais sejam a presença: i) do interesse público seja para a questão da saúde pública ou para cunho de investigação estatística, cientifica e histórica; ii) da liberdade de expressão e de informação que na ponderação de interesses prevaleça necessariamente; iii) de obrigação legal que deverá ser cumprida; iv) de declaração, exercício ou defesa de um direito no processo judicial, o que não deixa de ser uma obrigação legal a ser desempenhada.

Tal faculdade de supressão de dados pessoais no tocante à atividade dos motores de busca tem-se nomeado de um direito à desindexação de dados pessoais.

Tendo em vista todas as discussões que orientaram a reforma da Diretiva 95/46, digno de nota é um caso espanhol considerado paradigma para o tema e que avivou o interesse de outros países em regulamentar o que se chamou de direito ao esquecimento na Era Digital.

Trata-se do caso Mário Costeja González vs *Google Search Spain* que alterou de forma substancial o tratamento da matéria e o comportamento dos motores de busca como Google, Yahoo, Bing, entre outros, pois foi lhe reconhecido um direito à desindexação, como será demonstrado.

5.2. O exercício do direito à proteção dos dados pessoais em face dos motores de busca reconhecido pelo Tribunal Europeu

A Corte Europeia reconheceu um direito à desindexação de dados pessoais, em maio de 2014, caso que ficou conhecido como "*Gonzáles* vs *Google Spain*", o qual um advogado espanhol ajuizou uma demanda para que a informação sobre um leilão de um bem dele efetuado para pagar dívida da Previdência Social, nos anos 90, fosse retirada do site de busca[281].

Porém, um estudo se faz necessário para se compreender da onde surgiu essa figura da "desindexação", se esta decorre do direito à oposição (art. 14, "a") e ao cancelamento de dados pessoais (art. 12, "b"), de acordo com as normas da Diretiva 95/46/CE aplicada à época dos fatos.

Além disso, a atividade dos motores de busca reflete na vida dos usuários da internet que, muitas vezes, deixam se levar pelo serviço prestado, mas não compreendem que a atuação desse provedor de aplicação é altamente lucrativa justamente por conta do tratamento de dados que exerce.

Entretanto, em território brasileiro, não há um consenso, por assim se dizer, sobre a atividade desenvolvida dos motores e busca, isto é, se os motores de busca devem ser obrigados a desindexarem os dados pessoais. A principal questão que atrelaria os motores de busca ao cumprimento da legislação europeia de proteção de dados seria o seu enquadramento como "responsável" pelo tratamento de dados, o que somente se consegue averiguar por meio da seguinte pergunta: os motores de busca realizam ou não o tratamento de dados pessoais?

Para clarificar eventuais questões que naturalmente surgirão sobre o funcionamento da função de indexação pelos motores de busca, aponta-se, em síntese, que é uma das tarefas executadas pelo programa com o objetivo de possibilitar a localização de arquivos, web sites, imagens e vídeos que, em outro momento, serão apresentados como resultado da pesquisa realizada pelo usuário. Para maiores detalhes, sugere-se retornar ao Capítulo 3, o

[281] *An internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties***.** Press Release nº 70/14. Luxembourg, 13 May 2014. Disponível em: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf. Acesso em: 14/10/2014.

qual apresenta todas as definições e substrato necessário para compreender o que são os motores de busca e o funcionamento da internet.

Em suma, revela-se essencial descrever o Caso *Mário Costeja Gonzáles* vs *Google Spain* a fim de compreender os contornos do direito à desindexação dos dados pessoais solicitados pelo sujeito a quem este se refere.

5.2.1. Análise do caso do Mário Costeja González vs *Google Search Spain*

O Caso *Mário Costeja Gonzáles* origina-se de uma Reclamação efetuada por Mário junto a A*gencia Españhola de Protección de Datos* (AEPD)[282], em 05 de março de 2010, em face do jornal *La Vanguardia*, da *Google Spain* e da *Google Inc*, exigindo a exclusão da fonte original (site) bem como do motor de busca de determinada informação. Isso porque, quando o internauta digitasse o nome de Mario Costeja Gonzáles na interface do motor de busca do Google, obtinha a indexação de duas páginas daquele jornal sobre a venda de imóveis em hasta pública para saldar débitos que possuía junto à Seguridade Social.

Na verdade, originalmente, tal noticia era de uma edição impressa do jornal *La Vanguardia* que constavam dois editais sobre o leilão publicados no ano de 1998. Posteriormente, as publicações foram digitalizadas para fins de arquivamento.

Em novembro de 2009, Mario Costeja encaminhou uma notificação ao citado jornal para que este excluísse a publicação de seu site, sob o argumento de que o processo se encerrou há muito tempo. Em resposta, o jornal negou o pedido de exclusão uma vez que a informação era oficial e pública.

Posteriormente, em fevereiro de 2010, Mario acionou o *Google Spain* (Google do Estado-membro da Espanha) para que este excluísse de seu mecanismo de busca as

[282] A Agência Espanhola de Proteção de Dados é uma autoridade supervisora prevista na LOPD (Ley Ogânica 15/1999) que trata da proteção dos dados pessoais no território espanhol, pois por meio dessa lei que a Espanha internalizou as regras comunitárias da Diretiva 95/46/CE. Assim, a AEPD é definida como ““‘*un Ente de Derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones*” no artigo 35 da LOPD. Disponível em: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/2014/Ley_Organica_15-1999_de_13_de_diciembre_de_Proteccion_de_Datos_Consolidado.pdf. Acesso em: 12.12.2015.

páginas do site que continham tal informação, o que, por sua vez, remeteu o pedido ao *Google Inc*, que também o recusou. [283]

Mario ingressou com a tal reclamação em face do jornal postulou: a) a supressão ou alteração das respectivas páginas, fazendo com que seus dados viessem a desaparecer, ou b) a adoção de determinadas medidas disponibilizadas pelos próprios motores de busca para proteger esses dados.

Já, em face do Google, solicitou: a) obter a supressão ou ocultação de seus dados pessoais no provedor de pesquisa, fazendo com que os resultados do jornal *La Vanguardia* com a ligação do seu nome deixassem de aparecer ali.

A Agência Espanhola de Proteção de Dados, em 30 de julho de 2010, indeferiu o pedido de remoção das publicações das páginas do site do jornal *La Vanguardia*, mas acolheu o pedido contra a *Google Spain* e a *Google Inc*. O entendimento exarado foi o de que os motores de motores de busca deveriam respeitar a legislação de proteção de dados.

A *Google Spain* e a *Google Inc* manejaram apelo à Suprema Corte Espanhola, denominada de Audiência Nacional, abrindo um expediente para anular tal decisão. Diversos pontos foram alegados, dentre os quais cumpre destacar as seguintes indagações:

> 1) se as ferramentas de busca realizam atividades descritas no artigo 2º, alínea "b" da Diretiva 95/46/CE; 2) se o operador desta ferramenta de busca pode ser considerado responsável pelo tratamento dos dados nos termos da Diretiva 95/46/CE; e 3) se a *Google* estaria sujeita à lei espanhola e poderia ser processada e condenada por um órgão espanhol pois sua sede está em outro país, inclusive não sendo membro da União Europeia.[284]

O órgão jurisdicional nacional suspendeu a Instancia e submeteu o caso ao Tribunal de Justiça da União Europeia. A esse respeito, o advogado geral da Corte de Justiça européia Niilo Jääskinen, emitiu parecer, no dia 25 de junho de 2013, o qual opinou pela procedência do apelo do grupo *Google*:

> Hoje em dia, a proteção dos dados pessoais e da privacidade das pessoas singulares torna-se cada vez mais importante. Qualquer conteúdo que contenha

[283] MALDONADO, Viviane Nóbrega. *O direito ao esquecimento.* Barueri,SP: Novo Século Editora, 2017, p. 103-104

[284] LIMA, Cíntia Rosa Pereira. O conceito de tratamento de dados após o caso Google Spain e sua influência na sociedade brasileira. In: *III Encontro de Internacionalização do CONPEDI*. Madrid : Ediciones Laborum, 2015. V. 9., p. 120. Disponível também em: http://www.conpedi.org.br/wp-content/uploads/2016/03/Vol.-9-Madrid.pdf. Acesso em: 02.02.2016.

> dados pessoais, sob a forma de textos ou de materiais audiovisuais, pode ser disponibilizado de forma instantânea e permanente em formato digital a nível mundial. A Internet revolucionou as nossas vidas ao remover os obstáculos técnicos e institucionais à difusão e à recepção de informação, e criou uma plataforma para diversos serviços da sociedade da informação. Estes beneficiam os consumidores, as empresas e o conjunto da sociedade. Isto deu origem a condições inéditas nas quais há que encontrar um equilíbrio entre os diversos direitos. [285]

O advogado questiona, em um dos seus tópicos, se: "Os direitos de retificação, apagamento, bloqueio e oposição previstos na diretiva traduzem-se no direito da pessoa em causa de ser esquecida?" e, em seguida, entende: "Concluo, portanto, que os artigos 12.°, alínea b), e 14.°, alínea a), da diretiva não preveem um direito de ser esquecido".

