CAROLINE NARVAEZ LEITE

OS DESAFIOS DO ANONIMATO NO CONTEXTO DE TRATAMENTO AUTOMATIZADO DE DADOS PESSOAIS NA INTERNET

Dissertação de Mestrado
Orientadora: Profa. Associada Dra. Cíntia Rosa Pereira de Lima

UNIVERSIDADE DE SÃO PAULO
FACULDADE DE DIREITO
São Paulo
2018

CAROLINE NARVAEZ LEITE

OS DESAFIOS DO ANONIMATO NO CONTEXTO DE TRATAMENTO AUTOMATIZADO DE DADOS PESSOAIS 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 para obtenção do título de Mestre em Direito, na área de concentração Direito Civil, sob a orientação da Profa. Dra. Cíntia Rosa Pereira de Lima.

UNIVERSIDADE DE SÃO PAULO
FACULDADE DE DIREITO
São Paulo
2018

Catalogação da Publicação
Serviço de Biblioteca e Documentação
Faculdade de Direito da Universidade de São Paulo

Leite, Caroline Narvaez
Os desafios do anonimato no contexto de tratamento automatizado de dados pessoais na internet / Caroline Narvaez Leite ; orientadora Cíntia Rosa Pereira de Lima -- São Paulo, 2018.

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

1. Direito Civil. 2. Sociedade informacional. 3. Tratamento automatizado. 4. Dados pessoais. 5. Anonimato. I. Lima, Cíntia Rosa Pereira de, orient. II. Título.

BANCA EXAMINADORA

_____
_____
_____
_____

Dedico este trabalho aos meus pais,
por tudo o que me proporcionaram na vida.

AGRADECIMENTOS

À minha orientadora, Cíntia Rosa Pereira de Lima, por toda a sua dedicação, bem como pela confiança e gentileza, que, reunidos ao profundo conhecimento do Direito, fundam exemplos a serem seguidos por qualquer docente.

Ao meu pai, Mário Sérgio Leite, grande jurista e a pessoa com quem mais me identifico no universo, que sempre me deu apoio e palavras de força nos momentos necessários.

À minha mãe, Mônica Narvaez, por todo amor e tranquilidade durante a tormenta e pelas palavras de amor que me fizeram acreditar em mim mesma e sonhar mais alto.

Ao meu irmão, Henrique Narvaez Leite, pelas risadas, parceria, amizade, leveza e o maior amor que eu senti na vida.

Aos meus amigos Wévertton Flumignan, Daphne Noronha e Lívia Froner pelas inúmeras discussões jurídicas, por todos os momentos de apoio emocional, pelo desprendimento e pela amizade.

Ao amigo MM. Juiz Dr. Ricardo Felício Scaff pela confiança depositada e generosidade quando precisei dela.

HARD WIRED (TRACY CHAPMAN)

Your wants desires
Needs and wishes
Will be duly noted
Processed filed and cataloged
Labeled and encoded
Turned into sitcom dialog
And advertising slogans
(…)

RESUMO

LEITE, Caroline Narvaez. *Os desafios do anonimato no contexto de tratamento automatizado de dados pessoais na internet*, 2018, 183 p. Mestrado - Faculdade de Direito, Universidade de São Paulo, SP, 2018.

O presente trabalho se propõe a analisar o conteúdo dos dados pessoais, sua proteção no direito brasileiro e a fragilidade do conceito de anonimato no contexto da internet. Serão estudados os conceitos de dados pessoais, privacidade, sociedade informacional, além de uma análise das propostas contidas nos projetos de lei de proteção de dados pessoais, dentre outros. Pretende-se demonstrar de que forma os dados pessoais são capturados e tratados para posterior comercialização e uso, e as implicações jurídicas destas atividades, com foco especial na dificuldade do anonimato na internet.

PALAVRAS-CHAVE: Sociedade informacional; Internet; Dados Pessoais; Anonimato

ABSTRACT

LEITE, Caroline Narvaez. *The challenges of anonymity in the context of automated processing of personal data on the internet*, 2018, 183 p. Degree (Master)- Faculty of Law, University of São Paulo, São Paulo, SP, 2018.

This study intends to analyze the content of personal data, its protection under the Brazilian law and the fragility of anonymity on the internet. The concepts of personal data, privacy, information society will be analyzed, as well as the proposed draft bills within the Brazilian Congress regarding of personal data protection, among other themes. It intends to demonstrate how personal data are captured and processed for further marketing and use, with special focus on the difficulty of anonymity on the internet.

KEYWORDS: Informational Society; Internet; Personal Data; Anonymity

SUMÁRIO

INTRODUÇÃO

Como consequência da expansão na utilização da internet,[1] pode-se afirmar que a circulação de informações por meio desta — cada vez mais célere e intensa — tornou-se imprescindível para a vida do homem contemporâneo e para as suas inter-relações diuturnas. Um exemplo muito significativo é forma como a circulação de informações alterou as relações mercantis. Neste sentido, como ensina Cíntia Rosa Pereira de Lima, o comércio eletrônico é caracterizado pela contratação não presencial, utilizando os contratantes de diversos mecanismos e permitindo a disponibilização dos produtos a um número maior de pessoas.[2]

O advento e a evolução da tecnologia digital e das telecomunicações dinamizaram as relações comerciais e sociais em ambientes estruturados por tais tecnologias. O ingresso do indivíduo no ambiente digital, com o objetivo de iniciar as referidas relações, quase sempre implica na produção e coleta de dados pessoais.

O direito não ficou (e nem poderia ficar) alheio à expansão da internet e suas consequências. Tal situação é explicada por Mario Losano:

---

[1] Inicialmente cumpre esclarecer que será utilizada a palavra internet grafada com "i" minúsculo, pois se trata de substantivo comum feminino e, nos termos do padrão da língua portuguesa, assim deve ser grafado. É oportuno recordar que internet é a contração de *interconnected network,* expressão que pode ser usada para se referir a redes de computadores privadas interligadas, conforme ensina Lydia Parziale (PARZIALE, Lydia. *Tutorial and Technical Overview*, 8a edição. Armonk, Nova York, EUA: International Business Machines Corporation, 2006, p. 4). Da mesma forma, tal grafia foi adotada por Newton De Lucca. Conforme explica no prefácio da obra de Marcel Leonardi, deverá ser tratada como o nome genérico que é (como telefone, rádio ou televisão), já que não se trata de uma marca registrada; veja-se: "Não obstante tão respeitáveis considerações, porém, tenho me utilizado da palavra com "i" minúsculo — primeiramente em aspectos jurídicos da contratação informática e telemática e, posteriormente, no já citado artigo inaugural da obra coletiva Direito & Internet – Aspectos Jurídicos Revelantes — fundado nas razões tão bem expostas pelo Professor Le Tourneau, citado por Christiane Féral-Schuhl, na obra Cyber Droit – le droit à l'épreuve de l'internet, in verbis: *'Faut-il rappeler, avant de commencer, que le mot 'internet' n'est pas une marque, mais un nom générique qui, comme tel, doit recevoir un article (l'internet) et point de majuscule, exactement comme le téléphone, le mimitel, la radio, le telex ou la télévision*'"

[2] LIMA, Cíntia Rosa Pereira de. *Contratos de adesão eletrônicos (shrink-wrap e click-wrap) e os termos de condições de uso (browse-wrap)*. *In:* LIMA, Cíntia Rosa Pereira de; NUNES, Lydia Neves Bastos Telles (coords.). Estudos avançados de direito digital. Rio de Janeiro: Elsevier, 2014, pp. 105-133, p. 106.

> A informática jurídica estuda a aplicação dos computadores eletrônicos ao direito, unida aos pressupostos e consequências desta aplicação. A história real de tal disciplina está rigorosamente conexa à evolução tecnológica da informática e, portanto, a informática jurídica inicia com a difusão dos computadores eletrônicos na sociedade civil após a segunda guerra mundial. Convencionou-se fazer coincidir sua origem com a obra do estadunidense Lee Loevinger (1949). Dos EUA, a disciplina chega à Europa por volta da metade dos anos 60: como símbolo desta passagem pode-se tomar o Congresso Mundial de Juízes, realizado em Genebra, de 9 a 15 de julho de 1967, preparado com a difusão do breve texto Law Research by Computer, de agosto de 1966[3].

Nessa intersecção entre o direito e a internet é onde se encaixa o tema do trabalho, especialmente no tratamento automatizado dos dados pessoais.

Pode-se dizer que a internet é uma realidade constante na vida cotidiana sem a qual é quase impossível idealizar e materializar as relações humanas. Para se ter um parâmetro quantitativo da presença da internet, estima-se que atualmente existam cerca de 3,5 bilhões[4] de pessoas no planeta com acesso à rede mundial, sendo que a projeção para o futuro segue crescendo.

Na internet circulam ideias, manifestações de pensamentos, e dados e informações de cunho pessoal. Assim, sem prejuízo dos inegáveis benefícios da internet, este instrumento pode ser meio para o cometimento de graves violações aos direitos individuais, convidando o mundo jurídico, com urgência, a se preparar para coibir abusos decorrentes do mau uso dessa ferramenta.

No contexto em que estão inseridos, os indivíduos são altamente "vigiados" por meio da internet por diversas empresas que

---

[3] LOSANO, Mario. *A Informática Jurídica Vinte Anos Depois*, RT v. 715, fascículo I- Cível, maio de 1995, p. 350.

[4] De acordo com o site Internet World Stats <http://www.internetworldstats.com/stats.htm> pesquisa realizada em 7.jun.2016.

trabalham com captação de dados pessoais para uso preponderantemente comercial. Essas empresas se utilizam de dispositivos que permitem o permanente monitoramento do comportamento e preferências dos usuários, de forma individual ou coletiva. Portanto, como mencionado, especialmente no que diz respeito ao tratamento automatizado de dados pessoais, a internet como um ambiente de coleta de dados traz um grande risco para os direitos dos indivíduos.

O Marco Civil da Internet (Lei 12.965/2014) veio para corroborar e reforçar a necessidade de proteção dos dados pessoais dos indivíduos utilizados durante o acesso à internet, conforme se verá. A obtenção e o tratamento de informações diversas vezes são realizados sem que os usuários sequer tenham consciência, apesar de existir uma relação contratual de adesão. Com a nova lei, a tendência é de que haja maior proteção aos dados pessoais.

As questões envolvendo compartilhamento inadvertido de informações não suscitam questionamentos apenas no Brasil. O jornal norte-americano *The Wall Street Journal* publicou uma série de artigos a respeito do monitoramento dos usuários pelos 50 websites mais visitados dos Estados Unidos[5]. De acordo com as reportagens, os sites visitados instalaram, no total, 3180 dispositivos de rastreamento – os chamados *cookies*.

É por meio desses dispositivos de rastreamento, arquivos temporários armazenados na memória do computador quando o usuário visita determinadas páginas da web, que companhias especializadas monitoram quais as atividades *online* dos usuários (o que visitam e até mesmo o que digitam).

Depois de captadas as informações por meio por meio dos *cookies,* as empresas traçam perfis dos usuários, que são posteriormente vendidos para fins de propaganda direcionada. Tais empresas garantem que esses perfis não contêm os nomes dos indivíduos, apenas que são divididos por classes, como, por exemplo, idade, sexo, onde vivem.

---

[5] THE WALL STREET JOURNAL, Série de reportagens "What They Know" ou "O que eles sabem" em tradução livre Disponível em <http://online.wsj.com/public/page/what-they-know-digital-privacy.html> Acesso em 3.out.2014.

Essas atividades, segundo as reportagens, geram corrida competitiva pela obtenção de dados pessoais no meio digital. Com isso, fica claro também que a tendência é de crescimento nessa área de obtenção de dados, bem como que existe uma tendência para que os programas de monitoramento sejam cada vez mais sofisticados e agressivos, o que pode dar azo à um crescimento de violações ao direito à proteção de dados.

Tal aquisição e compilação de dados dos usuários da internet apresenta violação ao direito à proteção de dados em alguns casos. Há de se questionar: qual a destinação dos dados coletados? Depois de adquiridos os dados, os usuários não têm como saber o que realmente será feito com as informações coletadas. Também não lhes é conferida a possibilidade de não se sujeitarem a este tipo de coleta de dados.

Em uma declaração, o *chief executive officer* (CEO) da Google, Eric Schmidt, disse que o futuro da Google não é pesquisa, mas sim customização do conteúdo, veja-se:

> O Google pretende usar toda essa informação que está recolhendo sobre a gente há anos para definir nosso perfil e, a partir daí, tentar vender produtos, tentar customizar a nossa vida de uma forma que a gente não sabe muito bem ainda qual é[6].

Atualmente, está em trâmite o projeto de lei que estabelece princípios, garantias, direitos e obrigações referentes à proteção de dados pessoais, porém, o Brasil está atrasado na definição de tal legislação.

O assunto é debatido internacionalmente há mais de 40 anos. Já existem mais de 100 legislações específicas vigentes no mundo. A União Europeia, conforme se verá abaixo, foi pioneira no assunto, sendo seguida, na América Latina, por Argentina, Uruguai, Chile e Colômbia, que já criaram suas leis de proteção aos dados pessoais.

---

[6] Alessandra Pancetti. Privacidade na rede: questões de segurança e de direito. Site da *Organização dos Estados Ibero-Americanos.* <http://www.oei.es/divulgacioncientifica/reportajes127.htm> Acesso em 15.out.14.

Apesar de o Marco Civil da Internet ter regras relacionadas à proteção de dados, ainda há necessidade da existência de uma lei específica para o assunto, considerando a amplitude de implicações relacionadas. Além disso, o próprio Marco Civil da Internet faz referência à criação de uma lei para regulamentar o princípio da proteção de dados.

Após aprovada, a lei de proteção de dados pessoais deve criar práticas mais transparentes para os cidadãos, deixando claro para as empresas privadas e para a administração pública o que é permitido ser feito com os dados pessoais.

A ausência de legislação específica no Brasil para proteção de dados provoca insegurança jurídica para o cidadão e para o mercado de captação de dados, considerando a inespecificidade da legislação em vigor, nem sempre se consegue dar o tratamento adequado para o caso concreto que for submetido ao crivo do Poder Judiciário, que deverá se utilizar de conceitos e previsões legislativas nem sempre seguras e apropriadas.

Portanto, resumidamente, a importância do tema está associada à possibilidade de danos aos titulares dos dados pessoais e à incerteza jurídica que cerca o tema, sendo necessária uma incursão sobre os diversos tópicos e conceitos, jurídicos e extrajurídicos, de sorte a construir um sólido marco jurídico para o tema. Os tribunais brasileiros e de outros países têm se debruçado cada vez mais sobre questões referentes aos efeitos jurídicos da internet. Como consequência natural e necessária, os horizontes do direito se ampliam para que acompanhar a inexorável realidade do mundo virtual.