A Corte de Justiça da União Europeia não acolheu o Parecer do advogado e decidiu em 13 de maio de 2014[286] que a atividade de um motor de busca consistente na coleta das informações disponibilizadas na internet por terceiros, indexação, armazenamento e disposição, configura tratamento de dados pessoais, devendo o motor de busca ser responsável pelo tratamento que realiza, nos termos do artigo 2º, alínea "b" e "d" da Diretiva 95/46/CE.

Em síntese, o Tribunal decidiu ainda que a instalação de uma filial da *Google Inc.* no território espanhol, corrobora com o preenchimento do critério "estabelecimento", porque o tratamento é realizado com os dados dos cidadãos espanhóis, satisfeito o elemento de conexão definido no art. 4º, "a" da Dir. 95/46/CE.

E que o fato das informações serem inadequadas, impertinentes e excessivas em relação as finalidades do tratamento realizado pelo motor de busca, que tais informações deveriam ser desindexadas ou "deslistadas".

---

[285] JÄÄSKINEN, Nillo. Parecer no caso Google Spain x Agencia Espanhola de protección de Dados. Apresentado em 25 de junho de 2013 no Processo C – 131/12. Disponível em: https://www.conjur.com.br/dl/parecer-google-direito-esquecimento.pdf. Acessado em: 07.03.2016.

[286] Segue ementa do que foi decidido pela Corte de Justiça da União Europeia, no dia 13 de maio de 2014: "SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala) de 13 de mayo de 2014 «Datos personales — Protección de las personas físicas en lo que respecta al tratamiento de dichos datos — Directiva 95/46/CE — Artículos 2, 4, 12 y 14 — Ámbito de aplicación material y territorial — Motores de búsqueda en Internet — Tratamiento de datos contenidos en sitios de Internet — Búsqueda, indexación y almacenamiento de estos datos — Responsabilidad del gestor del motor de búsqueda — Establecimiento en territorio de un Estado miembro — Alcance de las obligaciones de dicho gestor y de los derechos del interesado — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 7 y 8»." Disponível em: Disponível em: http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_justicia/common/3._Sentencia_Gran_Sala_de_13_de_mayo_de_2014._Asunto_C-131-12._Google_v_AEPD_y_Mario_Costeja.pdf. Acessado em: 07.03.2016.

Ponto sensível da decisão foi a determinação de que as próprias ferramentas de busca teriam o poder de verificar o que deveria ser desindexado ou não da sua lista, o que gerou debates sobre a análise que este faria e a sua possível parcialidade.

Após o reconhecimento do direito à desindexação de dados pessoais nesta decisão paradigmática, qualquer usuário habitante da União Europeia pode responder a um formulário requerendo a exclusão de informações pessoais diretamente com a *Google*. Assim, após a referida decisão, o motor de busca *Google* da Espanha recebeu 12 mil pedidos de usuários para apagar informações pessoais em apenas 24 horas[287].

Sergio Branco critica o posicionamento de deixar a cargo do Google a decisão sobre as demandas que merecem ou não serem desindexadas: "além de atribuir ao entre privado o dever de julgar se uma informação deve ou não ser acessada, promove-se censura privada e o risco de se provocar um apagão histórico". [288]

Concorda-se que o ente privado não seria o órgão mais adequado para julgar as pretensões de direito à desindexação, já que poderá ter uma tendência de interesses por de trás da manutenção ou não do conteúdo/página do site, vídeo e imagem na lista de resultados. Por outro lado, abarrotar o Poder Judiciário com pedidos de remoção de links, que, infelizmente, não seria o órgão mais célere, poderá perpetuar a informação e, por consequência, continuar violando o direito à proteção dos dados pessoais.

Observa-se que o caso *Costeja* contra o motor de busca não foram verificadas a ponderação de interesse de informação e proteção de dados pessoais, mas tão somente decidiu-se pela desindexação que dificulta o acesso àquela informação, notadamente, pelos princípios da qualidade dos dados, finalidade e proporcionalidade.

Nesse sentido, entende Sergio Branco:

> Finalmente, aqui se torna mais evidente não se tratar propriamente de direito ao esquecimento, mas mero desejo de desindexação. Uma vez que o conteúdo repudiado continua disponível no site, não se pode nem mesmo de modo impróprio chamar o pleito de direito ao esquecimento. Há, no máximo, a emoção do link da lista de busca. [289]

[287] CHAVES, Reinaldo. *Direito ao esquecimento – Em um dia, Google recebe 12 mil pedidos para apagar informações.* Consultor Jurídico, 02/06/2014. Disponível em: http://www.conjur.com.br/2014-jun-02/dia-google-recebe-12-mil-pedidos-apagar-informacoes. Acesso em: 14/10/2015.
[288] BRANCO, Sérgio. *Memória e esquecimento na internet*. Porto Alegre: Editora: Arquipélago Editorial, 2017, p. 161.
[289] *Ibidem.*

Não houve a supressão da informação na sua fonte originária, logo a pretensão se relacionou com a desindexação que, nada mais é que o direito de oposição, cancelamento e remoção do link no motor de busca.

Por derradeira, a manutenção de dados desatualizados, irrelevantes e impertinentes, em prol de um "superinformacionismo", resultando na conservação de uma identidade "virtual" distante daquela real, pode ser uma atividade considerada como tratamento de dado pessoal indevido. Cediço que a obstrução do acesso a essas informações pode ser a pretensão do titular e que revela ser um importante aliado para o desenvolvimento da pessoa humana.

5.3. A desindexação como instrumento da proteção aos dados pessoais

A desindexação de dados pessoais promovida pelos motores de busca é um instrumento valioso para que o usuário do serviço não veja resultados irrelevantes, excessivos e desatualizados sobre si mesmo, inclusive, permanecendo à disposição de consulta pelos usuários da Web. A atividade desenvolvida pelos motores de busca caracteriza o conceito de tratamento de dados pessoais e, como tal, merece toda a tutela jurídica as leis de proteção.

Até porque, a capacidade de armazenamento de informações é tão potente que, em 2007, o motor de busca *Google* passou a construir perfis dos usuários a partir de arquivos de todas as pesquisas efetuadas por cada internauta e dos resultados de busca mais acessados[290]. Assim, André Brandão Nery Costa asseverou que não é exagero afirmar que os motores de busca conhecem mais sobre nós do que nós mesmos[291].

Tendo em vista a relevância da atividade desempenhada pelos motores de busca, imprescindível se faz o direito de remover da lista de consulta àqueles resultados que não merecem estar ali.

[290] HELF, Miguel. *Google Ads a Safeguard on Privacy for Searchers*, New York Times, 15.3.2007. Disponível em: Acesso em: http://www.nytimes.com/2007/03/15/technology/15googles.html?_r=0. Acesso em: 115/10/2014.

[291] COSTA, André Brandão Nery**.** *Direito ao esquecimento na Internet: a Scarlet Letter Digital*. In: SCHREIDER, Anderson (coord.). Direito e mídia. São Paulo: Atlas, 2013, p.188.

O direito à desindexação seria uma faculdade jurídica que está compreendida no novo Regulamento Geral Europeu. Não se trata de um direito autônomo, absoluto e oponível erga omnes, mas decorre do direito à proteção de dados pessoais.

Segundo Francisco Amaral, as "faculdades jurídicas distinguem-se, assim, dos direitos subjetivos por não terem autonomia e deles serem dependentes. São como desdobramentos do próprio direito, sem existência autônoma".[292] Nesse sentido que se defende uma desindexação de dados pessoais que no caso espanhol deu-se em razão da sua oposição ou cancelamento.

Define-se assim, o direito à desindexação, nas palavras de Franco Pizzetti como "[...] o direito de não ver facilmente encontrada uma notícia que não mais seja atual. O principal efeito de indexar e divulgar as notícias por meio do mecanismo de pesquisa é, de fato, concorrer de forma contínua para reativar toda a informação, criando um perfil da pessoa"[293], cujos elementos que se referem a pessoa se tornem o próprio produto a ser comercializado pelos motores de busca.

Na verdade, tal definição seria demasiadamente restritiva ao caso Costeja, pretende-se aqui compreender um direito à desindexação como uma faculdade jurídica do direito à proteção dos dados pessoais, cujo exercício ocorre pela remoção ou supressão da informação nos motores de busca, de acordo com os motivos legais, como por exemplo, aqueles expostos no Regulamento Geral Europeu que se convencionou em denominar de "direito ao esquecimento".