Como já brevemente dito, diante das imensas transformações vividas pelas últimas décadas, está-se diante de em uma sociedade que tem como base estrutural a produção e a circulação massificadas de informação por todos os membros da sociedade, aos quais se atribui o nome de “sociedade de informação” ou “sociedade informacional”, a depender do doutrinador.

Neste trabalho, será utilizada a expressão “sociedade informacional”, pois, conforme justificado por Manuel Castells (fazendo comparação entre indústria e industrial), o termo informacional indica qualidade de uma forma específica de

organização social, na qual fontes fundamentais de produtividade são a geração, o processamento e a transmissão da informação; veja-se:

> O termo sociedade da informação enfatiza o papel da informação na sociedade. Mas afirmo que informação, em seu sentido mais amplo, por exemplo, como comunicação de conhecimentos, foi crucial a todas as sociedades, inclusive à Europa medieval que era culturalmente estruturada e, até certo ponto, unificada pelo escolasticismo, ou seja, no geral uma infraestrutura intelectual (ver Southern, 1995). Ao contrário, o termo informacional indica o atributo de uma forma específica de organização social em que a geração, o processamento e a transmissão da informação tornam-se as fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico[7].

Nesse sentido, Cintia Rosa Pereira de Lima, ensina que, apesar de alguns autores utilizarem a expressão "sociedade do conhecimento" e "sociedade da informação", tais expressões não seriam adequadas, pois a primeira necessariamente implicaria em um estado de ignorância, o que não se aplica em todos os casos, e também porque o conhecimento depende de um preparo que nem sempre o indivíduo terá. Já "sociedade da informação" não parece ser adequada, pois *"seria uma sociedade que tem informação, o que se pode observar em todas as fases da evolução da humanidade*"[8]; veja-se:

> (...) a locução "sociedade informacional" destaca o papel da informação em determinada sociedade, isto é, a informação como riqueza

---

[7] CASTELLS, Manuel. *A Sociedade Em Rede* - Vol. I, 8ª ed. Trad. Roneide Venancio Majer. São Paulo: Paz e Terra, 2005, p. 65

[8] LIMA, Cíntia Rosa Pereira de. *A imprescindibilidade de uma entidade 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. Ribeirão Preto, 2015. p. 60.

> (economia informacional) e como instrumento de poder[9].

Castells explica que o caráter central do conhecimento e da informação na revolução tecnológica é a aplicação destes a aparatos de geração de conhecimento e processamento de informação.

> O que caracteriza a revolução tecnológica atual não é o caráter central do conhecimento e da informação, mas a aplicação deste conhecimento e informação a aparatos de geração de conhecimento e processamento da informação/comunicação, em um círculo de retroalimentação acumulativa entre a inovação e seus usos. [...] A difusão da tecnologia amplifica infinitamente seu poder ao se apropriar de seus usuários e redefini-los. As novas tecnologias da informação não são apenas ferramentas para se aplicar, mas processos para se desenvolver[10].

Na mesma obra (i.e. "A Sociedade Em Rede"), Manuel Castells afirma que uma nova economia — global e informacional — surgiu nas últimas décadas. A nova economia é informacional, porque a produtividade e a competitividade dependem da capacidade de gerar, processar e aplicar de forma eficiente a informação baseada em conhecimentos.

Da mesma forma, a nova economia é global porque as principais atividades produtivas, o consumo e a circulação, assim como seus componentes (capital, trabalho, matéria prima, administração, tecnologia e mercados) estão organizados em escala global, diretamente ou mediante uma rede de conexões entre agentes econômicos. A respeito do capitalismo informacional, Castells afirma:

> É, todavia, um tipo de capitalismo diferente daquele formado ao longo da História. É uma forma de capitalismo com objetivos mais

---

9 Idem. p. 61

[10] CASTELLS, Manuel. *A sociedade... Op. Cit.*. p. 66.

> firmes, porém com meios incomparavelmente mais flexíveis que qualquer um de seus predecessores. É o capitalismo informacional, que consta com a produtividade promovida pela inovação e a competitividade voltada para a globalização a fim de gerar riqueza e apropriá-la de forma seletiva. [...] inserido na cultura e equipado pela tecnologia, mas, desta vez, tanto a cultura como a tecnologia dependem de a capacidade de conhecimentos e informação agirem sobre uma rede recorrente de intercâmbios conectados em âmbito global[11].

No mesmo sentido, Cíntia Rosa Pereira de Lima ensina que, na economia informacional, a própria informação é o produto e a prestação de serviços, veja-se:

> Essa nova economia, a economia informacional, resultou da Revolução da Tecnologia da Informação. O conhecimento, a ciência e a tecnologia sempre foram importantes para qualquer tipo de economia, todavia esses eram utilizados para criar bens de consumo e prestar serviços. Em outras palavras, o resultado deste conhecimento e tecnologia era a base da sociedade industrial. Atualmente, a economia informacional destaca-se porque a própria informação é o produto e a prestação de serviços. A informação é um valor em si mesmo e não como um meio para criar bens e prestar serviços. Em 2004, o *Facebook* teve uma receita avaliada, inicialmente, em 400 mil dólares. Em 2014, suas receitas alcançaram a casa de 12.466 milhões de dólares. Por sua vez a Google, em 2001 teve uma receita de 86.426 milhões de dólares. Em 2015, as duas receitas alcançaram a casa de 66.001 bilhões de dólares. E essas empresas operam com dados e informações. Assim, os produtos das indústrias das novas tecnologias da informação são ferramentas de processamento de dados e da informação. Por isso, o adjetivo economia

[11] *Idem. p. 135.*

> informacional e sociedade informacional e não da informação[12].

Sob esse aspecto, ao se analisar as dimensões do direito à proteção de dados privados — seu conteúdo e limites, no contexto de "imediatidade" e liquidez das relações sociais, propiciados pelo advento de novos meios eletrônicos de armazenamento e transmissão de informações —, notar-se-á que o indivíduo não conta com proteção eficaz, considerando o atual conjunto legislativo.

A esse respeito, Cíntia Rosa Pereira de Lima, ensina que, apesar de as empresas que operam no *e-commerce*, tais como Amazon, E-Toys, Dell-Direct World, trazerem contribuição socioeconômica relevante (como criar empregos, gerar renda e acesso à informação), a monetização da informação traz riscos, principalmente no que se refere à proteção de dados pessoais:

> Em suma, esses novos *players* na economia informacional têm uma contribuição socioeconômica relevante, como, nos exemplos mais óbvios, criação de empregos, geração de rendas e acesso à informação. Todavia, a monetização da informação oferece riscos aos quais o Direito deve se atentar principalmente no que se refere à proteção de dados pessoais, a fim de que não seja prejudicada a efetiva tutela da dignidade da pessoa humana nos termos do art. 170, caput, da CF/88, dentre outros direitos fundamentais. Desta forma, deve-se buscar harmonizar os interesses financeiros e econômicos, relevantes para os particulares e a sociedade, e a tutela de direitos e garantias fundamentais[13].

Isso porque, no âmbito da internet, os responsáveis pela coleta de dados conseguem realizar cruzamentos de dados em diferentes fontes, a respeito de um único indivíduo – daí o conceito de *big data*. Tal situação permite a construção de perfis precisos de cada usuário (*profiling*).

---

[12] LIMA, Cíntia Rosa Pereira de. *A imprescindibilidade...Op. Cit.* p. 31-32.
[13] *Idem.* p. 37

Apesar de ser um termo com definições variadas e, por vezes, antagônicas, afirma-se que *big data* é *"um termo que descreve o armazenamento e análise de grandes e/ou conjuntos de dados complexos usando uma série de técnicas, incluindo, mas não limitado a: NoSQL, MapReduce e* machine learning*"*[14].

Um exemplo de ferramenta que se vale da tecnologia do *big data* é o *profiling*. Tal ferramenta, partindo das informações disponibilizadas pelos próprios indivíduos e com o auxílio de métodos estatísticos e inteligência artificial, trata os dados com o fim de obter uma "metainformação", conforme ensina Danilo Doneda:

> Esta técnica, conhecida como *profiling*, pode ser aplicada a indivíduos bem como estendida a grupos. Nela, os dados pessoais são tratados, com o auxílio de métodos estatísticos, técnicas de inteligência artificial e outras mais, com o fim de obter uma "metainformação", que consistiria numa síntese dos hábitos, preferências pessoais e outros registros da vida desta pessoa[15].

A preocupação que corre entre estudiosos do assunto diz respeito à ciência da parte dos usuários de que seus dados estejam sendo usados desta forma potencialmente lesiva dos seus direitos da personalidade, a despeito de consentimentos formais exarados em contratos de adesão assinados digitalmente. Deve-se buscar os limites jurídicos objetivos, impostos aos provedores no trato das informações pessoais inseridas pelos usuários quando da utilização dos serviços colocados à disposição deles.

Em conclusão, existe uma preocupação com a disponibilidade dos dados pessoais capturados na internet e tal situação gera uma salutar movimentação legislativa para tentar barrar os abusos. Nada obstante, verifica-se, de forma cada vez mais intensa, a possibilidade de captura e utilização de dados pessoais

---

[14] WARD, Jonathan Stuart and BARKER, Adam. *Undefined By Data: A Survey of Big Data Definitions*, School of Computer Science University of St Andrews, UK, arXiv:1309.5821v1 [cs.DB], 20.Sep.2013.

[15] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro, Renovar, 2006, p. 173.

para os mais diversos fins. Nesse contexto, podemos dizer que a chamada sociedade informacional é também "desprotegida".

Paul Schwartz e Daniel Solove ensinam que dados pessoais (identificados) dizem respeito a uma pessoa específica, enquanto dados identificáveis (anônimos) sugerem a relação do dado com uma pessoa, porém a conexão ainda não ocorreu — sendo possível que tal conexão ocorra a qualquer momento — por meios que transformem tais dados anônimos em dados pessoais[16] A anonimização, que será explicada em maior detalhes no capítulo 3, em resumo, é o nome que se dá para técnicas que visam proteger a privacidade de indivíduos em grandes bancos de dados.

Nesse sentido, para que haja real proteção dos dados pessoais, os dados pessoais identificados e identificáveis (anônimos) deverão ser protegidos, porque os processos de anonimização são reversíveis, ou seja, os dados considerados anônimos podem deixar de sê-lo por meio de processos de reidentificação do usuário. Defende-se um conceito expansionista. Ou seja, deverá ser protegido o dado pessoal relacionado a uma informação que potencialmente identifique alguém.

Apenas para que não haja dúvidas, entende-se que o conceito expansionista é o mais adequado, pois se, no caso concreto, os dados pessoais forem identificáveis, a lei deverá ser aplicada. Nesse sentido, uma maior gama de pessoas estará protegida pela lei quando seus dados pessoais forem aqueles considerados identificáveis e não só os identificados.

A dissertação será dividida em três capítulos. No primeiro capítulo, serão abordadas questões relacionadas aos dados pessoais na economia informacional, além de conceitos básicos para compreensão do tema. No segundo capítulo, será abordada a forma de tratamento dos dados pessoais e o tratamento despendido pela legislação para proteção dos dados pessoais.

---

16 SCHWARTZ, Paul; SOLOVE, Daniel J. The PII Problem: privacy and a new concept of personally identifiable information. 86 N.Y.U. L.Q. Rev. 1814 (2011). Disponível em http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2638&context=facpubs Acesso em 03.mar.2017 p. 1873 e 1874. No original: "Identified information already refers to a specific person, while identifiability suggests that such a connection has not yet occurred, but is possible

CAPÍTULO 1: DADOS PESSOAIS E A ECONOMIA INFORMACIONAL

1.1. Conceitos importantes para compreensão do tema

1.1.1. Conceito de dados pessoais

A abordagem conceitual sobre os dados pessoais é essencial à análise do tema de pesquisa proposto, porque que se trata da precisa delimitação do objeto, ou fato da vida, sobre o qual recaem os direitos e deveres que se procura analisar no presente trabalho. Os dados pessoais e a sua análise jurídica ganharam relevância pela popularização de novos modelos de negócio que se utilizam daqueles para produzir e vender informações sobre consumidores, de interesse de diversos fornecedores de produtos ou serviços, para isso se valendo das ferramentas tecnológicas colocadas à disposição por meio da internet.

As questões trazidas sobre coleta e tratamento de dados pessoais, inclusive sua conceituação, não são exclusivas da internet, já sendo levantadas em momentos anteriores, como com o advento do Código de Defesa do Consumidor e a formação de cadastros de inadimplentes. Contudo, neste trabalho, o corte epistemológico escolhido foi justamente a coleta e tratamento de dados pessoais na internet.

Não existe consenso a esse respeito entre os estudiosos do assunto. Conforme o enfoque e os objetivos de determinada pesquisa, moldam-se os elementos a serem agregados para definição do que vêm a ser dados pessoais. Desta forma, trata-se de um conceito plástico, indeterminado, que está sob constante modificação e atualização, mantendo, contudo, uma mínima unidade conceitual.

O adjetivo “pessoal”, que qualifica o substantivo “dado”, já referenciado anteriormente, dá a noção de singularidade, ou seja, de algo que se liga a um determinado indivíduo, distinguindo-o dos demais. Esta característica é essencial para a compreensão do relacionamento entre usuários e fornecedores de serviço da rede mundial de computadores.

Bruno Bioni e os demais integrantes do Grupo de Pesquisa em Políticas Publicas Para o Acesso à Informação da

Universidade de São Paulo, em interessante estudo acerca do assunto, destacam que um dado pessoal é "*um signo que permita estabelecer de forma imediata ou direta um vínculo com o seu titular, individualizando-o de forma precisa*"[17].

No âmbito da internet, a problemática relativa aos dados pessoais ganha relevância ainda maior. Isso porque o uso da rede mundial de computadores foi arquitetado e se desenvolveu de uma forma que os serviços colocados à disposição (de forma gratuita ou cobrada do usuário) formam uma base de dados gigantesca de dados pessoais. Tal base de dados possibilita, a qualquer um que tenha as necessárias ferramentas, a transformação de dados em conteúdo comercial relevante.

Com o desenvolvimento do conceito de dados pessoais e das suas consequências, fica ressaltada a necessidade de se atribuir qual o espectro de incidência da proteção de dados pessoais no mundo dos fatos. Caso contrário, podem ocorrer entraves jurídicos insuperáveis ao desenvolvimento de novas formas de exploração dos meios de comunicação que a internet propicia.

1.1.1.1. Diferenciação de dados pessoais e informação

Como precedente lógico do conceito de dados pessoais, impende estruturar uma diferenciação entre "dado", "informação" e "conhecimento". É importante destacar que os conceitos a serem trabalhados ultrapassam a esfera da análise jurídica, posto que dizem respeito a áreas específicas do conhecimento humano, e, portanto, são melhor desenvolvidos por profissionais que se dedicam ao estudo desses temas.

Valdemar Setzer, professor do Instituto de Matemática e Estatística da Universidade de São Paulo, explora essas noções em interessante artigo publicado na internet[18], conceituando e relacionando as noções ligadas a esses termos. Segundo o autor,

---

17 Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação. XEQUE-MATE - O Tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. Disponível em https://gpopai.usp.br/wordpress/wp-content/uploads/2016/06/Xeque-Mate.pdf, acesso em 10.7.16.

[18]SETZER, Valdemar W. - Dado, Informação, Conhecimento e Competência – disponível em https://www.ime.usp.br/~vwsetzer/dado-info.html, acesso em 03.jul.2016.

dados são uma "*sequência de símbolos quantificados ou quantificáveis*". Numa análise perfunctória, depreende-se que o conceito de dados remete a uma realidade simbólica e matemática.

Simbólica, pois diz respeito a uma representação de fatos que ocorrem no mundo fenomênico. Um dado pode ser expresso por qualquer tipo de signo, inclusive letras, números, imagens, sons, dentre outros.

O conceito de dado não se liga à sua inteligibilidade para um leitor, ou seja, é irrelevante a capacidade do leitor de certo dado de entendê-lo, sendo esta uma operação intelectual posterior. Com efeito, para ser considerado dado, nem mesmo é necessário que qualquer pessoa saiba interpretá-lo, como é o caso de algum escrito em uma língua já esquecida.

Um dado é, ainda, uma realidade matemática, pois se trata de algo quantificado ou quantificável, ou seja, de qualquer forma traduzível em números. Isso implica na possibilidade de sua tradução de forma estruturada, gerando a noção do que se chama "banco de dados".

Danilo Doneda, em monografia sobre o tema[19], anota que o conceito de dado remete a uma certa crueza informacional quando comparado com expressões como informação e conhecimento. Segundo o especialista, o dado consiste em uma informação em estado potencial, precedendo o tratamento intelectivo que configura esta última. Relaciona-se à ideia de cognoscibilidade, ou seja, relação direta com os fatos apontados sem ainda passar por um "filtro cognitivo".

A estruturação de dados em um banco de dados é o que possibilita seu processamento automatizado. Esse processamento pode ser realizado por meio de computadores e também de outros sistemas de computação continuamente conectados à internet, como se verá posteriormente.

O conceito de informação, por outro lado, também é tratado por Danilo Doneda como algo diverso do significado de dado, acima exposto. Ainda, segundo apontado por Valdemar Setzer,

---

[19] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro, Renovar, 2006, P. 152

informação é uma abstração informal que está na mente de alguém e que não pode ser expressa de maneira formal:

> Informação é uma abstração informal (isto é, não pode ser formalizada através de uma teoria lógica ou matemática), que está na mente de alguém, representando algo significativo para essa pessoa[20].

Nota-se que se trata de um conceito mais aberto do que o de dado, posto que as expressões que Valdemar Setzer utiliza não possuem significado preciso, carecendo de uma análise concreta para preenchimento das lacunas.

O processo informacional é intelectivo, posto que pressupõe um processo semântico entre significado e significante, dependendo, em larga escala da subjetividade daquele que recebe a informação para seu processamento. Desta forma, como apontado pelo autor, percebe-se que as diferenças entre dados e informações são de caráter estrutural.

Enquanto aqueles caracterizam-se como elemento sintático, ou seja, uma representação simbólica de algo real, estas últimas são semânticas, ou seja, trata-se de um processo de atribuição de significado a um significante, sendo este simbólico (dado) ou não. Destaca-se que, por se tratar de um processo subjetivo, é inviável a estruturação de informações de maneira lógica, justamente por pressupor a integração da mente humana no processo de formação da informação.

Ainda, o autor ensina que a informação pode ou não pressupor o recebimento de dados. Ou seja, o processo de geração de informações pode decorrer da atribuição de um significado a um determinado dado ou, ainda, mediante percepção direta de fatos. Assim, no atual estado da tecnologia, são inviáveis a coleta e o tratamento de informações por meio da internet, mas tão somente dos dados que as alimentam. A informação é criada e armazenada na mente do próprio destinatário.

Em conclusão, pode-se afirmar que informações são dados tratados, de forma que constituem efeito do processamento de

---

[20] SETZER, Valdemar W. *Op. Cit.*

dados. Assim, as informações trazem significado. Por meio dos dados analisados e interpretados sob determinada ótica (informação), é possível qualificar os resultados.

1.1.1.2. Amplitude do conceito de dados pessoais

A amplitude do conceito dos dados pessoais e, consequentemente, da proteção a ser conferida ao indivíduo enquanto titular destes tem relação com a precisão com que é possível atribuir certo dado pessoal a um individuo determinado. Neste sentido, estudiosos do tema entendem de diversas formas o que pode ser entendido como dados pessoais, estando, de um lado, aqueles que tendem a ampliar a abrangência deste conceito e, de outro, aqueles que preferem mantê-la no mínimo.

Esta discussão ganha especial relevância, mormente diante da existência de três projetos de lei, abordados mais à frente, que visam regular a coleta e o uso de dados pessoais pela internet. Esses projetos utilizam conceitos diversos, o que afeta de forma direta a amplitude da proteção a ser conferida ao usuário.

Apesar de existirem várias formas de classificação do conceito de dados pessoais, serão abordados dois conceitos mais abrangentes: o restritivo e o expansivo.

O primeiro conceito trazido pela doutrina, o restritivo, apega-se a uma ideia de "imediatidade", ou seja, restringe o alcance do conceito de dados pessoais somente às situações nas quais estes sejam diretamente relacionados a uma pessoa identificada de plano. Desta forma, aqueles que adotam este conceito acabam por restringir o conceito de dados pessoais àqueles dados que dizem respeito a uma pessoa identificada e determinada, não bastando a potencialidade de sua individualização. Neste sentido, veja-se a opinião de Marcel Leonardi:

> Se adotado esse conceito amplo [que engloba dados que não identificam necessariamente a pessoa natural, mas que estão relacionados a ela], ficarão sujeitos à lei praticamente todos os dados produzidos pela atividade humana, ainda que não possam ser razoavelmente utilizados

> para identificar uma pessoa natural determinada.
> Um conceito mais preciso é adotado pela legislação do Canadá, que fala em "dados sobre uma pessoa natural", e que com isso se mostrou mais adequado para equilibrar a proteção do titular com o livre fluxo de informações necessário à vida cotidiana moderna. Note-se que esse conceito mais preciso não impediu o Canadá de ser avalizado pela União Europeia como um país com legislação considerada adequada, para fins de transferência internacional de dados.
> Internacionalmente, o conceito de dados pessoais tem sido interpretado para englobar somente dados que razoavelmente permitam a identificação de uma pessoa natural, excluindo-se do conceito todos os dados que não sejam efetivamente capazes de identificar razoavelmente um indivíduo, bem como todos os dados que passarem por processos de anonimização.
> Teria sido melhor, portanto, que o projeto de lei adotasse conceito mais preciso, definindo dado pessoal como "dado que identifique ou permita, por meios razoáveis, a efetiva identificação da pessoa natural"[21].

Não são entendidos como dados pessoais, de acordo com esta linha de raciocínio, aqueles que somente podem ser relacionados a uma pessoa determinada por meios indiretos, ou seja, que necessitam de dados adicionais para identificação de seu titular.

De outro lado, também é possível adotar uma postura mais ampliativa em relação à abrangência da expressão "dados pessoais" o que, consequentemente, estende o espectro de proteção do usuário, nos termos a serem adiante alinhados[22]. Trata-se do

---

21 [especial] O que são dados pessoais?, Equipe responsável pelo conteúdo: Dennys Antonialli, Francisco Brito Cruz, Beatriz Kira, Juliana Pacetta Ruiz e Fabiane Midori Nakagawa. Disponível em http://www.internetlab.org.br/pt/opiniao/especial-o-que-sao-dados-pessoais/ Acesso em 03.dez.2017.

22 Cabe destacar que, no âmbito da União Europeia, foi adotada uma posição expansionista nas normas que regem a matéria. O texto da Diretiva 95/46, em seu artigo 2º, "a" define dados

conceito expansivo. Aqueles que adotam este conceito defendem que a mera potencialidade de identificação do titular de determinado dado é suficiente para qualificar este último como pessoal e, portanto, sujeito à proteção enquanto direito individual e subjetivo, oponível contra qualquer um que o viole, por ação, omissão ou abuso. Neste sentido, veja-se Danilo Doneda e Laura Schertel Mendes:

> O conceito de dados pessoais proposto no PL 5.276/2016 – entendido como aquele que permite identificar a pessoa natural – é adequado e apto para possibilitar que a lei atinja o seu objetivo principal, qual seja, o de proteger a pessoa contra os riscos derivados do processamento de dados pessoais na sociedade da informação. Além disso, o conceito está em consonância com as legislações internacionais sobre proteção de dados pessoais. (...) A informação pessoal difere de outras informações por possuir um vínculo objetivo com a pessoa, isto é, por revelar aspectos que lhe dizem respeito. Desse modo, resta claro que tais informações merecem tutela jurídica, uma vez que, por terem como objeto a própria pessoa, constituem um atributo de sua personalidade. Fundamental é perceber que tal tutela visa à proteção da pessoa e de sua personalidade e não dos dados *per se*[23].

Desta forma, encontram-se abrangidos pela noção de dados pessoais aqueles dados que são relacionados de forma

---

pessoais como "qualquer informação relativa a uma pessoa singular identificada ou identificável ('pessoa em causa'); é considerado identificável todo aquele que possa ser identificado directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social". A mesma linha seguiu o artigo 2º da Convenção 108/81, também da União Europeia. Da mesma forma, o Regulamento Geral de Proteção de Dados Europeu, de 27 de abril de 2016, em seu art. 4º, 1, prescreve que é "considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular".

[23] [especial] O que são dados pessoais?... *Op. Cit.*

imediata a determinado sujeito, assim como aqueles que demandam certo esforço cognitivo para tal vinculação, mediante processamento desses dados junto a outros dados.

Estudiosos no assunto têm se debatido acerca do limite dos esforços cognitivos que devem ser empreendidos para que determinado dado seja considerado identificável. Como destacam os integrantes do Grupo de Pesquisa em Políticas Publicas Para o Acesso à Informação da Universidade de São Paulo, em estudo publicado no ano de 2015, a existência de dados anônimos, ou não identificáveis, é algo impossível, do ponto de vista da ciência da análise de dados[24].

Na prática, a proteção de todos os dados que circulam pela internet como pessoais, mediante o alargamento da identificabilidade, é algo que inexoravelmente levaria à derrocada dos modelos de negócio que atualmente são utilizados neste ambiente, além de restringir a circulação de informações de forma a tornar praticamente impossível a exploração da comunicação.

Dentro da técnica jurídica, a razoabilidade tem sido entendida como limitação lógica aos direitos individuais, servindo como contraponto ao sistema do "tudo ou nada", de exclusividade de direitos, ou seja, no caso concreto, aferindo-se objetivamente os meios e os fins, o aplicador da norma deve atentar-se para critérios aceitáveis de exercício dos direitos.

A identificabilidade dos dados pessoais também não deve passar despercebida. Por isso, propostas têm sido formuladas, no meio acadêmico e em discussões legislativas, para a adoção do critério da razoabilidade como limitador da abrangência do conceito de dados pessoas identificáveis.

Dessa forma, entende-se que o conceito mais apropriado para a proteção dos dados pessoais é o expansionista. Por meio de tal conceito, estariam protegidos os dados identificados e identificáveis. É mais adequado à proteção dos dados pessoais, porque apresenta maior flexibilidade para que, diante do caso concreto, haja possibilidade de amparo ao individuo titular dos dados em situações em que seus dados possam vir a ser identificados.

---

[24] Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação. *Op.Cit.*

Em oposição ao conceito expansionista, existe o reducionista, aquele no qual, por meio de uma lógica mais restritiva, entende-se que seriam considerados dados pessoais apenas aqueles que tenham identificação imediata com a pessoa[25].

Paul Schwartz e Daniel Solove ensinam que os Estados Unidos utilizam-se da lógica reducionista do conceito de dados pessoais, e, por outro lado, a União Europeia utiliza-se da lógica expansionista, já que trata de dados identificados ou identificáveis: "*In the European Union, moreover, information that refers to an identifiable person is treated in the same fashion as that which refers to an identified person*"[26].

Apenas para que não haja dúvidas, entende-se que, no caso concreto, se os dados pessoais forem identificáveis, a lei deverá ser aplicada. Isso porque deve-se ter em mente que, apesar de existirem técnicas para retirada do vínculo entre a pessoa à qual se refere o dado e o dado em si (desanonimização), tais técnicas são reversíveis, ou seja, o dado considerado anônimo (identificável) pode deixar de sê-lo por processos de reidentificação. Neste sentido, uma maior gama de pessoas estará protegida pela lei quando seus dados pessoais forem aqueles considerados identificáveis e não só os identificados.

1.1.2. Captura de Dados Pessoais

Em um mundo cada vez mais móvel, os fornecedores de tecnologia, redes de publicidade e corretores de dados colaboram para obter ganhos com os dados pessoais. As empresas estão observando, coletando e compartilhando dados pessoais com as outras sem que o usuário tenha concordado e sequer tenha conhecimento.

Um exemplo dessa troca de informações é o que acontece quando se entra em um *site* de comercialização de sapatos e posteriormente se faz o *login* no Facebook. O par de sapatos visitado na página da empresa — que não possui qualquer relação direta com o Facebook — reaparece na rede social.

---

[25] DONEDA, Danilo. *Da privacidade... Op. Cit.* p. 156
[26] SCHWARTZ, Paul; SOLOVE, Daniel J. The PII Problem … *Op Cit*. p. 1874.

Tal situação é chamada pela indústria de anúncios na internet como de *re-targeting* (que pode ser realizada por meio de *data mining*). As empresas esperam que, ao mostrar esse item ao usuário que antes o visitou, o consumidor irá realizar a compra. Trata-se de uma tática bem agressiva que costuma funcionar. Assim ensina Alessandro Hirata:

> Por meio da chamada mineração de dados (*data mining*), ou prospecção de dados, as empresas são capazes de melhorar suas vendas e lucratividade. Com esses dados, as empresas podem delinear o comportamento *on-line* de clientes em potencial, atingindo seu público-alvo facilmente. Pode-se definir a mineração de dados como o processo de explorar grandes quantidades de dados à procura de padrões consistentes[27].

Para verificar como ocorre esse fenômeno, a forma de transferência dos dados pessoais após sua captura na internet deverá ser analisada.

A coleta de dados pessoais no Facebook, por exemplo, começa com a inscrição (abertura de perfil). A partir desse momento, quanto mais informações forem preenchidas, como quando cursou o colégio ou se é casado, mais possibilidades o Facebook tem sobre a construção de perfis de consumo de seus usuários. Esse é o primeiro passo para a elaboração do chamado "gráfico social": um mapa de tudo que o usuário faz, o que "curte" e todas as pessoas que conhece (inclusive, diferencia os amigos entre aqueles com quem o usuário interage mais ou menos).