A apreciação de casos concretos que se denote a ausência de razoabilidade na exibição dos resultados de busca que tenham um conteúdo essencialmente privado e particular, conforme a aplicação da legislação ou arcabouço protetivo que se refere ao tratamento de dados pessoais, sem que isso revele a imputação de que o motor de busca realizaria a função de um "verdadeiro censor digital", filtrando o conteúdo inserido por terceiros.

Embora os Estados Unidos não adotem um modelo de proteção de dados pessoais que comporta um Regulamento Geral de proteção de dados pessoais como o da comunidade europeia, privilegiando assim um sistema de "autorregulação do setor

[292] AMARAL, Francisco. *Direito civil.* Introdução. Rio de Janeiro: Renovar, 2008, P. 238.

[293] Segue trecho original: *"[...] il diritto a non vedere facilmente trovata uma notizia non più attuale. L'effetto principale della indicizzazione e difusione dele notizie attraverso il motore di ricerca è infatti quello di concorrere in modo continho a riattualizzare tutte le informazioni, facendole diventare tutte elementi del prodilo in atto della persona a cui si riferiscono"*. PIZZETTI, Franco. Le autorità per la Protezione dei Dati Personali e la Sentenza della Corte di Giustizia sul Caso Google Spain: è Tempo di Far Cadere il "Velo di Maya". In: Il Diritto dell'informazione e dell'informatica, 2014, fasc. 4-5, Giuffrè, pp. 805-829, p. 808.

privado"[294], o advogado norte-americano Mark T. Andrus destacou que os motores de busca são pessoas jurídicas que reúnem informações pessoais e obtêm lucro com as mesmas, o que as enquadraria no conceito de *Consumer Reporting Agency* (CRA), isto é, um banco de dados de consumidores que trabalham com crédito. Isso porque, o marketing e a publicidade que envolve os motores de busca que lucram com a publicação dos anúncios seria suficiente para ampliar o conceito de CRA a fim de tutelar os usuários como consumidores. [295]

Ao discorrer sobre esse artigo, Viviane Maldonado entende que "os motores de busca operam na forma de base de dados de consumidores, de sorte que tal aspecto, de *per si*, pode sustentar a formulação de pedidos de exclusão ou *delisting* em solo-americano".[296] De certo que tratar a ideia dos usuários como consumidores, ainda no âmbito do modelo norte-americano, seria uma saída a fim de se proteger os dados pessoais, isto é, a própria pessoa. Ocorre que, nem todos os motores de busca se valem da publicidade direta ou indireta para realizarem a sua atividade de tratamento de dados, o que, nessa linha de raciocínio, restringiria o direito à desindexação para apenas uma parcela dos usuários e diminuindo o âmbito de sua aplicação.

---

[294] Para se aprofundar sobre a questão, sugere-se a leitura da tese de livre docência da Cintia Rosa Pereira de Lima que trata, além de diversos pontos, com cuidado das diferenças do modelo norte-americano dos demais modelos de proteção de dados pessoais. LIMA, Cíntia Rosa Pereira de. *A imprescindibilidade de uma entidade de garantia para a efetiva proteção de dados pessoais no cenário futuro do Brasil*. Tese de Livre Docência apresentada à Faculdade de Direito de Ribeirão Preto. Ribeirão Preto: USP, 2015, p. 181.

[295] Nesse sentido, o advogado especialista em proteção de dados pessoais conclui: "O direito da UE de ser esquecido fornece uma base para o fortalecimento dos direitos de privacidade nos Estados Unidos. Além disso, pode fornecer uma base para o tratamento de mecanismos de pesquisa como CRAs. Pesquisadores de fatos razoáveis nos Estados Unidos têm uma base sólida para expandir o conceito tradicional de CRAs para incluir mecanismos de pesquisa devido à amplitude de informações pessoalmente identificáveis que podem existir e serem vinculadas a indivíduos por mecanismos de pesquisa globais. Tanto a UE como os Estados Unidos devem começar a reanalisar alguns dos conceitos básicos de relatórios de crédito para permitir uma estrutura mais completa que utilize tanto leis de privacidade fortes quanto leis de proteção ao consumidor. Para os Estados Unidos, isso significa fortalecer o direito individual à privacidade inerente ao propósito da FCRA. Na UE, isso significa desenvolver leis fortes de proteção ao consumidor, semelhantes às da FCRA. Ao fazer isso, ambas as jurisdições podem aprender umas com as outras e evitar os efeitos negativos que surgem da miopia jurisprudencial". (tradução livre) . Segue trecho original: "*The EU's right to be forgotten provides a basis for strengthening rights of privacy in the United States. In addition, it may provide a basis for treating search engines as CRAs. Reasonable fact finders in the United States have a strong basis to expand the traditional concept of CRAs to include search engines due to the breadth of personally identifiable information that may exist and be linked to individuals by global search engines. Both the EU and the United States should begin to reanalyze some of the basic concepts of credit reporting to allow for a more complete framework that utilizes both strong privacy laws as well as consumer protection laws. For the United States, this means strengthening individual's right to privacy inherent within the purpose of the FCRA. In the EU, this means developing strong consumer protection laws akin to the FCRA. By doing so, both jurisdictions may learn from each other and avoid the negative effects that arise from jurisprudential myopia*". ANDRUS, Mark T. The Right to be Forgotten in America: Have Search Engines Inadvertently Become Consumer Reporting Agencies?. Disponível em: https://www.americanbar.org/publications/blt/2016/05/05_andrus.html. Acesso em: 06.10.2017.

[296] MALDONADO, Viviane Nóbrega. *Direito ao esquecimento.* Barueri: Novo Século Editora, 2017, p. 132.

No Brasil, o Superior Tribunal de Justiça tem adotado o entendimento de que os motores de busca como provedores de aplicação não devem remover os resultados de pesquisa da lista. É o que o que compreende a 3ª Turma do Superior Tribunal de Justiça que, no julgamento do REsp 1.593.873[297], posicionou-se que o pedido de direito ao esquecimento, isto é, à desindexação, não pode ser direcionado ao Google, pois os provedores de busca não podem ser obrigados a eliminar de seu sistema os resultados de determinado termo, expressão, foto ou texto específico, por ausência de fundamento normativo, exceto no caso de encaminhamento do próprio provedor ao conteúdo de fotografias ou notícias.

Não se pode coadunar com esse entendimento, já que os motores de busca realizam atividade de tratamento de dados, no sentido de coleta, processamento, utilização e armazenamento, ao passo que os dados pessoais como prolongamentos da própria pessoa merecem ser tutelados. Até porque, decidir pela não desindexação contraria inclusive a garantia do consentimento do titular.

[297] Segue ementa do caso: PROCESSUAL CIVIL E CIVIL. RECURSO ESPECIAL. AÇÃO DE OBRIGAÇÃO DE FAZER. PROVEDOR DE PESQUISA. DIREITO AO ESQUECIMENTO. FILTRAGEM PRÉVIA DAS BUSCAS. BLOQUEIO DE PALAVRAS-CHAVES. IMPOSSIBILIDADE. - Direito ao esquecimento como "o direito de não ser lembrado contra sua vontade, especificamente no tocante a fatos desabonadores, de natureza criminal, nos quais se envolveu, mas que, posteriormente, fora inocentado". Precedentes. - Os provedores de pesquisa não podem ser obrigados a eliminar do seu sistema os resultados derivados da busca de determinado termo ou expressão, tampouco os resultados que apontem para uma foto ou texto específico, independentemente da indicação da página onde este estiver inserido. - Ausência de fundamento normativo para imputar aos provedores de aplicação de buscas na internet a obrigação de implementar o direito ao esquecimento e, assim, exercer função de censor digital. - Recurso especial provido. (STJ, 3ª Turma, REsp. 1.593.873, relatora ministra Nancy Andrighi. Julgado em: 11/12/2014.)

CAPÍTULO VI – A DESVINCULAÇÃO DE DADOS PESSOAIS

6.1. O que é o mecanismo do "*Dynamic query suggestion*"?

O "*Dynamic query suggestion"* é o mecanismo criado para que o próprio motor de busca faça uma "auto-sugestão" ou então complete os termos que o usuário pretende escrever na ferramenta para realizar a sua pesquisa. É uma técnica dinâmica que mostra a sugestão ao mesmo tempo em que o usuário está digitando na página. Se não bastasse, essa sugestão efetuada pelo próprio mecanismo de busca, poderá inclusive se basear no histórico de consultas do usuário. [298]

Essa sugestão feita pelo próprio motor de busca poderá, no entanto, vincular o nome da pessoa, isto é, um dado pessoal com uma expressão vexatória e ilícita que não se relaciona com a pessoa. Até porque, nesse caso, poderá acontecer da sugestão indicar uma expressão que não consta nenhum resultado na lista indexada pela ferramenta.

Como exemplo, temos o caso de uma liminar deferida pelo Tribunal de Justiça de São Paulo que determinou que a Google deixe de associar os termos "Templo de Salomão" e "Anticristo" para levar os usuários nos resultados da localização de uma igreja no aplicativo "Google Maps" que também conta com mecanismo de pesquisa[299], o que causa dano a honra objetiva da igreja.

Nesse contexto, a associação indevida poderá infringir outros direitos da personalidade, além da proteção dos dados pessoais, como honra, imagem, nome e identidade pessoal. Caberá deixar para as normas técnicas e os cientistas da computação analisar se essa espécie de associação se traduz em uma falha no sistema impulsionada por usuários que tentam manipular os algoritmos do motor de busca.

[298] YATES, Ricardi Baeza. NETO, Berthier Ribeito. *Modern Information Retrieval: the concepts and technology behind search*. 2 ed. New York: Addison-Wesley Publishing Company, 2011, p. 28/29.
[299] *Justiça obriga Google a desassociar "anticristo" do "templo de Salomão".* Disponível em: http://sao-paulo.estadao.com.br/noticias/geral,justica-obriga-google-a-desassociar-anticristo-do-templo-de-salomao,10000071676. Acesso em: 10.01.2018.

6.2. O fenômeno do "*Google bomb*"

O *Google bomb* é um fenômeno caracterizado pelas tentativas de influenciar a classificação de uma determinada página ou site nos resultados retornados pelo Google. Em outras palavras, usuários mal intencionados seja por razões políticas ou humorísticas tentam modificar a seleção do algoritmo *PageRank* das páginas da Web, arquivos e vídeos[300].

O *Spamdexing* seria o responsável pela prática de fazer modificações no código fonte e, assim, iludir o *robot* ou *Crawler*.. Tal fenômeno pode ocorrer de duas maneiras: a primeira seria dar maior visibilidade a uma determinada página, colocando-a em melhores posições no índice de resultados e a segunda seria para influenciar a categoria ou critério ao qual a página foi designada.

A grande problemática do *Google Bomb* é a vinculação indevida do nome ou dados de certas pessoas à expressões inverídicas ou vexatórias. Como por exemplo, o caso da cantora brasileira Preta Gil, no qual qualquer pessoa que digitasse a expressão "atriz gorda" o Google sugeria "experimente também: Preta Gil". Indignada com o acontecimento, a cantora concedeu entrevista a um site e disse: "Vindo do Google, que hoje é o manual de todo mundo, é algo deplorável.". [301]Além disso, noticiou que iria processar o motor de busca.

No caso em questão, não havia um website para desindexar a pesquisa do índice, mas tão somente era necessário desvincular o nome da pessoa com uma representação preconceituosa. A cantora sentiu-se ofendida com o ocorrido.

Nessa seara, a arquitetura da rede[302], isto é, o código fonte, pode ser revisto pelos especialistas a fim de que esse fenômeno de influência dos resultados dos termos de busca não ocorra, bem como inviabilize a vinculação indevida do nome da pessoa com termos pejorativos, caracterizando uma verdadeira ofensa à pessoa humana e seus dados pessoais.

---

[300] Definição de "Google bomb". Disponível em: https://pt.wikipedia.org/wiki/Bomba_do_Google. Acesso em: 12.07.2016.

[301]Conforme a notícia "*Busca Coloca Preta Gil contra o Google*", reportagem publicada em 15.02.2008. Disponível em: http://g1.globo.com/Noticias/Tecnologia/0,,MUL300855-6174,00-BUSCA+COLOCA+PRETA+GIL+CONTRA+O+GOOGLE.html. Acesso em: 12.07.2016.

[302] LESSIG, Lawrence. *Code and other laws of cyberspace, version 2.0*. Nova York: Basic Books, 2006.

6.3. A desvinculação de dados pessoais como exercício da proteção de dados pessoais e do direito à identidade pessoal

A desvinculação de dados pessoais pode ser notada no caso da apresentadora Xuxa Meneghel e a empresa Google Brasil, julgado no Recurso Especial nº 1316921/RJ. A apresentadora pleiteava que os resultados de pesquisa não vinculassem a expressão "xuxa" com a palavra "pedófila", ou, "ainda, qualquer outra que associe o nome da autora, escrito parcial ou integralmente, e independentemente de grafia, se correta ou equivocada, a uma prática criminosa qualquer".

Em sede de pedido de tutela de urgência, magistrado de primeiro grau determinou que o Google se abstivesse de disponibilizar aos usuários do seu motor de busca links ou resultados que associassem os termos "Xuxa", "pedófila", "Xuxa Meneghel", "ou qualquer grafia que se assemelhe a estas, isolada ou conjuntamente, com ou sem aspas", sob pena de multa de R$20.000,00, por cada resultado disponibilizado indevidamente ao usuário.

Interposto agravo de instrumento perante o Tribunal de Justiça do Rio de Janeiro, este restringiu parcialmente a decisão liminar para que se desvinculasse apenas as imagens expressamente citadas na exordial, e sem desindexar os resultados de pesquisa.

Em sede de recurso especial interposto pelo Google, que se delimitou a considerar a questão da responsabilidade civil dos motores de busca pelo conteúdo dos resultados que apresenta.

A 3ª Turma do STJ, de forma unânime, acompanhando o voto da Ministra Relatora Nancy Andrighi, deu provimento ao recurso para cassar a antecipação de tutela deferida, por falta de interesse de agir da apresentadora Xuxa contra o Google. Para tanto, consagrou-se o entendimento de que os provedores de aplicação como as ferramentas de busca que "não incluem, hospedam, organizam ou de qualquer outra forma gerenciam as páginas virtuais indicadas nos resultados", não devem ser responsabilizados pelo conteúdo de terceiros já que a sua atividade se limita a indicar os links ou páginas dos sites onde aquilo o que se pesquisa pode ser localizado.

Infelizmente, por todo um sistema protetivo de dados pessoais, pela lucratividade com a vigilância irrestrita do usuário, pela criação de verdadeiros perfis virtuais e pelo tratamento de dados em si, não há como se admitir que os motores de busca não sejam responsáveis pelo fluxo de informações que disponibiliza.

Vislumbra-se que mecanismos devem ser criados para impedir que associações ofensivas sejam feitas pela sugestão do próprio Google (associação de termos) ou indexações de conteúdos ilegais que não representam a pessoa, a sua identidade, deve ser removidos ou indisponibilizados pela internet. A associação de palavras entre “Xuxa” e “Pedofila”, cuja vinculação não representa e nunca representou a apresentadora, compreende-se a particular situação jurídica em que o direito de desvinculação merece guarida. Nesse particular, a desvinculação pode ser pleiteada em face do motor de busca com a finalidade de proteger os dados pessoais, a dignidade e o seu livre desenvolvimento.

CONCLUSÃO

A sociedade informacional viabiliza a comunicação mais rápida e a obtenção de dados pessoais, razão pela qual se discorreu ao seu respeito a fim de contextualizar no espaço e no tempo, o surgimento de novos direitos da personalidade, frente aos avanços tecnológicos.

O usuário da internet que costuma divulgar informações e aspectos de sua vida privada sem notar o alto grau de exposição e visibilidade que emprega no meio virtual pode vir a sofrer prejuízos presentes e futuros. Isso porque, o valor que seria extraído do dado é a própria pessoa, vigiada e monitorada pelos responsáveis pelo tratamento de dados pessoais e pelos usuários da rede.

O superinformacionismo leva a cada vez mais na obtenção de informações. E, com base nessas considerações, os motores de busca exercem um papel extremamente importante, pois facilitam o acesso às informações enquanto coletam dados pessoais.

Viu-se que o motor de busca mais famoso, o Google, rastreia os hábitos, comportamentos, opiniões e juízo de valor diariamente, sendo um filtro ou uma lente de contato pela qual se observa o mundo. Também, os motores de busca processam, selecionam, indexam e distribuem o conhecimento que determina o que se considera como bom, verdadeiro, relevante e de valor.

Nessa esteira, as novas tecnologias são capazes de invadir a esfera privada da pessoa, razão pela qual muito se debateu sobre o direito à privacidade e sua conceituação na contemporaneidade.

Entendeu-se que “as coisas da vida privada” merecem tutela no sentido de exclusão e controle da divulgação de informações pessoais que agridam o íntimo do ser ou aquilo que se almeje manter fora do domínio do público.