O Facebook também rastreia quantas horas por dia cada usuário gasta no *site*. Um usuário ativo e com uma ampla rede de amigos que sejam ativos será identificado pela plataforma como um "influenciador". Tais perfis são capazes de gerar propaganda para seus amigos.

---

[27] HIRATA, Alessandro. O Facebook e o direito à privacidade. *Revista De Informação Legislativa,* v. 201, p. 20. *Disponível em* <https://www2.senado.leg.br/bdsf/bitstream/handle/id/502950/001002775.pdf?sequence=1>. Acesso em 5.mar.16.

Mesmo que o usuário não acesse muitos *sites* de compra, caso algum amigo com quem ele interaja frequentemente acesse determinado *site*, será identificada a situação e o usuário também pode receber publicidade referente àquele *site*. Quando o usuário joga algum jogo ou aceita alguma oferta, o gráfico social se expande.

Ao se visitar um *site* usando o Facebook, o *site* acessado também tem acesso a toda a informação que o Facebook tem no gráfico social do usuário. Tais dados permanecem supostamente anônimos até que seja feito um cadastro no *site*. Caso seja realizado o cadastro, o *site* pode construir o seu próprio perfil de cliente completo com a informação Facebook.

Porém, tal acesso e compartilhamento de dados não é algo exclusivo do Facebook. Por meio de muitos aplicativos móveis — especialmente os gratuitos — encontram-se anúncios que podem capturar de diversas formas os dados pessoais. Esse compartilhamento de dados, para ser considerado lícito, precisa respeitar os direitos usuário, o que nem sempre ocorre, especialmente da maneira como a rede está arquitetada para capturar e compartilhar os dados pessoais.

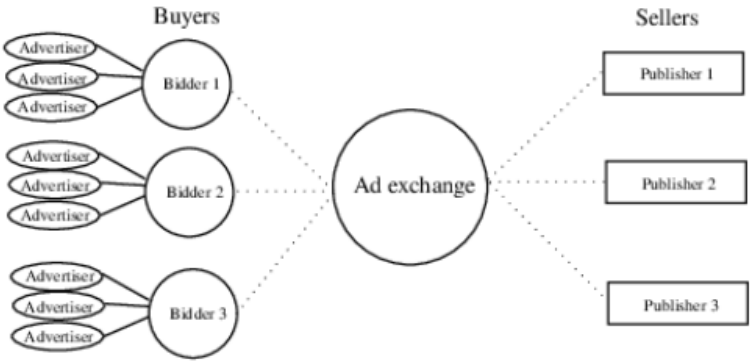
Há ainda empresas de *marketing* de dados pessoais especializadas em captura de dados pessoais. Entre elas, há o que se chama de *real time bidding,* que é um leilão de dados pessoais que ocorre em tempo real, e a cada minuto, de sorte a dinamizar a negociação pela preferência nos resultados de buscas de certos perfis de usuários.

As empresas que participam de tais leilões, como AppNexus, Turn ou Doubleclick, são muito grandes, e seu faturamento decorre, em larga escala, dessas operações e de *data mining* sobre os usuários. Tal leilão deve ocorrer (e ocorre) de forma muito veloz e oferece um vislumbre de quão rapidamente os dados pessoais são utilizados sem o conhecimento do usuário.

Lukasz Olejnik, PhD no instituto de pesquisa Inria, explica que os leilões em tempo real começam assim que o usuário acessa um *site*, independentemente do dispositivo que estiver usando.

Iniciam-se os lances em seguida sobre os dados que normalmente contêm "informações versáteis" sobre os usuários[28].

Segue abaixo infográfico para facilitar a compreensão do *real time bidding* elaborado por Lukasz Olejnik:



Como se nota no infográfico acima, assim que o usuário acessa o *site*, iniciam-se os lances de compra pelos *bidders* que, posteriormente, vendem os dados para o anunciante (*advertiser*). Paralelamente, os editores (*publisher*) vendem os dados adquiridos com o acesso do usuário no *site*. Assim, negociação pela preferência nos resultados de buscas de certos perfis de usuários segue de maneira totalmente dinâmica.

Em outras palavras: assim que o usuário que visita determinado *site*, é desencadeada uma solicitação de lance (que pode incluir vários dados, como informações demográficas do usuário, histórico de navegação, localização e a página que está sendo carregada).

Tal pedido passa do editor (*publisher*) para uma troca de anúncios (*ad exchange*), que abre a possibilidade de compra dos dados aos *bidders*, que enviam automaticamente lances em tempo real para que os anunciantes (*advertiser*) façam a propaganda

---

[28] OLEJNIK, Lukasz, *Real-time Bidding systems and how much are we worth*. Disponível em < http://lukaszolejnik.com/rtbdesc > Acesso em 20.5.16.

direcionada de seus anúncios ao usuário. Assim se dá a troca de dados pelo *real time bidding*. Na maioria das vezes, tudo isso se sem que o usuário tenha conhecimento e, como mencionado, de forma extremamente ágil e eficaz.

Lukasz Olejnik afirma, ainda, que informações como localização, sexo, idade e, até mesmo, renda, bem como demais identificadores baseados em *cookies* estão disponíveis[29].

Verifica-se, portanto, que o anonimato na internet é algo extremamente frágil. Os participantes do leilão (*bidders*) avaliam todas essas informações disponíveis pelo *real time bidding*, inclusive comparando-as com as suas próprias bases de dados e perfis de usuários, antes de fazer uma oferta. Isso tudo leva menos de 100 milissegundos[30].

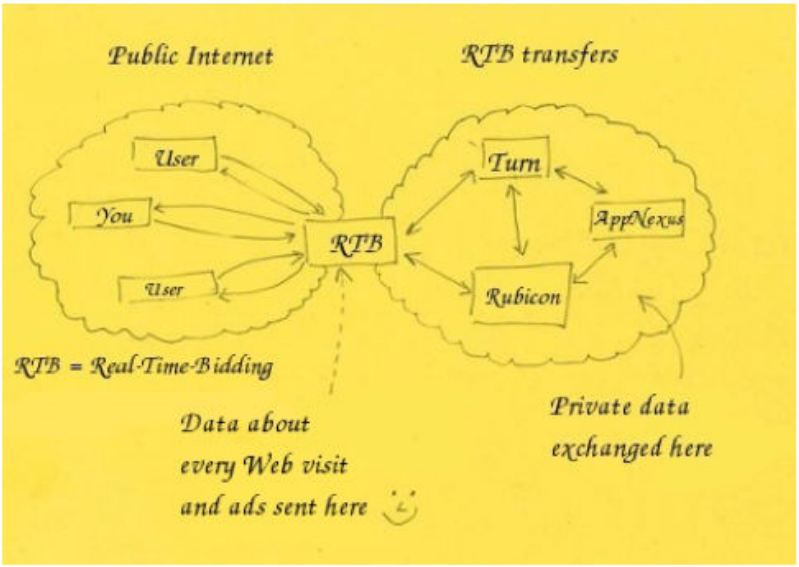
A esse respeito, segue abaixo outro gráfico, elaborado também por Lukasz Olejnik, no qual fica claro o caminho dos dados pessoais obtidos pelo *real time bidding* na internet.

De um lado, estão os usuários da internet pública; todos eles fornecem dados que possibilitam a ocorrência do *real time bidding,* e nele há informações sobre todas as páginas da internet visitadas e também sobre todos os anúncios recebidos pelo usuário. De outro lado, estão as empresas que fazem os lances para aquisição dos dados (*bidders*). Note que, entre elas, há a troca de dados:

---

[29] *Idem*. *Bidders* (such as AppNexus, Turn or Doubleclick) bid in the auction: they submit the monetary amounts they are willing to pay for this user's visit. The winner can present his advertisement (or resell it to other bidders via their own auctions). It is interesting to note that the bidders who did not win still obtain information on the user (for example, sites he visited). However, the winning bidder can initiate a Cookie Matching protocol and match the cookies related to this user with a cookie (or a cookie id) as seen by the RTB; Real-Time Bidding tied with Cookie Matching forms a very effective profiling platform where 3rd-party advertisers are no longer required to place their tracking scripts directly on the publisher's sites. After displaying of an advertisement, a bidder can potentially combine his previous knowledge on this user obtained from past bid requests he saved to enhance his profiling capabilities.

30 *Ibidem*.



Com os gráficos acima, fica evidente a facilidade de circulação de dados pessoais na internet e, como isso, em grande escala, torna-se cada vez mais difícil a possibilidade do anonimato na internet.

Apenas para que fique clara a forma de circulação de dados pela internet, será realizada uma breve digressão sobre a forma de captura dos dados (do ponto de vista técnico), para que seja possível a realização do *real time bidding.*

A captura de dados pode ocorrer de diferentes formas. Os protocolos MQTT, HTTP e Coap são os mais utilizados para captura dos dados pessoais. Cada um deles tem seus benefícios e casos de uso, veja-se:

- HTTP apresenta um método adequado para fornecer dados pessoais dos dispositivos para os sistemas centrais. Originalmente desenvolvido para o modelo de computação cliente-servidor, hoje ele suporta navegação na *web* todos os dias por meio de mais serviços especializados na internet. Enquanto ele atende aos

requisitos de funcionalidade para o envio de dados, HTTP inclui muito mais dados em torno da mensagem nos seus cabeçalhos.

- MQTT foi desenvolvido como um protocolo para máquina-a-máquina. Baseia-se em um modelo de publicação e assinatura para a entrega de mensagens a partir do dispositivo para um sistema central que atua como um mediador. A partir dele, serão enviados os dados para todos os outros sistemas que irão utilizá-los. MQTT é mais leve que o HTTP em termos de tamanho da mensagem, por isso é mais útil para implementações onde a banda é um problema potencial. No entanto, ele não inclui criptografia como padrão, de modo que deve ser considerado separadamente.
- Coap é outro padrão desenvolvido para ambientes de baixo consumo de energia e baixa banda larga. Coap é mais destinado a conexões de um-para-um. Ele é projetado para atender aos requisitos do projeto RESTO, fornecendo uma maneira de interagir com HTTP, mas ainda atender às demandas de dispositivos de baixa potência.

Os dados capturados devem ser precisos, sob pena de comprometer os próprios objetivos das aplicações. Levando em consideração um aplicativo que informa o trânsito em tempo real: se a ordem dos dados não está completamente alinhada e precisa, ele apontará para resultados potencialmente diferentes. Se uma determinada parte começa a falhar em condições particulares, há o risco de produção de resultados incorretos.

Alternativamente, os dados pessoais podem ser enviados ao sistema central por lotes (o registro histórico dos dados não disponível em tempo real). Isso é comum, por exemplo, com dispositivos em que a vida da bateria seja um requisito fundamental que supere a necessidade de entrega em tempo real dos dados.

Nesse sentido, Daniel Solove, mencionando o fato de seres humanos serem mais do que “porções” de dados, assinala para o fato de que os dados, mesmo quando corretos, não possuem nuances suficientes para demonstrar verdadeiramente o indivíduo

que os gerou. Afirma, ainda, que erros em *data mining* e *profiling* podem arruinar a vida de uma pessoa[31]

Também ocorre a venda de dados pessoais fora da internet, quando, por exemplo, utilizamos um cartão fidelidade. Por meio de seu uso, a empresa agrega informações sobre hábitos de consumo, endereço e, muitas vezes dados bancários, além de todas as informações cedidas quando realizado o cadastro.

Por fim, nota-se que, apesar de complexo, o sistema de transferência de dados pessoais ocorre a cada clique do usuário na internet, o que evidencia mais ainda os riscos que se colocam na proteção de dados pessoais e a necessidade de proteção a tal direito no Brasil com a urgência que merece.

1.2. Tratamento automatizado de dados pessoais

A definição de tratamento de dados é muito ampla e é difícil conceber qualquer interesse de uma empresa (na coleta de dados pessoais) que não seja o seu processamento. Conforme o art. 3º do Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, esse tratamento significa 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, por difusão ou por qualquer outra forma de disponibilização, a comparação ou
- a interconexão, a limitação, o apagamento ou a destruição.

[31] SOLOVE, Daniel J., The Digital Person: Tecnology and Privacy in The Information Age, NY: New York University Press, 2004, p. 41.

A grosso modo, o tratamento trata da manipulação de dados por uma máquina. As empresas normalmente utilizam sistemas de computador para executar uma série de operações sobre os dados, a fim de apresentar, interpretar, ou obter informações, conforme se verá abaixo. Tudo isso se dá por meio do ciclo de processamento de dados. E, após todo o processo, as informações úteis podem ser apresentadas de várias formas, tais como diagramas, relatórios, gráficos, ou como aquele que está tratando os dados entender mais adequado.

Para melhor compreensão do processo, seguem os estágios do ciclo de processamento de dados:

- Coleta: a primeira fase do ciclo é extremamente importante, pois todo o processamento dependerá dos dados coletados neste momento. Todos os dados colhidos devem ser definidos e precisos, para que as decisões subsequentes e conclusão sejam válidas. Esse estágio proporciona uma base para o início do ciclo, bem como um objetivo sobre o que deve ser melhorado. Alguns tipos de coleta de dados incluem (a) censo (levantamento de dados sobre tudo de determinado grupo ou população estatística), (b) pesquisa por amostragem (método de coleção que inclui apenas uma parte da população total) e (c) administrativa de subproduto (coleta de dados é um subproduto do dia a dia de uma empresa).

- Preparação: é a manipulação de dados numa forma adequada para posterior análise e processamento. Dados brutos não podem ser processados, assim, devem ser preparados para que se possa checar sua precisão A preparação é sobre a construção de um conjunto de dados, de uma ou mais fontes, a ser utilizado para uma maior exploração e processamento. Se nesse processo forem incluídos dados que não tenham sido cuidadosamente selecionados para os problemas, podem produzir resultados errados.

- *Input*: nessa fase, os dados codificados são convertidos em uma forma que seja legível para a máquina, para que

possam ser totalmente processados por meio de um computador. Este processo requer velocidade e precisão. A maioria dos dados precisa seguir uma sintaxe formal e rigorosa, uma vez que há um grande processamento acontecendo para que os dados complexos tornem-se inteligíveis.

- Processamento: ocorre quando os dados são submetidos a vários meios e métodos de manipulação; é o ponto em que um programa de computador está sendo executado, por meio de código de programa. O processo pode ser constituído por vários segmentos de execução que são capazes de efetuar simultaneamente diferentes instruções. Enquanto um programa de computador é um conjunto de instruções passivas, um processo é a real execução dessas instruções (do computador). Muitos *softwares* estão disponíveis para o processamento de grandes volumes de dados em prazos muito curtos.

- *Output* e interpretação: é a fase em que a informação processada é transmitida para a organização. O *output* é apresentado às empresas em vários formatos de relatórios (impresso, áudio, vídeo). Os relatórios serão interpretados de modo que possam fornecer informações significativas que irão orientar as decisões futuras da empresa.

- Armazenamento: é o último estágio do ciclo de processamento de dados, no qual os dados, a instrução e as informações são armazenadas para uso futuro. A importância deste ciclo é que ele permite um acesso rápido e a recuperação da informação processada, permitindo pular etapas do processamento de dados, quando necessário.

Assim, pode-se dizer que o ciclo de processamento de dados é constituído por uma série de etapas realizadas para extrair informações de dados brutos. Embora cada passo deva ser tomado em ordem, a ordem é cíclica. O estágio de *output* e de

armazenamento pode levar à repetição da fase de coleta de dados, por exemplo, resultando em um outro ciclo de processamento de dados. O ciclo oferece uma visão sobre a forma como os dados viajam e se transformam desde a coleta até a interpretação, para, finalmente, serem utilizados em decisões comerciais eficazes.

A respeito do tratamento e utilização de dados para gerar decisões comercialmente eficazes, segue exemplo retirado do *site* da empresa Dior Couture (Portugal). Empresas com tamanha rentabilidade nem sempre consideram vantajosa a contratação de empresas terceirizadas para tratar os dados coletados dos usuários. No caso, pode-se verificar que, após o consentimento do usuário, é a própria Dior que realiza a coleta e tratamento dos dados:

> Esses dados, qualquer que seja a sua natureza, podem permitir direta ou indiretamente que a Christian Dior Couture identifique e conheça melhor os internautas e lhes envie o seu boletim informativo e/ou responda às suas mensagens. (...)
> Consentimento
> Nenhum dado de caráter pessoal será coletado sem o consentimento dos internautas. A natureza facultativa ou obrigatória das menções a comunicar à Christian Dior Couture no âmbito da coleta efetuada no Portal será previamente indicada aos internautas. Esses últimos não são obrigados de forma alguma a transmitir à Christian Dior Couture dados de caráter pessoal. Contudo, em caso de recusa, a Christian Dior Couture não estará em condições de enviar aos internautas o seu boletim informativo e/ou de responder às suas mensagens. (...)
> 3.3 Identidade do responsável do tratamento de dados de caráter pessoal
> A sociedade Christian Dior Couture é responsável pela coleta e tratamento dos dados de caráter pessoal efetuados no Portal.
> 3.4 Destinatário (s) dos dados de caráter pessoal
> A sociedade Christian Dior Couture é a única destinatária dos dados de caráter pessoal

> coletados no Portal. Os dados de caráter pessoal não serão comunicados a terceiros[32].

Em conclusão, pode-se verificar do que foi exposto acima que o processo de tratamento de dados se dá de diferentes formas e não é algo extremamente complexo, ou seja, é possível que seja realizado com relativa facilidade pelas próprias empresas (vide caso Dior). Sendo assim, cria-se ainda maior vulnerabilidade ao indivíduo a quem os dados pessoais dizem respeito.

1.3. Sociedade Informacional e Sociedade da Vigilância

O Direito, enquanto ciência das relações sociais, não fica alheio às mudanças sociais provocadas pela internet. Essa modificação da realidade — que altera o pensamento jurídico — pode ser observada ao longo dos últimos anos, em especial na jurisprudência.

Porém, antes de tratar do conceito de sociedade informacional, é importante fazer uma breve digressão sobre a internet e seu surgimento. A internet teve a sua origem, em 1969, no Departamento de Defesa dos Estados Unidos, no denominado programa ARPANET (*Advanced Research Projects Agency Network*), conforme mencionam Garcia Marques e Lourenço Martins[33]. Lima explica que o sistema ARPANET era restrito ao ambiente interno e, somente a partir de 1972, teve início a transmissão de dados por meio do Protocolo de Internet. Em 1983, esse método de transmissão foi adotado universalmente[34].

Naquele momento, a internet foi implementada com o objetivo de assegurar uma rede de comunicação segura para organizações ligadas à área da defesa do país. Posteriormente, na

---

32 Dior, *Dados de Caráter Pessoal*, Disponível em https://www.dior.com/couture/pt_br/dados-de-carater-pessoal, Acesso em 25.nov.2017.

[33]MARQUES, Garcia; MARTINS, Lourenço. *Direito da Informática*. Coimbra: Livraria Almedina, 2000. p 50

[34] LIMA, Cíntia Rosa Pereira de. *Validade e obrigatoriedade dos contratos de adesão eletrônicos (shrink-wrap e click-wrap) e dos termos e condições de uso (browse-wrap): um estudo comparado entre Brasil e Canadá*. Tese de Doutorado. Universidade de São Paulo. 2009, p. 1.

década de 1990, houve sua expansão por meio da criação do aplicativo que organizava a internet de acordo com as informações:

> Um novo salto tecnológico permitiu a difusão da Internet na sociedade em geral: a criação de um novo aplicativo, a teia mundial (*world wide web* – WWW), que organizava o teor dos sítios da Internet por informação, e não por localização, oferecendo aos usuários um sistema fácil de pesquisa para procurar as informações desejadas[35].

Marco Aurélio Greco assevera que, com a expansão da internet, "*acontece uma revolução mais do que de natureza técnica, revolução ligada ao próprio padrão da civilização ocidental, que está se alterando em sua concepção básica*"[36].

Após breve contextualização histórica, parte-se para o conceito de internet. Ricardo L. Lorenzetti[37] a define como uma rede internacional de computadores interconectados, que permite que dezenas de milhares de pessoas se comuniquem entre si, bem como possibilita o acesso a colossal quantidade de informações do mundo todo. Com o seu surgimento e ampliação, a internet revolucionou as relações em todo o mundo, sendo certo que seus efeitos sociais vão desde a mais singela troca de mensagens até a negociação e celebração de negócios complexos.

Ao tratar da expansão e popularização do espaço virtual, Emilio Tosi ensina que a internet não é um fenômeno unitário, sendo formada por um sistema complexo que congrega outros meios de comunicação, como o telefone e o satélite. Em suas palavras, a internet não é, portanto, um fenômeno unitário que pode ser rastreada até um centro organizado: é uma rede de redes, um conjunto complexo e articulado de redes de intercomunicação estabelecidas

---

[35] CASTELLS, Manuel. *A sociedade... Op. Cit.*, p. 87.
[36] GRECO, Marco Aurélio. Internet e Direito. São Paulo: Dialética, 2000. p. 16.
[37] LORENZETTI, Ricardo Luis. *Comércio Eletrônico*. Trad. Fabiano Menke. São Paulo: Revista dos Tribunais, 2004. p. 25.

por tantos computadores interligados por meio de linhas telefônicas comuns, digitais ou via satélite[38].

Sobre o conceito de rede, Castells pontua que se trata de um conjunto de nós interconectados. Explica que nó é o ponto no qual uma curva se entrecorta. Redes são estruturas abertas capazes de se expandir de forma ilimitada, integrando novos nós, desde que consigam comunicar-se dentro da rede, ou seja, desde que compartilhem os mesmos códigos de comunicação[39].

A internet é a rede das redes de computadores interligados entre si[40], nela cada computador possui um endereço IP, ou seja, um número de identificação. Por meio das redes, milhões de pessoas se comunicam, diversas transações comerciais são realizadas e informações são compartilhadas a todo momento.

A simplificação cada vez maior da internet, aliada aos movimentos de popularização do espaço virtual, na década de 2000[41], foi marcada pela implementação de transformações cada vez maiores no chamado mundo virtual. Ao passo em que a internet se popularizava, foi-se criando o conceito de cultura digital, desenvolvido por especialistas que estudaram a internet e os seus diversos impactos na vida contemporânea.

A respeito do conceito de cultura digital, Lima elucida que a cultura digital promove o uso de *software* livre e ações de inclusão digital, ampliando a criação e circulação de informação[42].

O conceito de cultura digital também foi definido por Manuel Castells, em um dossiê publicado pela revista Telos, ao pontuar algumas de suas características, conforme se vê abaixo em tradução livre.

---

[38] TOSI, Emilio. *Il Contrato Virtuale – Procedimenti formativi e forme negoziali tra tipicità e atipicità*. Milão: Giuffrè Editore, 2005. p. 4.
No original: (*...) internet non è, quindi, un fenomeno unitario riconducibile ad un centro organizzato: è una rete di reti, ossia un insieme complesso e articolato di reti locali intercomunicanti costituite da tanti computer collegati tra loro attraverso linee telefoniche ordinarie, digitali o satellitari*

[39] CASTELLS, Manuel. *Op. Cit.*, p. 497.

[40] TEIXEIRA, Tarcísio. *Direito Eletrônico*. São Paulo: Editora Juarez de Oliveira, 2007. p. 10.

[41] O surgimento de empresas como Google e Yahoo! criou ferramentas de produção de informação e conhecimento como *blogs*, redes de relacionamento e *sites* interativos que possibilitaram a todos criarem e compartilharem conteúdo interagindo na internet com os demais usuários. Esta forma de utilização da internet foi chamada de "Web 2.0".

[42] LIMA, Cíntia Rosa Pereira de. *Op. Cit*. p. 63.

- Capacidade de comunicar ou misturar qualquer produto com base em uma linguagem digital comum.

- Capacidade de se comunicar do local ao global em tempo real, e vice-versa, de modo a desfocar o processo de interação.

- Existência de múltiplos modos de comunicação.

- Interconexão de todas as redes digitalizadas de redes de dados ou a realização do sonho de hipertexto de Nelson, com o sistema de armazenamento e recuperação de dados chamado "Xanadu" em 1965.

- Capacidade para reconfigurar todas as configurações, criando um novo significado nas diferentes multicamadas dos processos de comunicação.

- Criação gradual de uma mente coletiva devido ao trabalho *online* por meio de um conjunto de cérebros sem limites. Nesta fase, o autor se refere a conexões entre os cérebros em linha e a mente coletiva[43].

---

[43]CASTELLS, Manuel. *Creativity, Innovation and Digital Culture*. A Map of Interactions. Disponível em https://telos.fundaciontelefonica.com/telos/articulocuaderno.asp@idarticulo=3.htm. Acesso em 4.abr.2016. Texto original:
"Ability to communicate or mix any product based on a digital common language.
Ability to communicate from the local to the global in real time, and vice versa, in order to blur the interaction process.
Existence of multiple modes of communication.
Interconnection of all data bases digitalized networks or the achievement of Nelson's hypertext dream with the storage and retrieving data system called "Xanadu" in 1965.
Capacity to reconfigure all configurations creating a new meaning in the different multilayers of the communication processes.

Após a digressão sobre o conceito de internet e cultura digital, passa-se ao conceito de sociedade informacional para que se possa compreender de que forma a realidade criada pela imersão do indivíduo na cultura digital se dá. Inicialmente é importante esclarecer que a expressão "sociedade da informação", conforme ensina o Newton De Lucca, é um termo equívoco e empregado em contextos diversos[44]. Tal expressão é usada desde a década de 70 pela sociologia, pelo menos, para se referir à fase pós-industrial.[45] Ou seja, a sociedade pós-moderna já era classificada como a sociedade "guiada pela informação e pelo conhecimento" segundo Daniel Bell[46].

Neste sentido, José de Oliveira Ascensão afirmou que a expressão sociedade da informação *"não é um conceito técnico: é um slogan. 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 toda a mensagem como informação"*.[47]

Para Pierre Levy, a sociedade de informação é fruto do conjunto de todos os impactos sócio-técnico-culturais da inovação e do desenvolvimento científico e tecnológico digital. Todos estes fatores teriam propiciado as novas configurações sociais, que são próprias da atual cultura digital[48].

No mesmo sentido, Adalberto Simão Filho e Kelly de Souza Barbosa ensinam que a sociedade informacional:

> O advento da sociedade da informação numa Era posterior a pós-modernidade (século XX) causou metamorfoses sociais, econômicas e

---

Gradual creation of a collective mind due to online work through a set of brains without any limits. At this stage, I am referring to connections between online brains and the collective mind."

[44] Prefácio. In: LEONARDI, Marcel. *Tutela e Privacidade na Internet*. São Paulo: Saraiva, 2012. p. 11.

[45] BELL, Daniel. *In*: *Business and Society Review/Innovation*. Disponível em: <https://www.os3.nl/_media/2011-2012/daniel_bell_-_the_coming_of_post-industrial_society.pdf>, acessado em 20 de outubro de 2015. p. 07.

[46] *Idem, Ibidem*.

[47] ASCENSÃO, José de Oliveira. *Direito da Internet e da Sociedade da Informação*, Rio de Janeiro: Forense, 2002, p. 71.

48 LEVY, Pierre. Ciberculura. Rubí (Barcelona) Editorial: México: Universidad Autónoma Metropolitana - Iztapalapa, 2007, p. 18.

> jurídicas, interferindo na forma como as pessoas se inter-relacionam, trabalham e contratam. A economia informacional rompeu velhos paradigmas e o conhecimento tecnológico foi supervalorizado no atual estabelecimento empresarial virtual[49].

Trata-se de uma sociedade que nasce com uma ínsita contradição fundamental: o acesso amplo ao conteúdo produzido, mas, em contrapartida, um profundo desequilíbrio no que diz respeito ao domínio da informação[50].

Para Cíntia Rosa Pereira de Lima, a sociedade da informação é permeada por relações jurídicas que se resumem em números, ou seja, são equacionadas, dispensando o contato mediato ou imediato entre as partes contratantes para conclusão do negócio jurídico, o que torna o processo de contratação mais rápido, barato e eficiente.[51]

Manuel Castells, ao tratar do assunto, afirma que o dinamismo da internet impede que sejam criados controles às ameaças criadas aos indivíduos e expõe quais são as características da chamada sociedade informacional, conforme tradução livre abaixo:

> Uma estrutura social baseada em rede é um sistema altamente dinâmico, aberto e suscetível a inovações, sem que isso seja uma ameaça para seu equilíbrio. As redes são instrumentos apropriados para uma economia capitalista baseada na inovação, na globalização e na concentração descentralizada; para trabalho, trabalhadores e empresas com base em flexibilidade e adaptabilidade; para uma cultura de desconstrução e reconstrução sem fim; para uma política voltada para o processamento instantâneo de novos valores e estados de

---

[49]SIMÃO FILHO, Adalberto e BARBOSA, K. S. Upgrade no direito de arrependimento virtual: projetos de lei 281/2012, 283/2012 e 4678/2016. *Revista de direito globalização e responsabilidade nas relações de consumo,* v. 1, p. 203-224, 2017. p. 204.

[50] ASCENSÃO, José de Oliveira. *O direito de autor no ciberespaço*. Revista Ajuris, Porto Alegre, vol. 26, nº 80, p.335, dez.2000.

[51] LIMA, Cíntia Rosa Pereira de. Op. Cit. p. 71.