Considerou-se que a privacidade não precisa ser identificada como uma pluralidade de significados, um termo indeterminado ou como palavra-camaleão. É possível definir a sua essência através do método tradicional de linguagem e conceituação.

Compreendeu-se que a privacidade seria o poder da pessoa de abstenção contra interferências alheias (aspecto negativo) e o controle dinâmico de suas informações pessoais intimas ou privadas (aspecto positivo), ao passo que conjuga a feição clássica e contemporânea do direito à privacidade.

A internet promoveu uma maior interação entre as pessoas e a facilidade na divulgação de acontecimentos pessoais desabonadores ou não tais como a embriaguez, o uso de substâncias ilícitas, quais amores foram correspondidos, vídeos das pessoas dançando e cantando ainda enquanto crianças, fotos comprometedoras, entre outros. Se não bastasse, enfatizou a captação e o armazenamento de dados pessoais como nome, estado civil, filiação, raça, sexo, endereço, tipo sanguíneo e atividade profissional disponíveis em banco de dados. Apesar da relação que se possa identificar entre esses acontecimentos pessoais e os dados coletados do indivíduo, garante-se que a privacidade e a proteção aos dados pessoais são tutelas diferenciadas e cada qual com conteúdo próprio.

Por outro lado, a proteção aos dados pessoais não leva em consideração a esfera privada da pessoa, mas evidencia uma tutela dinâmica de controlar a circulação de dados que se inicia com a coleta e permanece até com a circulação e armazenamento, independentemente se esses dados estejam à disposição do público.

O direito à proteção aos dados pessoais pode ser conceituado como o direito de uma pessoa física ou jurídica, individualizada ou individualizável, de controlar seus dados pessoais, corrigi-los ou apagá-los nos termos da lei.

Nesse sentido, a massificação dos meios de comunicação leva à perpetuidade de informações e lembranças que podem vir a causar um estigma social, uma marca que acompanhará a pessoa por uma vida inteira, o que poderá gerar prejuízos e até a perda de uma chance. Em suma, a permanência da circulação de informações pessoais verídicas, porém descontextualizadas, poderá arruinar as possibilidades de um recomeço.

Diversas propostas de nomenclatura foram concretizadas para delimitar o direito ao esquecimento, tais como, na língua inglesa, o *right to be forgotten* (direito de ser esquecido), *right to forget* (direito de esquecer), *right to be let alone* (direito de ser deixado em paz), *right to erasure* (direito ao apagamento), *right to delete* (direito de apagar) e *right to delist* (direito de delistar). Diante do consagrado termo na jurisprudência, preferiu-se adotar a expressão de direito ao esquecimento.

Distinguiu-se que a expressão "direito ao esquecimento" que tem sido utilizada pelo menos em três acepções: i) uma tradicional; ii) a segunda no âmbito da internet; iii) a terceira criada com base no modelo de proteção dos dados pessoais europeu.

Vislumbrou-se que a primeira acepção relaciona-se com a seara das condenações criminais, do poder de ressocialização do individuo que cometeu um erro e se redimiu. Compreende-se nessa tradicional acepção, de maneira um pouco mais ampla, que o direito

ao esquecimento vincular-se-ia à questão subjetiva do ser humano em não ser relembrado de fatos que almeja esquecer por meio da republicação da informação legítima e verídica que se distanciou do debate público pelo transcurso do tempo.

Na segunda acepção compreendeu-se que o direito ao esquecimento não se trata apenas ou necessariamente de uma republicação da informação, mas da sua própria permanência na rede de internet.

Observou-se que da primeira acepção para a segunda há uma enorme diferença que é a potencialização da informação em manter-se, circular na rede. Assim, a republicação da informação em televisões, rádios e jornais costumeiramente acontece de forma momentânea e pontual enquanto na internet não é necessário que um ato de "republicação" seja realizado para que a informação ali permaneça.

A terceira acepção de direito ao esquecimento é aquela que se refere ao direito à proteção dos dados pessoais exercida pelo ato de apagar, cancelar e se opor ao tratamento de dados pessoais, nos termos do modelo de proteção europeu, especificamente, na Diretiva nº 95/46/CE e também no novo Regulamento Geral de Proteção de Dados Pessoais, do Parlamento e Conselho Europeu.

O que inspirou tal terceira acepção foi justamente o julgamento do Caso *Mario Costeja* em face do motor de busca *Google* em que se determinou, em maio de 2014, que os resultados de pesquisa fossem desindexados da lista de busca para minimizar a propagação do conteúdo da informação sem, contudo, removê-la de sua fonte original.

Ora, a terceira acepção não se trata de um direito ao esquecimento, mas do exercício do direito à proteção dos dados pessoais, evidenciado pelo cancelamento ou apagamento dos dados que foram considerados irrelevantes, inadequados e excessivos, conforme o princípio da qualidade dos dados e o princípio da finalidade.

O direito ao esquecimento trata de informações verdadeiras que, apesar da existência de um interesse público no passado, não mais assumem essa condição, causando consequências para a sua esfera privada e para si.

O conceito de direito ao esquecimento seria aquele em que apresenta uma faceta positiva (obrigação de fazer) quanto negativa (abstenção). Positiva, porque permite ao titular exercer a sua pretensão contra terceiros, exigindo que removam o conteúdo infringente deste direito seja nos meios de comunicação tradicionais ou na internet. Negativa, porque impõe que a esses terceiros se abstenham de processar, publicar, republicar e conservar tal informação pessoal.

Quanto ao seu fundamento, em síntese, aborda-se o entendimento de Massimiliano Mezzanotte[303] que configura o direito ao esquecimento como sendo uma "situação jurídica subjetiva com *corpus* de um direito à identidade pessoal; mas *animus* de direito à privacidade". O indivíduo que alega o direito ao esquecimento pretende resguardar determinado acontecimento de que tenha participado e, portanto, que este fato de sua vida privada seja resguardado ou, pelo menos, não perenizado, faceta da privacidade. Em contrapartida, a representação de si mesma pode ter se alterado com o tempo, já que o fato de ele ter cometido um erro no passado não quer dizer que ele irá reincidir no erro.

Como dito anteriormente, a proteção dos dados pessoais é autônoma e poderá auxiliar no exercício do direito ao esquecimento por meio da remoção do conteúdo de informações verídicas e constrangedoras que devem permanecer no passado. É nesse sentido que se consagra o direito à oposição como direito à desindexação de dados pessoais no caso do espanhol Mario Costeja em face dos motores de busca.

Na pretensão do citado espanhol não houve a supressão da informação na sua fonte originária, logo relacionou-se com a desindexação que, nada mais é que o direito de oposição, cancelamento e apagamento (remoção do link no motor). Por derradeira, a economia informacional, o valor que os dados pessoais possuem e os reflexos que sua manutenção podem acarretar, quando ainda distante da finalidade proposta, sendo dados desatualizados, irrelevantes e impertinentes, bem verdade que a obstrução do seu acesso é um aliado para o desenvolvimento da pessoa humana.

O "*Dynamic query suggestion"* é o mecanismo criado para que o próprio motor de busca faça uma "auto-sugestão" ou então complete os termos que o usuário pretende escrever no "retângulo" para realizar a sua pesquisa. Tal sugestão feita pelo próprio motor de busca poderá, no entanto, vincular o nome da pessoa, isto é, um dado pessoal com uma expressão vexatória e ilícita que não se relaciona com a pessoa. Até porque, nesse caso, poderá acontecer da sugestão indicar uma expressão que não consta em nenhum resultado na lista indexada pela ferramenta.

Analisou-se o caso da apresentadora Xuxa Meneghel em face da empresa Google Brasil, julgado no Recurso Especial nº 1316921/RJ para compreender o direito à desvinculação. Em suma, a apresentadora pleiteou que os resultados de pesquisa não vinculassem a expressão "xuxa" com a palavra "pedófila", ou, "ainda, qualquer outra que associe o nome da autora, escrito parcial ou integralmente, e independentemente de grafia,

[303] *Il diritto all'oblio:* contributo allo studio della privacy storica. Napoli: Edizioni Scientifiche Italiane, 2009. 81.

se correta ou equivocada, a uma prática criminosa qualquer", porém ainda não conseguiu pleito satisfatório.

Verificou-se que a não associação do nome com termo pejorativo como "pedofilia" guarda tutela no direito autônomo de proteção aos dados pessoais.

Logo, há a distinção de direito ao esquecimento e o direito à desvinculação, sendo que este não pressupõe a existência de informações passadas e irrelevantes para o seu exercício, bastando à atividade de associação entre dois termos nos motores de busca com o condão de causar sérios prejuízos para a pessoa e seu desenvolvimento humano.

Conclui-se, então, que o direito ao esquecimento, o direito à desindexação e o direito à desvinculação de dados pessoais não se confundem, porém a desindexação e a desvinculação podem auxiliar para que, após transcurso de tempo, as informações pessoais não se perenizem e as pessoas não sejam monitoradas eternamente por meio da Internet.

REFERENCIAS BIBLIOGRÁFICAS

ABRAMS, Martin. *The Marco Civil and Beyond: Privacy Governance for the Future*. In: ARTESE, Gustavo (coord.). *Marco Civil da Internet: análise jurídica sob uma perspectiva empresarial*. São Paulo: Quartier, 2015.

_____. *The Origins of Personal Data and its Implications For Governance*. The Information Accountability Foundation, 2014. Disponível em: <http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf>. Acessado em: 04.11.2017.

AMARAL, Francisco. *Direito civil.* Introdução. Rio de Janeiro: Renovar, 2008.

AMBROSE, Meg Leta. *You are What Google Says You Are: The Right to be Forgotten and Information Stewardship***.** Internacional Review of Information Ethics. Vol 17 (07/2012).

ANDRADE, Noberto Nuno Gomes de. *Oblivion: The Right to Be Different ... from Oneself Reproposing the Right to Be Forgotten*. *Revista de Internet, Direito e Política*. Universitat Oberta de Catalunya. February, 2012.

ANDRUS, Mark T. *The Right to be Forgotten in America: Have Search Engines Inadvertently Become Consumer Reporting Agencies?. Disponível em: https://www.americanbar.org/publications/blt/2016/05/05_andrus.html. Acessado em: 06.10.2017.*

ASCENÇÃO, José de Oliveira da. *A Sociedade da Informação*. In: *Direito da Sociedade da Informação*. V. 1. Coimbra: Coimbra Editora, 1999.

BAUMAN, Zygmunt. *Vigilância: diálogos com David Lyon*. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar Editores, 2013.

BARRETO JUNIOR, Irineu Francisco. *Atualidade do Conceito Sociedade da Informação para a Pesquisa Jurídica*. In: PAESANO, Liliana Minardi (coord.). Direito na Sociedade da Informação. São Paulo: Atlas, 2007.

BIONI, Bruno. *Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil*. Grupo de Estudos em Políticas Públicas em Acesso à Informação da USP – GPOPAI. 2015. Disponível em: http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf. Acesso em: 02.10.2017.

BITTAR, Carlos Alberto. Os direitos da personalidade. Rio de Janeiro: Forense Universitária, 1989.

BRANCO, Sérgio. *Memória e esquecimento na internet*. Porto Alegre: Editora: Arquipélago Editorial, 2017, p. 161.

BRASIL. Lei n 12.414/2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12414.htm. Acesso em: 02.10.2017.

BRASIL. Lei n 12.527/2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 02.10.2017.

BRASIL. Lei nº 8.078/1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8078.htm. Acesso em: 02.10.2017.

BRASIL. Decreto nº 8.771/2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm. Acesso em: 02.10.2017.

BRASIL. Lei nº 12.965/2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 02.10.2017.

BRASIL. Decreto nº 8.771/2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm. Acesso em: 02.10.2017.

BRASIL. Decreto-lei nº 2.848, de 07 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm. Acesso em: 01.06.2018.

CABRAL, Marcel Malizia. *A colisão entre os direitos de personalidade e o direito de informação*. In: RODRIGUES JUNIOR, Otavio; MIRANDA, Jorge; FRUET, Gustavo Bonato. Direitos da personalidade. São Paulo: Atlas, 2012.

CASTELLANO, Pere Simon**.** *El régimen constitucional del derecho al olvido en Internet. Neutralidad de la red y otros retos para el futuro de Internet. Actas del VII Congreso Internacional Internet, Derecho y Política Universitat Oberta de Catalunya***.** Barcelona: Huygens Editoral, 11-12 de julho de 2011. Disponível em: file:///C:/Users/user/Downloads/El_regimen_constitucional_del_derecho_al%20(1).pdf. Acesso em: 06.06.2016.

CASTELLS, Manuel. *A Era da Informação: economia, sociedade e cultura***.** V.1, a sociedade em rede. 8 ª ed. São Paulo: Paz e Terra, 2005.

_____. *A galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade.* Traduzido por Maria Luiza X. de A. Borges; revisão Paulo Vaz. Rio de Janeiro: Zahar, 2003.

CASTRO, Catarina Sarmento. *Direito da Informática, Privacidade e Dados Pessoais***.** Coimbra: Almedina, 2005.

CATE, Fred H. *The failure of Fair Information Practice Principles*. In: *Consumer Protection in the Age of the 'information economy' (Markets and the Law).* Hampshire: Ashgate Publish, 2006.

CHAVES, Antonio. *Lições de direito civil: parte geral* 3. São Paulo: Bushatsky – Edusp, 1972.

CHAVES, Reinaldo. *Direito ao esquecimento – Em um dia, Google recebe 12 mil pedidos para apagar informações*. Consultor Jurídico, 02/06/2014. Disponível em: http://www.conjur.com.br/2014-jun-02/dia-google-recebe-12-mil-pedidos-apagar-informacoes. Acesso em: 14/10/2014.

CHINELLATO, Silmara Juny de Abreu. *Pessoa Natural e novas tecnologias*. Aula magna na Faculdade de Direito da Universidade de São Paulo. *Revista do Instituto dos Advogados de São Paulo*. Ano 14. N. 27. Jan/ju/2011.

_____. Comentários à parte geral – artigos 1º a 21 do Código Civil. In: MACHADO, Antonio Cláudio da Costa. (Org.). CHINELLATO, Silmara Juny (Coord.). Código civil interpretado: artigo por artigo, parágrafo por parágrafo. 5. ed. Barueri: Manole, 2012

CÉDON, Beatriz Valadares. *Ferramentas de Busca da Web*. In: Revista C. Informática. Brasília, v. 30. n.1. Jan./Abr. 2001, p. 39-49. Disponível em: http://www.scielo.br/pdf/ci/v30n1/a06v30n1. Acesso em: 25.05.2016.

CONSALTER, Zilda Mara. *Para além do rio lete: o direito ao esquecimento como aporte teórico para a proteção efetiva da intimidade na era virtual***.** Tese de doutorado apresentada no Programa de Pós Graduação da Faculdade de Direito da Universidade de São Paulo. Orientador Dr. Álvaro Villaça Azevedo. São Paulo, 2016.

COOLEY, Thomas McIntyre. *A Treatise on the law of torts*. Chicago: Callaghan, 1880.

COSTA, André Brandão Nery**.** *Direito ao esquecimento na Internet: a Scarlet Letter Digital*. In: SCHREIDER, Anderson (coord.). Direito e mídia. São Paulo: Atlas, 2013.

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

CUNHA, Renan Severo Teixeira da. *Introdução ao estudo do direito*. Campinas/SP: Editora Alínea, 2008.

CURIA. *An internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties*. Press Release nº 70/14. Luxembourg, 13 May 2014. Disponível em: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf. Acesso em: 14/10/2014.

DA SILVA, Roberto da Silva Baptista Dias. PASSOS, Ana Beatriz Guimarães. *Entre lembrança e olvido: uma análise das decisões do STJ sobre o direito ao esquecimento.* In: Revista Jurídica da Presidência. Vol. 16, nº 109, jun./set.. Brasília: 2014

DE LUCCA, Newton**.** *Direito de Arrependimento no Âmbito do Comércio Eletrônico*. In: MENDES, Gilmar F. (coord). *Direito, Inovação e Tecnologia*. São Paulo: Saraiva, 2015.

_____. *Aspectos jurídicos da contratação informática e telemática*. São Paulo: Saraiva, 2003.

DE SOUSA, Rabindranath V. A. Capelo, *O Direito Geral de Personalidade*. Coimbra: Coimbra Editora, 1995

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Renovar, 2006.

_____. *O Direito Fundamental à Proteção de Dados Pessoais*. In: MAGALHÃES, Guilherme (coord.). *Direito Privado e Internet*. São Paulo: Atlas, 2014.

DOTTI, René Ariel. *O direito ao esquecimento e a proteção do habeas data*. In: WAMBIER, Teresa Arruda Alvim (Coord.). *Habeas Data*. São Paulo: Revista dos Tribunais, 1998.

ESPANHA. Cosntitucion Española de 1978. Disponível em: http://www.congreso.es/docu/constituciones/1978/1978_cd.pdf. Acessado em: 31.11.2017.

ESPANHA. LOPD. Disponível em: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/2014/Ley_Organica_15-1999_de_13_de_diciembre_de_Proteccion_de_Datos_Consolidado.pdf. Acessado em: 12.12.2015

EUA. *Records, computers and the rights of citizens*. Report of the Secretary's Advisory Committee on Automated Personal Data Systems. U.S. Department of Health, Education & Welfare. Julho de 1973. Disponível em: <https://www.justice.gov/opcl/docs/rec-com-rights.pdf.> Acessado: 05.11/2017.