> espírito públicos; e para uma organização social visando a superação do espaço e a aniquilação do tempo.[52]

Para Roberto Senise Lisboa, a sociedade informacional:

> "Sociedade da informação", também denominada de "sociedade do conhecimento" é expressão utilizada para identificar o período histórico a partir da preponderância da informação sobre os meios de produção e da distribuição dos bens na sociedade que se estabeleceu a partir da vulgarização das programações de dados utiliza dos meios de comunicação existentes e dos dados obtidos sobre uma pessoa e/ou objeto, para realização de atos e negócios jurídicos.[53]

Pode-se afirmar que o grande centro da sociedade em que estamos inseridos é a aplicação dos conhecimentos e informações (para geração de conhecimentos) obtidos por meio da captura de dados para gerar ganhos. "*Pela primeira vez na história, a mente humana é uma força direta de produção, não apenas um elemento decisivo no sistema produtivo*"[54].

O surgimento de um novo paradigma que se organiza em torno de novas tecnologias da informação acaba por possibilitar que a própria informação torne-se o produto do processo produtivo. Ou seja: as novas indústrias de tecnologia têm como produto

---

[52] CASTELLS, Manuel. *The rise of the network society* (Information age, v. 1), 2nd ed., Malden: Wiley-Blackwell, 2010, p. 501 – 502:
A network-based social structure is a highly dynamic, open system, susceptible to innovating without threatening its balance. Networks are appropriate instruments for a capitalist economy based on innovation, globalization, and decentralized concentration; for work, workers, and firms based on flexibility and adaptability; for a culture of endless deconstruction and reconstruction; for a polity geared toward the instant processing of new values and public moods; and for a social organization aiming at the supersession of space and the annihilation of time.

[53] LISBOA, Roberto Senise. Direito da Sociedade da Informação. *Revista dos Tribunais,* ano 95, vol. 847, maio de 2006. São Paulo: 2006. p. 85.

[54] CASTELLS, Manuel. *A sociedade… Op. Cit.*, p. 69.

dispositivos de processamento de informações ou o próprio processamento destas.

Tal fato pode ser sintetizado com a seguinte frase de John Perry Barlow, um dos maiores defensores do *copyleft* e da internet livre: "*noncommercial distribution of information increases the sale of commercial information. Abundance breeds abundance*"[55]. Considerando tamanha lucratividade e o modelo econômico em que estamos inseridos, e que a informação é produto da tecnologia da sociedade informacional, os dados pessoais encontram-se, cada vez mais, sujeitos a ameaças.

Como ensina Rodotà, o progresso incontido da internet — com a voraz coleta de dados e a conexão entre diversos bancos de dados que possibilita o cruzamento de dados — faz surgir também a sociedade do controle, da vigilância e da classificação[56]. Muitos atribuem à guerra contra o terror a justificativa para o surgimento da sociedade da vigilância, mas esta não é a única causa. Isso porque, cada vez mais, a coleta de dados mostra-se como um importante aliado do poder e influência no mundo (vide Wikileaks).

Com efeito, Cíntia Rosa Pereira de Lima reafirma o papel das tecnologias da informação nas formas de controle e vigilância de pessoas, veja-se:

> Em suma é cediço que as tecnologias da informação viabiilazm novas e variadas formas de controle e de vigilância das pessoas. Por exemplo, o sistema de identificação por radiofrequência (RFID), através do qual é possível utilizara tecnologia capaz de armazenar e transmitir dados coletados mediante o emprego de ondas de radiofrequência, também denominada de etiqueta eletrônica (*e-tag - eletronic tag*), coloca em risco a proteção da privacidade e dos

---

[55] BARLOW, John Perry. *The Next Economy of Ideas.* The Wired. 2010. Disponível em http://www.wired.com/2000/10/download/. Acesso em 2.mar.2016.

[56] RODOTÀ, Stefano. *A vida na sociedade da vigilância.* Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 145- 146.

> dados pessoais delineados para um sistema tradicional. [57]

Verifica-se que a coleta de dados se dá por entidades públicas e privadas e dos jeitos mais variados, atingido uma enorme parcela da população. Com o crescente uso de tais ferramentas para *data mining* e vigilância governamental, o individuo cada dia menos se vê diante da possibilidade de resguardo e controle de seus dados pessoais.

A sociedade da vigilância varre a linha existente entre as esferas pública e privada, isso porque o que é público e o que é privado estão totalmente conectados e juntos na captação de dados pessoais[58]. É certo que inúmeras vezes o poder público precisa do privado para implementar sistemas de captação de dados.

No artigo "*The Constitution in the National Surveillance State"*, o professor de Yale Jack Balkin ensina que existem dois tipos de estado de informação: o democrático e o autoritário[59].

---

[57] LIMA, Cintia Rosa Pereira de. *A imprescindibilidade de... Op. Cit.* p. 65

[58] O'HARROW Jr., Robert, *No Place to Hide,* New York: Free Press, 2006. p. 155.
Para exemplificar: "*For insight about the importance of these firms to ChoicePoint's new aims, consider Homeland Security White Paper: The Right Information a Right Time in the Right Place. At first glance, it looks like any other marketing material. But with each page, it becomes more interesting. ChoicePoint had teamed up with Templar, iMapData, and another little known company called Orion Scientific, a private intelligence-gathering specialist with close ties to the Defense Department, to produce the document. The paper described how the team was preparing networks that would serve as a public-private clearinghouse for all kinds of data. This wasn't limited to the 17 billion commercial records maintained by ChoicePoint. The system would also help police combine such information with details from their own database and then use software tools to automatically look for suspicious patterns or links among people".*

[59] Jack M. Balkin, *The Constitution in the National Surveillance State* (2008). Faculty Scholarship Series. Paper 225, p. 18 e 19. Disponível em: <http://digitalcommons.law.yale.edu/fss_papers/225>. Acesso em: 15.dez.15.
"We might begin by distinguishing between an authoritarian information state and a democratic information state. Authoritarian information states are gluttons and information state. Like gluttons they grab as much information as possible because this helps maximize their power. Authoritarian states are information misers because they try to keep the information they collect - and their own operations - secret from the public. (…)
By contrast, democratic information states are information gourmets and information philanthropists. Like gourmets they collect and collate only the information they need to ensure efficient government and national security. They do not keep tabs on citizens without justifiable reasons; they create a regular system of checks and procedures to avoid abuse. They stop collecting information when it is no longer needed and they dis- card information at regular intervals to protect privacy. When it is impossible or impractical to destroy information

> Os estados de informação autoritários são como glutões da informação. Como glutões, eles pegam tanta informação quanto possível porque isso ajuda a maximizar seu poder. Os estados autoritários são aversos à informação porque tentam manter a informação que eles coletam — e suas próprias operações — em segredo do público.
> Em contrapartida, os estados de informação democrática são *gourmets* e filantropos de informação. Como os *gourmets*, eles coletam e classificam apenas as informações de que precisam para garantir um governo eficiente e segurança nacional. Eles não controlam os cidadãos sem razões justificáveis; eles criam um sistema regular de controles e procedimentos para evitar abusos. Eles deixam de coletar informações quando não são mais necessárias e eles descartam informações em intervalos regulares para proteger a privacidade. Quando é impossível ou impraticável destruir informações, por exemplo, porque foram armazenadas de forma redundante em muitos locais diferentes, os estados de informação democrática regulam estritamente seu uso subsequente.
> Os estados de informação democrata também são filantropos de informação porque distribuem de boa vontade informações valiosas que criam para o público, sob a forma de educação, pesquisa científica e informações agrícolas e médicas. (tradução livre).

Em conclusão, Balkin afirma que os Estados Unidos vivem em um estado de vigilância autoritário, "*national surveillance state*". E, infelizmente, não há motivos para acreditar que não se viva a mesma situação no Brasil.

---

for example, because it is stored redundantly in many different locations-democratic information states strictly regulate its subsequent use. If the information state is unable to forget, it is imperative that it be able to forgive.
Democratic information states are also information philanthropists because they willingly distribute much valuable information they create to the public, in the form of education, scientific research, and agricultural and medical information. (...)".

William Staples afirma, ainda, que devemos esquecer o "Big Brother". Isso porque a imagem de uma vigilância externa deve ser superada por não ser apropriada atualmente. O autor ensina que a vigilância é acionada pela própria sociedade e todos estão envolvidos diretamente com a prática e processos da vigilância[60].

Priscila M. Regan afirma, inclusive, que a sociedade em que vivemos é a sociedade de risco, na qual as instituições, quaisquer que sejam, que lidam com indivíduos, coletam seus dados a seu respeito e a respeito de suas atividades. Afirma que tal situação gera uma necessidade, cada vez maior, de compilar informações sobre o indivíduo e eventuais riscos que ele pode apresentar. Finaliza afirmando que o conhecimento gerado pela vigilância não gera sensação de confiança ou de segurança, mas sim incertezas (o que, consequentemente, acarreta mais vigilância e coleta de informações sobre os indivíduos)[61].

Assim, da mesma maneira com que as relações estabelecidas por meio da internet cresceram enormemente, os repertórios de dados pessoais disponíveis também se multiplicaram. A existência de documentos, fotos, relatórios e outros *online* muitas vezes é esquecida pelos indivíduos.

---

[60] STAPLES, William G., Everyday Surveillance: Vigilance and Visibility in Postmodern Life. Lanham, MD: Rowman and Littlefield, 2000, p. 153

[61] REGAN, Priscilla M. (2002) Privacy as a Common Good in the Digital World, Information, Communication & Society, 5:3,382-405, DOI: 10.1080/13691180210159328, Disponível em http://dx.doi.org/10.1080/13691180210159328, Acesso em 13.dez.2017. p. 358.
No original: In a "risk society" every institution with which an individual deals collects information about that individual and her activities. This information is assessed in comparison to profiles of "trustworthy" and "untrustworthy," or "good" or "bad," in order to determine how the institution should structure its dealings with that individual. Ericson and Haggerty describe the logic as follows: "Risk society operates within a negative logic that focuses on fears and the social distribution of 'bads'…Collective fear and foreboding underpin the value system of the unsafe society, perpetuate insecurity, and feed demands for more knowledge of risk" (449). The risk society requires surveillance as a way of managing risk. But surveillance creates an unquenchable thirst for more and more information about the risks that exist generally and the risks posed by particular individuals. The knowledge produced by the surveillance systems does not result in a sense of security or trust, but produces instead new uncertainties leading to more surveillance and collection of information. Again to quote Ericson and Haggerty, "The problem is that they [the police] are constantly faced with imperfections in rules, formats, and technologies, which gives rise to both a sense of failure and a renewed sense that more such devices will work where fewer have not" (296). Given this logic, the prior actions of individuals bear little responsibility for surveillance systems and their concomitant privacy invasions.

Portanto, com as informações prestadas pelos próprios usuários, cria-se um ambiente no qual é possível a captura de dados pessoais, *profiling* e vigilância pelo poder público sob o argumento da proteção desses indivíduos sendo observados.

Pode-se dizer que um dos maiores riscos da atualidade é o que o sociólogo Zygmunt Bauman denomina de "danos colaterais da modernidade líquida" [62], ao ensinar que a fusão entre público e privado apresenta graves riscos à liberdade dos indivíduos. Tal situação coloca em evidência a necessidade da proteção dos dados pessoais o quanto antes, bem como de desenvolvimento de meios jurídicos para que as relações entre o indivíduo e o coletor de dados sejam mais equilibradas.

1.4. Monetização de dados pessoais

Os dados pessoais alcançaram importância no mercado de consumo atual. A coleta gigantesca de dados (possível graças ao desenvolvimento de tecnologias que permitem o refinamento dos dados com sua rápida circulação na sociedade) tornou os dados pessoais uma importante moeda de mercado. A sociedade informacional converge com a sociedade contemporânea de consumo, na medida em que a economia exige, para seu complexo funcionamento, uma enorme quantidade de dados pessoais possíveis de serem armazenados, processados e transmitidos por meio da tecnologia da informação[63].

Nesse sentido, Roberto Senise Lisboa ensina que, na sociedade informacional, o sucesso de uma organização dependerá mais dos ativos de conhecimento do que dos ativos físicos e financeiros, veja-se:

> Afinal, na sociedade da informação, os ativos do conhecimento determinam o sucesso ou o

---

[62] BAUMAN, Zygmunt. *Danos Colaterais; desigualdades sociais numa era global.* Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013. p. 108

[63] MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental,* São Paulo: Saraiva, 2014, p. 89.

> fracasso da organização e prevalecem sobre os ativos físicos e financeiros[64].

É evidente que, na economia atual, os dados dos consumidores têm valor potencial, e que, após coletados e tratados, atesta-se seu valor. Ou seja: primeiro tudo é coletado para que depois ocorra eventual organização de dados.

Exemplos claros do valor dos dados pessoais são as redes sociais. Como modelo de negócios, seu valor está condicionado à quantidade de dados pessoais que possuem. Por tal motivo, as redes sociais incentivam os usuários a alimentá-las com seus dados. A esse respeito, afirma Danilo Doneda:

> (...) é natural que elas incentivem seus usuários a alimentá-las com seus próprios dados. A indução ao fornecimento dos próprios dados pessoais é constante no relacionamento da rede social online com seus usuários, e o modo com que este convite ao compartilhamento é realizado pode ser relevante para que se verifique se há, efetivamente, vontade livre e informada quanto aos efeitos deste compartilhamento no momento em que os dados pessoais são fornecidos[65].

Danilo Doneda afirma que as redes sociais, (i) além de serem um modelo de negócio que se torna viável justamente diante da possibilidade de monetização dos dados pessoais coletados, (ii) são, basicamente, uma ferramenta de tratamento de dados pessoais[66].

Neste sentido, Cíntia Rosa Pereira de Lima ensina que a monetização dos dados acaba por desencadear atuação desmedida dos agentes econômicos podendo causar danos aos usuários, veja-se:

---

[64] LISBOA, Roberto Senise. Proteção do Consumidor na Sociedade da Informação. Revista do Direito Privado da UEL, Londrina, v. 2, n. 1, p.1-27, jan/abr 2009. Quadrimestral. Disponível em: http://www.uel.br/revistas/direitoprivado/artigos/Roberto_Senise_Lisboa_Proteção_Consumidor_Sociedade_Informação.pdf. Acesso em: 11.mai.2016. p. 14.

[65] DONEDA, Danilo. *Reflexões sobre proteção de dados pessoais em redes sociais.* Universidad de los Andes. Facultad de Derecho (Bogotá, Colombia), No. 1 Julio. Diciembre de 2012. p. 11.

[66] DONEDA, Danilo. *A privacidade... Op. Cit*. p. 11.

> (...) destacam-se os desafios da economia informacional ensejados pelo aumento da capacidade de armazenamento de dados e pelo barateamento dos *hardwares* e *softwares*. De maneira que a monetarização dos dados faz com que os agentes econômicos atuem de maneira desmedida e, muitas vezes, causando danos aos usuários cujos dados pessoais são coletados e compartilhados sem conhecimento disto e sem prévio consentimento[67].

No mesmo sentido, Alessandro Hirata ensina que, a coleta, organização e classificação de dados (ainda que tais dados sejam públicos) para utilização em fins comerciais levam à importante questão de invasão de privacidade:

> Mesmo que esses dados sejam públicos, a sua coleta e posterior organização e classificação para a utilização em fins – comerciais, por exemplo – levam à importante questão sobre a invasão de privacidade. Vale lembrar ainda que tais dados, mesmo depois de apagados pelos usuários de redes sociais, permanecem sob controle dessas redes, que os armazenam para fins econômicos seus e de terceiros.[68]

Dessa forma, pode-se dizer que a monetização de dados pessoais, ou seja, a atribuição de valor monetário aos dados pessoais, se mostra como mais um obstáculo à proteção do chamado consumidor de vidro[69].

1.5. Neutralidade da rede

É interessante abordar o tema da neutralidade da rede apenas para que fique demonstrado que não é admitido, pela

---

[67] LIMA, Cíntia Rosa Pereira de. A imprescindibilidade... Op. Cit. p. 60. p. 40.
[68] HIRATA, Alessandro. *Op.Cit.*. p. 20.
[69] LACE, Suzane. *The Glass Consumer: life in a surveillance society*. Bristol: Policy Press, 2005.
A autora explica por qual motivo o consumidor é de vidro *"as organizações sabem tanto sobre os consumidores, que elas podem quase que ver através deles"*.

legislação nacional, o tratamento desigual dos conteúdos, *sites* e plataformas. A neutralidade da rede está prevista nos artigos 3º, IV e 9º do Marco Civil da Internet[70] e é considerada por alguns o grande trunfo do diploma legal, apesar de o tema ter sido abordado em outros instrumentos legais[71].

Tim Wu, considerado o pai da terminologia neutralidade da rede (*net neutrality*), define-a da seguinte forma:

> um princípio de *design* de rede, segundo o qual uma rede pública de utilidade máxima procura tratar os conteúdos, *sites* e plataformas de maneira igualitária. Isso permitiria que a rede transportasse todas as formas de informação e aceitasse todos os tipos de aplicações[72].

---

[70] Art. 3º. A disciplina do uso da internet no Brasil tem os seguintes princípios: (...) IV - preservação e garantia da neutralidade de rede;
Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.
§ 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:
I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e
II - priorização de serviços de emergência.
§ 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º, o responsável mencionado no caput deve:
I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei no 10.406, de 10 de janeiro de 2002 - Código Civil;
II - agir com proporcionalidade, transparência e isonomia;
III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e
IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.
§ 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

[71] Por exemplo, a Resolução n. 614 de 28.05.2013 - Art. 75. As Prestadoras de Serviço de Comunicação Multimídia devem respeitar a neutralidade de rede, conforme regulamentação, nos termos da legislação.

[72] WU, Tim. *Network Neutrality FAQ*. Disponível em http://www.timwu.org/network_neutrality.html. Acesso em 03.dez.2017. No original: "Network neutrality is best defined as a network design principle. The idea is that a maximally useful public information network aspires to treat all content, sites, and platforms equally. This allows the network to carry every form of information and support every kind of application. The principle suggests that information networks are often more valuable when they are less specialized – when they are a platform for multiple uses, present and future".

O princípio sugere que as redes de informação são muitas vezes mais valiosas quando menos especializadas, ou seja, quando são uma plataforma para múltiplos usos (presentes e futuros)[73].

Para Silvia Regina Barbuy Melchior, a neutralidade é o tratamento isonômico dado aos pacotes que transitam na internet e na infraestrutura de suporte. Assim, o tratamento de dados se dará *"de forma isonômica, independentemente de seu conteúdo, da sua origem ou destino, da aplicação ou do serviço acessado, tecnologia e padrões técnicos envolvidos"*[74].

O Marco Civil da Internet proíbe a filtragem ou privilégio de tráfego que poderia gerar acesso desigual ou discriminação (degradação ou priorização de determinados conteúdos, *sites* ou plataformas) sobre o tráfego da rede, bem como incentivo de práticas anticompetitivas (exemplo: quando o detentor da infraestrutura e rede que controla o acesso tem a habilidade de degradar o tráfego de serviços de concorrentes seus)[75].

Pode-se dizer que a neutralidade da rede proporciona um tráfego sem interferências, já que trata os conteudos, *sites* e plataformas de maneira igualitária, sem que possa haver discriminação. Dessa forma, fica evidente que a dinâmica da neutralidade é de extrema relevância para que a internet seja aquilo que se propôs a ser desde sua criação: livre.

De qualquer forma, deve-se ter em mente que, da maneira que está posta a internet — ainda não haja lei que determine o tratamento isonômico os "pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação" — a neutralidade não é uma realidade absoluta.

---

[73] *Idem*.
[74] MELCHIOR, Silvia Regina Barbuy. *Neutralidade no Direito Brasileiro. In: Marco Civil da Internet*; MASSO Fabiano Dolenc Del; ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurélio (coords.), São Paulo: Editora Revista dos Tribunais, 2014, p. 101.
[75] *Idem*. p. 102

1.6. Sistemas de formação de banco de dados e processamento de dados pessoais na internet

Os dados pessoais podem ser coletados das mais diversas formas. Porém, as principais fontes dos dados são: transações comerciais, censo e registros públicos, pesquisas de mercado e estilo de vida, sorteios, concursos, comercialização e cessão de dados e tecnologias de controle da internet, conforme Martin Evans[76]. Os dados coletados formam os chamados bancos de dados que "contêm dados inter-relacionados que podem ser compartilhados entre as várias partes de uma organização"[77].

Os *cookies* se configuram como uma das principais formas de coleta e circulação de dados pessoais utilizados pelas empresas na internet. De acordo com Martinez, trata-se de pequenos arquivos não executáveis que são capazes de enviar ao servidor do *site* o comportamento de quem o visita. [78]

Pode-se dizer que os *cookies* são "pequenos arquivos gravados pelo servidor no disco rígido do usuário, os quais armazenam informações sobre os hábitos do usuário, frequência de visitas a um determinado *site*, tipos de noticias que prefere etc."[79]. Em outras palavras, são marcadores digitais inseridos pelos *sites* visitados no dispositivo de navegação do usuário e que permitem a identificação e o armazenamento do histórico de navegação deste.

Zhou e Evans explicam que os *cookies* são usados como *tokens* de autenticação por quase todos os *sites* que exigem credenciais do usuário. Eles se caracterizam por serem uma forma de gerenciamento de informações dos usuários. [80]

Jegatheesen alerta que, apesar de ser uma ferramenta de uso comum pelas empresas como uma estratégia de *marketing*, os

---

[76] EVANS, Martin. The data informed marketing model and its social responsibility, In LACE, Susan. *The glass consumer... Op. Cit*. p. 103-104.

77 MANNINO, Michael V. Projeto, Desenvolvimento de Aplicações e Administração de Banco de Dados - 3ª ed. São Paulo: McGraw Hill Education, AMGH Editora Ltda., 2008. p. 20.

[78] MARTINEZ, Marina. Cookies. 2015, p. 1.

[79] TOMIZAWA, Guilherme. A invasão de privacidade através da internet. Curitiba: JM, 2008. p. 99.

[80] ZHOU, Yuchen; EVANS, David. Why aren't HTTP-only cookies more widely deployed. *Proceedings of 4th Web,* v. 2, 2010, p. 1.

cookies podem ser considerados facilmente como uma invasão de privacidade, com o compartilhamento ilícito de dados pessoais. De acordo com o autor, os *cookies* são considerados uma violação de segurança, já que a maioria dos *sites* não pede autorização do usuário para utilizá-los, e, por vezes, o usuário nem mesmo tem consciência de que suas informações e preferências estão sendo utilizadas[81].

Os *cookies* podem se apresentar em diferentes tipos, conforme se apresenta no quadro a seguir.

Tipo	**Descrição**
Cookies de persistência	Trata-se da forma tradicional do uso de *cookies*, podendo ficar mantidos no computador do usuário por dias, meses ou até anos, sendo capazes de armazenar conjunto de dados para uso posterior ou como forma de personalizar serviços, direcionando-os de acordo com o perfil dos usuários.
Cookies de sessão ou temporários	Semelhante ao *cookie* de persistência, sua diferença está no tempo de armazenamento, já que sua duração é proporcional ao tempo de navegação.
Cookies de primeira parte	Trata-se de mecanismos de manutenção da sessão ou de captura de informações pertencentes ao domínio que o usuário está diretamente visitando. Nesse tipo de *cookie,* há uma relação consciente entre usuário e *site*.
Cookies de terceiros	São *cookies* utilizados por *websites* que mantêm relação com o *site* utilizado pelo usuário, sendo criados e manipulados por provedores terceiros à relação estabelecida entre cliente e provedor.

O uso de *cookies*, para ser considerado lícito, deve ser previamente autorizado pelo usuário de forma expressa, tendo em vista que envolve seus dados pessoais, devendo-se citar os incisos II e III do artigo 3º do Marco Civil da Internet, que colocam a proteção à privacidade e aos dados pessoais como princípios a serem seguidos no uso da internet.

---

[81] JEGATHEESAN, Sowmyan. Cookies Invading Our Privacy for Marketing Advertising and Security Issues. *arXiv preprint arXiv:1305.2306*, 2013.

Os *cookies,* apesar de se configurarem como uma das principais formas de coleta de dados, não são a única, isto é, há outros métodos de coleta de dados para formação de bancos de dados que são posteriormente tratados para gerar informação. Existem diversas maneiras para tratar os dados coletados; algumas delas estão elencadas nos itens abaixo, de maneira não exaustiva.

1.6.1. *Data warehousing*

Data warehouse, expressão criada em 1990 por William Inmon, refere-se a um repositório central para dados no qual dados de bancos de dados operacionais e de outras fontes são integrados, limpos e padronizados para extração dos benefícios da junção dos dados[82].

Conforme lição de Laura Schertel Mendes[83], a expressão *data warehousing* denota a atividade de organizar dados de inúmeros sistemas operativos e heterogêneos, transformando-os e selecionando-os, com vistas a possibilitar a tomada de decisão estratégica pela empresa. Com isso, os dados coletados podem ser armazenados de acordo com critérios específicos.

A exploração desse repositório central pode ocorrer por inúmeras técnicas como, por exemplo, o *profiling* e o *data mining* que serão explicados abaixo (vide itens 1.6.2. e 1.6.3.).

1.6.2. *Data mining*

Uma outra técnica bastante utilizada é a do *data mining.* Ela consiste na busca de correlações, recorrências, formas, tendências e padrões significativos a partir de quantidades muito grandes de dados, com o auxilio de instrumentos estatísticos e matemáticos. Assim, a partir de uma grande quantidade de

---

[82] MANNINO, Michael V. *Op. Cit.* p. 554.
[83] MENDES, Laura Schertel. *Privacidade...Op. Cit.* p. 109.

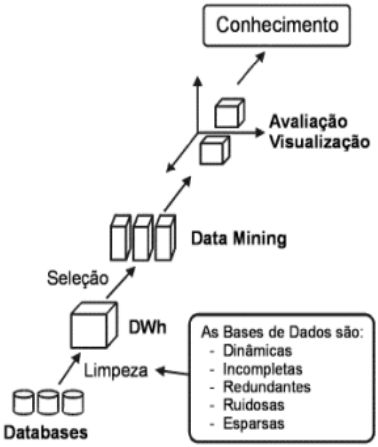
informação em estado bruto e não classificada podem ser identificadas informações de potencial interesse[84].

Como ensina Alessandro Hirata "*pode-se definir a mineração de dados como o processo de explorar grandes quantidades de dados à procura de padrões consistentes*"[85]. De acordo com Danilo Doneda[86] o *data mining* se configura como uma das técnicas de mineração de dados que rastreiam informações disponíveis na rede que possibilitam a construção de perfis com base no comportamento do usuário. Xu et al. [87] conceituam o *data mining* como o processo de descobrir padrões e conhecimentos interessantes de grandes quantidades de dados. No mesmo sentido, Usama Fayyad et. al. definem o *data mining* como sendo "o processo não-trivial de identificar, em dados, padrões válidos, novos, potencialmente úteis e ultimamente compreensíveis"[88].

Por meio de passos específicos, o processo de *data mining* consiste na técnica para descobrir padrões e, ao final, criar informação, conforme explica Sergio Navega[89] na imagem abaixo:

---

[84] DONEDA, Danilo. *A proteção de dados pessoais nas relações de consumo: para além da informação creditícia.* Escola Nacional de Defesa do Consumidor. Brasília: SPE/DPDC, 2010. p 34.
[85] HIRATA, Alessandro. *O Facebook ... Op. Cit.* p. 20.
[86] DONEDA, Danilo. *Da privacidade ... Op. Cit.,* p. 25.
[87] XU, Lei et al. Information security in big data: privacy and data mining. *IEEE Access,* v. 2, p. 1149-1176, 2014.
[88] FAYYAD Usama; Piatetski-Shapiro, Gregory; Smyth, Padhraic (1996) The KDD Process for Extracting Useful Knowledge from Volumes of Data. In: Communications of the ACM, pp.27-34, Nov.1996
[89] NAVEGA, Sérgio. Princípios essenciais do Data Mining. São Paulo, SP: 2002. Publicada nos Anais do Infoimagem, 2002.



Como pode se observar da imagem acima, o *data mining* utiliza-se de dados capturados e existentes nas bases de dados (que são dinâmicas, incompletas, redundantes, ruidosas e esparsas), e aplicam diversos algoritmos para processar os dados - criando informação para os analistas dos dados[90].

Sobre o assunto, Aldeen, Salleh e Razzaque[91] elucidam que a preservação da privacidade na mineração de dados surgiu como um pré-requisito absoluto para a troca de informações confidenciais em termos de análise, validação e publicação de dados.

Porém, ainda que tenha sido criada com o intuito da preservação da privacidade (aqui, entende-se proteção de dados pessoais também), resta claro que levando-se em conta que a qualidade das informações obtidas a partir do *data mining* cresce à medida em que aumenta a quantidade de informação disponível, pois a mineração dos dados será mais apurada a medida em que haja mais dados disponíveis, existe uma grave ameaça de propagação generalizada de informações na web.

---

[90] *Idem*

[91] ALDEEN YAAS, SALLEH M, RAZZAQUE MA. Uma revisão abrangente sobre privacidade preservando a mineração de dados. *SpringerPlus* 2015; 4: 694.

1.6.3. *Profiling*

Profiling se consubstancia na metodologia que cria um perfil do usuário da rede mundial de computadores, com base nos registros eletrônicos de hábitos de navegação associados a outras fontes de informação[92]. Trata-se basicamente de perfis dos usuários (criados, geralmente, a partir da mineração de dados) que são elaborados com base no seu comportamento na internet, isto é, o que o usuário visita, quanto tempo passa em navegação, suas preferências, enfim, o uso que faz na internet.