EUROPEAN COMMISSION. *A comprehensive approach on personal data protection in the European Union* (2010). Disponível em: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf. Acesso em: 19/10/2014.

EUROPEAN COMMISSION. *Proposal for Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data ando n the free movement of such data (General Data Protection Regulation)*, COM (2012), 11 final, 2012/0011 (COD), Brussels, 25-01-2012. Disponível em: http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf . Acesso em: 13/10/2014.

FRANÇA, Rubens Limongi. *Direitos da personalidade coordenadas fundamentais*. Revista do Advogado, São Paulo, n. 38, p. 5-13, dez. 1992.

FERREIRA, Aurélio Buarque de Holanda. *Dicionário Aurélio da Lingua Portuguesa.* 5 ed. Curitiba: Editora Positivo, 2010.

FINOCCHIARO, Giusella. *Il diritto all'oblio nel quaro dei diritti dela personalità*. In: *Il Diritto Dell'informazione e dell'informatica*. Rivista Promossa Dalla Fondazione Centro di Iniziativa Giuridica Piero Calamandrei. 2014

GALVÃO, Alexander Patêz. *A informação como commodity: mensurando o setor de informações em uma nova economia. Ciência da Informação*. V. 28, n. 1, Brasília: IBICT, 1999. Disponível em: http://revista.ibict.br/ciinf/article/view/861/895. Acesso em: 01.10.2017.

GARCIA, Enéas. *Responsabilidade civil dos meios de comunicação.* São Paulo: Juarez de Oliveira, 2002

GODOY, Claudio Luiz Bueno de. *A liberdade de imprensa e os direitos a personalidade*. São Paulo: Atlas, 2001.

HALBWACHS, Maurice. *La memoria colectiva.* Tradução de Inés Sancho-Arroyo. Zaragoza: Prensas Universitarias de Zaragoza, 2004.

HARDY, Quentin**.** *Impondo limites aos titãs da internet***.** *The New York Times*, 30 abr. 2012

HELF, Miguel. *Google Ads a Safeguard on Privacy for Searchers*, New York Times. Disponível em: http://www.nytimes.com/2007/03/15/technology/15googles.html?_r=0. Acesso em: 15/10/2017.

HIRATA, Alessandro. O Facebook e o direito à privacidade. *Revista de Informação Legislativa*, Brasília, v. 51, n. jan./mar. 2014.

HIRATA, Alessandro. O público e o privado no direito de intimidade perante os novos desafios do direito. In: DE LIMA, Cíntia Rosa Pereira de. NUNES, Lydia Neves Bastos Telles. *Estudos avançados de direito digital.* Rio de Janeiro: Elsevier, 2014.

HOLDENER, Antony. *Geolocation*. Sebastopol**:** O'Reilly Media, 2011.

HORAN, Eileen C.; AHEARN, Frank M. *How to disappear: Erase Your Digital Footprint, Leave False Trails, and Vanish Without a Trace*. Guilford Connecticut: Lyons Press. 2010.

HOUAISS, Antonio. VILLAR, Mauro de Salles. *Minidicionário da Língua Portuguesa*. Rio de Janiro: Objetiva, 2004.

JÄÄSKINEN, Nillo. *Parecer no caso Google Spain x Agencia Espanhola de protección de Dados.* Apresentado em 25 de junho de 2013 no Processo C – 131/12. Disponível em: https://www.conjur.com.br/dl/parecer-google-direito-esquecimento.pdf. Acessado em: 07.03.2016.

KANT, Immanuel. *Fundamentação da metafísica dos costumes e outros escritos*. Tradução de Leopoldo Holzbach. São Paulo: Martin Claret, 2004.

KLEE, Antonia Espíndola Longoni. MARTINS, Guilherme Magalhães Martins. A privacidade, a proteção dos dados e dos registros pessoais e a liberdade de expressão: algumas reflexões sobre o Marco Civil da Internet no Brasil (Lei nº 12.965/2014)**.** In: LUCCA, Newton de. FILHO, Adalberto Simão. LIMA, Cíntia Rosa Pereira de. (coords.) *Direito & Internet III – Tomo I: Marco Civil da internet (Lei º 12.965/2014)*. São Paulo: Quartier Latin, 2015.

LEONARDI, Marcel. *Tutela e Privacidade na Internet*. São Paulo: Saraiva, 2012.

LESSIG, Lawrence. *Code and other laws of cyberspace, version 2.0*. Nova York: Basic Books, 2006.

LÈVY, Pierre. *Collective Inteligence: mankind's emerging world in cyberspace*. Tradução de Robert Bononno. Cambridge (MA): Perseus Books, 1997.

LIMA. Cíntia Rosa Pereira de. *Direito ao Esquecimento e Internet: O Fundamento Legal no Direito Comunitário Europeu, no Direito Italiano e no Direito Brasileiro*. *Revista dos Tribunais*. n. 946. Ago/2014.

_____. *A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil.* Tese de Livre Docência apresentada junto à Faculdade de Direito de Ribeirão Preto. Ribeirão Preto: USP, 2015.

_____**.** O ônus de ler o contrato no contexto da "ditadura" dos contratos de adesão eletrônicos. In: *Direito e novas tecnologias*. Florianópolis: CONPEDI, 2014, p. 443-465. Disponivel em: http://publicadireito.com.br/artigos/?cod=981322808aba8a03. Acessado em: 01.10.2017.

_____. O conceito de tratamento de dados após o caso Google Spain e sua influência na sociedade brasileira**.** In: *III Encontro de Internacionalização do CONPEDI*. Madrid : Ediciones Laborum, 2015. V. 9., p. 120. Disponível também em: http://www.conpedi.org.br/wp-content/uploads/2016/03/Vol.-9-Madrid.pdf. Acesso em: 02.02.2016.

_____. *Parecer técnico encaminhado para a Comissão Especial destinada a proferir Parecer ao Projeto de Lei nº 4.060 de 2012, do Deputado Milton Monti, que dispõe sobre o tratamento de dados pessoais e dá outras providências*. Disponível em: http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/dra-cintia-rosa-pereira-de-lima-usp. Acesso em: 06.12. 2017.

_____. Direito ao Esquecimento e Internet: o fundamento legal no Direito Comunitário europeu, no Direito italiano e no Direito brasileiro. *In: Revista dos Tribunais,* ano 103, vol. 946, agosto de 2014, p. 77 – 109. _____; NUNES, Lydia Neves Bastos Telles (coords.). *Estudos avançados de direito digital*. Rio de Janeiro, Elsevier, 2014.

LIMBERGER, Têmis. Proteção dos dados pessoais e comércio eletrônico: os desafios do século XXI. *Revista de Direito do Consumidor*. São Paulo, ano 17, nº 65, p. 225, jul./set. 2008.

LISBOA, Roberto Senise. A inviolabilidade de correspondência na Internet. In: LUCCA, Newton De. SIMÃO FILHO, Adalberto. *Direito & Internet*. Aspectos Jurídicos Relevantes. Bauru, SP: EDIPRO, 2001.

LORENZETTI, Ricardo Luis. *Fundamentos do direito privado*. Tradução de Vera Maria Jacob Ferreira. São Paulo: Revista dos Tribunais, 1998.

MALDONADO, Viviane Nóbrega. *O direito ao esquecimento.* Barueri,SP: Novo Século Editora, 2017.

MANEY, Kelvin. *Tornando um mundo melhor*. New Jersey: IBM Press, 2011. Disponível em: <ftp://public.dhe.ibm.com/la/documents/imc/br/news/events/book_centennial/2011_09_14_0516_Tornando_O_Mundo_Melhor_PDF.pdf.>. Acessado em: 30.09.2017.

MARQUES, Garcia. LOURENÇO, Martins. *Direito da informática*. Coimbra: Almedina, 2000.

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

MARTINS, Leonardo. *Introdução à jurisprudência do Tribunal Constitucional Alemão*. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Organização e introdução: Leornado Martins. Trad. Beatriz Henning et al. Prefácio: Jan Woischnik. Montevidéu: Fundação Konrad Adenauer, 2005.

MAYER-SCHÖNBERGER, Viktor. *Delete: The Virtue of Forgetting in the Digital Age***.** New Jersey: Princeton University Press, 2009.

MAYER-SCHÖNBERGER, Viktor. CUKIER, Kenneth. *Big Data: a revolution that will transform how we live, work, and think.* Boston: Houghton Mifflin Harcourt Publishing Company, 2013.

MENDES, LAURA Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

_____. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo.* Faculdade de Direito. Universidade de Brasília, Brasília: 2008

MEZZANOTE, M.. *Il diritto all'oblio:* contributo allo studio della privacy storica. Napoli: Edizioni Scientifiche Italiane, 2009.

MORATO, Antonio Carlos. Dano à imagem. In: RODRIGUES JUNIOR, Otávio Luiz. et al. (coord.) *Responsabilidade civil contemporânea:* em homenagem a Silvio de Salvo Venosa. São Paulo, Atlas, 2011, p. 566.

MURRAY, Andrew. *Information tecnology law*. Oxford University Press, 2010.

OECD. *Exploring the Economics of Personal Data: a survey of methodologies for measuring monetary value*. In: The OECD Digital Economy Papers. (nº 220). Publicado em 02 de abril de 2013. Disponível em: <http://www.oecd-ilibrary.org/docserver/download/5k486qtxldmq-en.pdf?expires=1515318608&id=id&accname=guest&checksum=A1A7FF2A4D6C418E522518EBE4906E81>. Acessado em: 04.11.2017.

PAESANI, Liliana Minardi. *Direito e Internet – Liberdade de Informação, Privacidade e Responsabilidade.* 4ª ed. São Paulo: Atlas, 2008.

PARENTONI, Leonardo. O direito ao esquecimento (*right to oblivion*). In: DE LUCCA, Newton. (coord.). *Direito e Internet III*: Marco Civil da Internet (Lei n. 12.965/2014). Tomo I. São Paulo: Quartier Latin, 2015, p 546.

PARISIER, Eli. *The filter bubble*. New York: Penguin Books, 2011.

PARISER, Eli. *O filtro invisível: o que a internet está escondendo de você*. Tradução de Diego Alfaro. Rio de Janeiro: Zahar, 2011.

PINO, Giogio apud ANDRADE, Noberto Nuno Gomes de. *Oblivion: The Right to Be Different ... from Oneself Reproposing the Right to Be Forgotten*. Revista de Internet, Direito e Política. Universitat Oberta de Catalunya. February/2012.

PORTUGAL. Constituição da República Portuguesa de 1976. Disponível em: https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx. Acessado em: 31.11.2017.

RAMIRO, Livia Froner M.; DE LUCCA, Newton. *A tutela da privacidade e a proteção à identidade pessoal no espaço virtual.* V ENCONTRO INTERNACIONAL DO CONPEDI MONTEVIDÉU. Florianópolis: CONPEDI, 2016. Disponível em: https://www.conpedi.org.br/publicacoes/9105o6b2/v4u5j0t6/lZL7VI9LojzjW2o3.pdf. Acessao em: 12.12.2016.

RAMOS, Mário Hernandez. *El derecho al olvido em la web 2.0.* Salamanca: Universidad de Salamanca, 2013.

REINALDO FILHO, Demócrito. As "histórias patrocinadas do Facebook": os limites da utilização de dados pessoais no *marketing on-line*". *Revista Síntese Direito Empresarial*. São Paulo, ano 7, nº 38, p. 195, maio/jun. 2014.

REDING, Viviane. *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital* Age 5 (Jan. 22, 2012). Disponível em:http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF. Acesso em: 15.12.2017.

RICOEUR, Paul. *A memória, a história, o esquecimento.* Tradução de Alan François et. Al. Campinas: Editora UNICAMP, 2007, p. 510.

RODOTÀ, Stefano. *A vida na sociedade da Vigilância: a Privacidade Hoje*. Rio de Janeiro: Renovar, 2008.

_____. *Elaboratori elettronici e controllo sociale*. Bologna: II Mulino, 1973.

RULLI JÚNIOR, Antonio; RULLI NETO, Antônio. Direito ao esquecimento e o superinfornacionismo: apontamentos no direito brasileiro dentro do contexto da sociedade da informação. *Revista Instituto do Direito Brasileiro*. Ano 1.. n.1. 2012.

RÚSSIA. *Constituição da Rússia de 1993***.** Disponível em: <http://www.constitution.ru/en/10003000-01.htm>. Acessado em: 31.11.2017.

SARLET, Ingo Wolfgang. *Dignidade da pessoa humana e Direito Fundamentais na Constituição Federal de 1988.* 5ª ed. Porto Alegre: Livraria do Advogado, 2007.

SAMPAIO, José Adércio Leite. *Direito à intimidade e à vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte.* Belo Horizonte: Del Rey, 1998

SANTOS, Manoel J. Pereira dos. Princípios para Formação de um Regime de Dados Pessoais. In: LUCCA, Newton de. (coord.); SIMÃO FILHO, Adalberto (coord). Direito e Internet – Aspectos Jurídicos Relevantes. Vol II. São Paulo: Quartier Latin do Brasil, 2008.

SCHMIDT, Eric. ROSENBERG, Jonathan. EAGLE, Alan. *Como o Google funciona*. Trad. André Gordirro. Rio de Janeiro: Intrinseca, 2015.

SCHREIBER, Anderson. *Direitos da Personalidade.* 3 ed. São Paulo: Atlas, 2014

_____. Marco Civil da Internet: Avanço ou Retrocesso? A responsabilidade Civil por Dano Derivado do Conteúdo Gerado por Terceiro. In: DE LUCCA, Newton. (coord.). *Direito e Internet III: Marco Civil da Internet (Lei n. 12.965/2014)***.** Tomo II. São Paulo: Quartier Latin, 2015

SOLOVE, Daniel J. *Understanding Privacy*. Cambridge, Massachusetts: Harvard University Press, 2009.

_____. *Conceptualizing Privacy*. California Law Review. vol. 90.

SOUSA, Rabindranath Valentino Aleixo Capelo**.** *O direito geral da personalidade*. Coimbra: Coimbra, 1995.

STAIR, Ralph M. *Princípios de Sistemas de Informação: uma abordagem gerencial.* Trad. Maria Lúcia Iecker Vieria e Dalton Conde de Alencar. 2 ed. Rio de janeiro: LTC Editora, 1998.

SZANIAWSKI, Elimar. *Direitos da Personalidade e sua Tutela*. São Paulo: Revista dos Tribunais , 1993.

UNIÃO EUROPÉIA. *Convenção de Estrasburgo para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais***.** 1981. Disponível em: https://rm.coe.int/1680078b37. Acessado em: 02.11.2017.

UNIÃO EUROPÉIA. *Charter of Fundamental Rights of the European Union*. 2000. Disponível em: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12016P/TXT. Acesso em: 03.112017.

UNIÃO EUROPÉIA. *General Data Protection Regulation***.** Disponivel em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 04.11.2017.

UNIÃO EUROPEIA. *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*. Disponível em: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52012PC0010. Acesso em: 04.11.2017.

TEPEDINO, Gustavo. Cidadania e os direitos da personalidade. In: Revista da Escola Superior da Magistratura de Sergipe. Aracaju, n. 3, 2002.

TOMACEVICIUS FILHO, Eduardo. Em direção a um novo 1984? A tutela da vida privada entre a invasão da privacidade e a privacidade renunciada. Revista da Faculdade de Direito da Universidade de São Paulo, vol. 109, p. 129-169, jan./dez. 2014.

VAIDHYANATHAN, Siva. *The Glooglization of everything (and why we should worry).* Los Angeles: University of California Press, 2011.

XANTHOULIS, Napoleon. Conceptualising a Right to Oblvion in the Digital World: a human rights-based approach. *University College London Research Papers*. p. 01-38, maio/2012

WALD, Arnoldo. *Curso de direito civil brasileiro: introdução e parte geral*. 7. Ed. São Paulo: Ed. Revista dos Tribunais, 1992.

WARREN, Samuel D. BRANDEIS, Louis D. The right to privacy. In: *Harvard Law Review*. Cambridge: Harvard University Press, v.4, n. 5, p. 193-220, Dec.1890.

WEINRICH, Harald. *Lete:* arte e crítica do esquecimento. Tradução de Lya Luft. Rio de Janeiro: Civilização Brasileira, 2001.

WESTIN, Alan. *Privacy and Freedom*. Nova York: Atheneum, 1967, p. 7.
GIACOMO, Claudio de. *Diritto, libertà e privacy nel mondo dela comunicazione globale*. Milano: Giuffrè, 1999.

YATES, Ricardi Baeza. NETO, Berthier Ribeito. *Modern Information Retrieval: the concepts and technology behind search*. 2 ed. New York: Addison-Wesley Publishing Company, 2011.

ZECHMAN, Ashley. *So long, Farewell, Auf Wiedersehen* Yahoo Directory. Disponível em: https://searchenginewatch.com/sew/news/2373344/so-long-farewell-auf-wiedersehen-yahoo-directory. Acesso em: 08.06.2016.