Louzada e Venturini elucidam que o *profiling* se configura como uma excelente prática para coletar e processar automaticamente informações sobre usuários. Por meio dela presumem-se as personalidades e interesses dos usuários, o que permite a quem analisa os dados prever comportamentos futuros: a chamada publicidade comportamental. A técnica do *profiling* é uma importante prática para as empresas, já que podem tomar essas informações como base para construção de propagandas personalizadas e no momento oportuno, o que traz vantagens para concretização de vendas. [93]

A partir do tratamento automatizado de dados e da criação de perfis (*profiling*) muitas vezes há verdadeira violação aos dados pessoais dos usuários e, ainda, sua própria autonomia.

Danilo Doneda ensina que o estabelecimento do perfil não é necessariamente um mal em si, podendo sê-lo caso o consumidor não tenha consciência sobre a criação do seu perfil de usuário:

> o estabelecimento de um perfil para um determinado consumidor não é, taxativamente,

---

[92] MONTEIRO, Renato Leite. *Da Proteção aos Registros, aos dados pessoais e às comunicações privadas*, *in* MASSO, Fabiano Del et. al. (coord.), Marco Civil Da Internet, São Paulo: Revista dos Tribunais, 2014, p. 141.

[93] LOUZADA, Luiza; VENTURINI, Jamila. A regulamentação de proteção de dados pessoais no Brasil e na Europa: uma análise comparativa. 2015. *3o Simpósio Internacional* LAVITS: Vigilância, Tecnopolíticas, Territórios. 13 à 15 de Maio, 2015. Rio de Janeiro, Brasil, p. 22- 39.

> um mal em si - muito embora apresente grande potencial para tornar-se um mal caso o consumidor não tenha consciência efetiva do que ocorre[94].

O que ocorre é que quando se cria um perfil do usuário, estão em jogo não somente aspectos da privacidade do consumidor, mas também da sua própria autonomia e liberdade de escolha, já que, a partir da criação de perfis são realizadas decisões automatizadas para esses indivíduos.

Como ensina Danilo Doneda, a perda de controle da pessoa sobre o que sabe em relação a ela mesma ocorre diuturnamente no contexto em que os dados pessoais passam a ser os intermediários entre a pessoa e a sociedade. Em última análise, a perda deste controle representa uma diminuição da própria liberdade[95]. Assim, o tratamento automatizado de dados pode imputar decisões automatizadas que, por sua vez, podem impactar a livre desenvolvimento da personalidade dos usuários da internet.

1.7. O grande banco de dados: *big data*

O *big data* não tem um conceito determinado, o que gera já uma dificuldade inicial sobre o tema. Doug Laney associa o *big data* a três "V's": volume, variedade e velocidade[96]. Classifica-o desta forma porque, em alta velocidade de processamento, o *big data* é capaz de organizar, em diversos formatos (dados de texto ou de uma foto, por exemplo) e em velocidade muito superior a uma base de dados comum, os dados coletados.

Em entendimento mais atualizado, considera-se que o *big data* possua cinco indicadores e não somente três, quais sejam: volume, velocidade, variedade, veracidade e valor, conforme propõe

---

[94] DONEDA, Danilo. *A proteção... Op. Cit.* p. 84
[95] DONEDA, Danilo. A proteção de dados pessoais nas relações de Op. Cit. p 84.
[96] LANEY, Doug. 3D Data Management: Controlling Data Volume, Velocity, and Variety. Disponível em https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf Acesso em 06.mar.2017.

Rijmenam[97]. Os últimos dois indicadores foram acrescentados porque (i) os dados deverão ser corretos, ou seja, corresponder à realidade para que tenham valor; e (ii) os dados disponíveis graças ao *big data* têm valor financeiro.

Conforme McKinsey Global Institute: "*B*ig data refere-se aos conjuntos de dados cujo tamanho está além da capacidade de ferramentas típicas de software de banco de dados para capturar, armazenar, gerenciar e analisar".

> O cardápio de *big data* é vasto e tende a crescer cada vez mais. Com a indústria aprimorando tecnologias e conquistando empresas de diferentes segmentos, os negócios têm grandes oportunidades de ganhar competitividade analisando seus dados e seus consumidores[98].

Manyka et. al destacam:

> A quantidade de dados do nosso mundo está explodindo. Empresas capturam trilhões de *bytes* de informações sobre seus clientes, fornecedores e funcionários, e milhões de sensores conectados estão sendo inseridos no mundo físico em aparelhos como celulares e automóveis, percebendo, criando e comunicando dados. Indivíduos com *smartphones* e em *sites* de redes sociais continuarão incrementando crescimento exponencial. *Big data* – grandes poços de dados que podem ser capturados, comunicados, agregados, armazenados e analisados – é agora parte de cada setor e função da economia global.[99]

---

[97] RIJMENAM, Mark van. Why The 3V's Are Not Sufficient To Describe Big Data. Disponível em https://datafloq.com/read/3vs-sufficient-describe-big-data/166 Acesso em 06.mar.2017.

[98] OLIVEIRA, Déborah. O Desafio de Garimpar Informações. 2013.. p. 17.

[99] MANYIKA, J., Chui,. M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H. *Big data: The next frontier for innovation, competition, and productivity.* McKinsey Global Institute. 2011, p. 4.

O *big data* é diferente dos demais tradicionais sistema de base de dados (como *data warehouse*), pois não há necessidade de prévia estruturação dos dados para sua análise e processamento. Neste sentido, veja-se o conteúdo na página da Microsoft[100]: os sistemas de banco de dados tradicionais geralmente usam um modelo relacional, em que todos os dados são armazenados usando esquemas predeterminados e vinculados, aplicando os valores em colunas específicas de cada tabela. Dessa forma, ao exigir um esquema predeterminado na coleta de dados, é possível que alguma informação escondida nos dados seja perdida.

Por outro lado, com o *big data*, é possível armazenar quase qualquer tipo de dados estruturados, semi-estruturados ou não estruturados e, em seguida, aplicar um esquema adequado quando se consultam esses dados. No *big data,* os dados são armazenados em seu formato bruto e aplica-se um esquema somente quando os dados são lidos, o que preserva toda a informação dentro dos dados.

Além disso, os sistemas de banco de dados tradicionais geralmente consistem em um nó central onde todo o processamento ocorre, o que significa que todos os dados do armazenamento devem ser movidos para a localização central para processamento. A capacidade desse nó central pode ser aumentada e existe uma limitação física no número de CPUs (*central processing unit*; em português: unidade central de processamento) e memória, dependendo da plataforma de *hardware* escolhida. A consequência disso é uma limitação da capacidade de processamento, bem como a latência da rede quando os dados são movidos para o nó central.

O *big data* é capaz de armazenar grandes quantidades de dados usando formatos de arquivos simples e mecanismos de armazenamento altamente distribuídos, e o processamento inicial dos dados ocorre em cada nó de armazenamento. Da maneira como está estruturado o *big data*, os dados são analisados em toda a sua extensão — não por amostra ou em pequenas quantidades. Com tal configuração, o *big data* é capaz de armazenar quantias inimagináveis de dados. Neste sentido, explica Ariano:

---

[100]MICROSOFT, *Why should I care about big data?* Disponível em https://msdn.microsoft.com/pt-br/library/dn749785.aspx Acesso em 06.mar.2017.

> Conforme a utilização das mídias sociais aumenta, a quantidade de informações geradas por redes sociais como Facebook, Pinterest e Twitter também aumenta consideravelmente. O conjunto crescente de informações gerado e armazenado por elas numa velocidade estrondosa pode ser considerado um exemplo de *big data*[101].

Por tal razão, como ensina Bruno Bioni, tornou-se possível correlacionar uma "série de fatos (dados), estabelecendo entre eles uma relação para desvendar padrões, inferindo-se probabilidades de acontecimentos futuros"[102].

O autor continua afirmando que, diferentemente do que se pensa, o *big data* não é um sistema inteligente, pois não se trata de ensinar o computador a pensar como um humano, mas apenas uma nova ferramenta que processa e organiza os dados para inferir a ocorrência de acontecimentos. Por meio da relação estabelecida entre fatos (dados fornecidos pelo usuário em sua atividade na internet), é que se revela um padrão, ou seja, é a recorrência de um evento a ponto de se permitir prever que ele se repetirá no futuro.

Com tamanha movimentação e coleta de dados, os indivíduos encontram-se mais desprotegidos do que anteriormente em relação à proteção de seus dados pessoais. Conforme ensina Cíntia Rosa Pereira de Lima, há propostas de três medidas para proteção dos dados pessoais, quais sejam: 1) consentimento informado do indivíduo (aquele livre e informado, em que há plena ciência e concordância com a coleta de dados); 2) sistema *opt out,* que viabiliza a exclusão dos dados quando solicitado por seu titular; e 3) anonimização de dados, ou seja, a utilização de meios que impossibilitem associar os dados a um indivíduo[103].

---

[101] ARIANO, Erica. Descubra como o Big Data tem influenciado as mídias sociais. Disponível em http://www.ideiademarketing.com.br/2013/11/15/descubra-como-o-big-data-tem-influenciado-as-midias-sociais/ Acesso 06.mar.2018.

[102] BIONI, Bruno. *Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet.* Dissertação (Mestrado), Faculdade de Direito, Universidade de São Paulo, São Paulo, 2016. p. 59.

[103] LIMA, Cíntia Rosa Pereira de. *A imprescindibilidade... Op. Cit.* p. 50.

Para Lima, as três medidas não passam de uma falácia, já que nenhuma delas garante verdadeiramente a proteção de dados pessoais; veja-se:

> Contudo, tais medidas não nos parecem suficientes. Primeiro porque o consentimento, que deve ser livre e informado, não o é, tendo em vista os longos termos e condições utilizados pelas grandes empresas que inviabilizam o real conhecimento pelos indivíduos que anuem sem saber ao certo com o quê.
> Segundo porque o sistema *opt out*, muitas vezes, é utilizado justamente para continuar rastreando as atividades dos indivíduos.
> E, terceiro, porque já é cediço que a anonimização de dados na economia informacional é uma falácia já que é possível, através de associações e tratamento de dados, partir de um dado anônimo e chegar a informações pessoais que revelem opção sexual, filiação partidária, convicções religiosas etc[104].

Em resumo, no big data os dados são coletados indiscriminadamente — sem que se dê conta do motivo pelo qual um determinado evento ocorre —, há apenas a absorção dos dados para o conjunto de maneira indiscriminada. Com isso, calcula-se a possibilidade de um determinado evento ocorrer, com base no que ocorreu. Não há uma análise causal, portanto. Conforme afirmam Mayer-Schonberger e Cukier,[105] "*big data does not tell us anything about causality*". Há um diagnóstico apenas do que está acontecendo e não das razões pelas quais um determinado evento ou uma cadeia de eventos está ocorrendo.

---

[104] *Idem* p. 50-*51*.
[105] *Ibidem.* p. 163.

CAPÍTULO 2: O TRATAMENTO AUTOMATIZADO E A PROTEÇÃO DE DADOS PESSOAIS NA INTERNET

2.1. Panorama geral do direito à proteção de dados pessoais

A Constituição Federal de 1988 garante, em seu artigo 5º, inciso XII, a "*inviolabilidade do sigilo da correspondência, comunicações telegráficas, de dados e das comunicações telefônicas*". Originariamente, tal garantia foi expressa na Constituição como forma de proteção do indivíduo ante as arbitrariedades do Estado na condução de investigações, calcadas em fundamentos ideológicos, como forma de manter governos autoritários.

Considerando o contexto histórico da edição da norma supramencionada, não há guarida explícita ao direito fundamental à proteção de dados pessoais na internet nem na Constituição Federal nem no Código Civil. No entanto, a doutrina e os tribunais pátrios, pacificamente, entendem que o rol de direitos fundamentais é apenas exemplificativo, amparado pelo Estado Democrático de Direito. Por análise do caso concreto e mediante sopesamento dos valores inerentes à sociedade em um dado tempo e lugar, pode-se determinar quais são os novos direitos.

Modernamente, o direito à proteção de dados pessoais, apesar de não positivado na Constituição Federal ou no Código Civil, tem sido alçado à categoria de direito da personalidade, de forma independente do direito à privacidade. Ademais, com a aprovação do Marco Civil da Internet, houve positivação do direito à proteção de dados no artigo 3º, III.

Desta forma, não restam dúvidas de que o direito à proteção de dados é um dos direitos da personalidade. Conforme ensina Danilo Doneda, a privacidade mantém íntima relação com a proteção de dados pessoais, na medida em que "*a proteção de dados pessoais, em suma, propõe o tema da privacidade, porém modifica seus elementos; aprofunda seus postulados e toca nos pontos centrais dos interesses em questão*"[106]. Porém, entende-se que são

[106] DONEDA, Danilo. *Op. Cit*., p. 205.

direitos distintos os da privacidade e da proteção de dados pessoais, conforme será demonstrado.

A palavra privacidade não possui um conceito único e objetivo; sendo assim, há vários posicionamentos doutrinários quanto ao seu significado. Rodotà ensina que o reconhecimento dos direitos da personalidade (incluindo o direito à privacidade) têm seu fundamento no direito à propriedade. Assim, em suas palavras, o direito à privacidade é uma consequência óbvia da estrutura geral dos sistemas jurídicos burgueses, em que o reconhecimento formal dos direitos da personalidade se traduz principalmente na garantia acentuada da propriedade, entendida como a projeção máxima dos direitos individuais da liberdade. E continua, afirmando que o privilégio concedido à informação econômica, em termos de sigilo, é precisamente um instrumento que fortalece a posição de donos e empresários, despojados de controles contínuos e substantivos pela comunidade.[107]

O direito à privacidade, assim como os demais direitos fundamentais, possui caráter eminentemente elástico e variável, conforme o tempo, o espaço e o titular da garantia. O doutrinador Sergio Niger ensina que, na antiguidade grega, a privação da "privacidade" na própria palavra era considerada predominante. Isso significava:

> um estado de privação que poderia tocar em faculdades ainda maiores e mais humanas. Um homem que vivesse apenas uma vida privada e que, como o escravo, não pudesse acessar a esfera pública, ou que, como o bárbaro, optou por não estabelecendo tal domínio, não era totalmente humano. (Tradução livre).

---

[107] RODOTÁ, Stefano. *Il terribile diritto, studi sulla proprietà privata,* Il Mulino: Bologna, 1981, p. 31.
"(...) di una unicamente conseguenza ovvia della struttura complessiva dei sistemi giuridici borghesi, nei quali il riconoscimento formale dei diritti della personalità si è prevalentemente tradotto nella garanzia accentuata della proprietà, intesa appunto come la massima proiezione dei diritti individuali di libertà. Il privilegio accordato alle informazioni economiche, sotto il profilo della segretezza, costituisce appunto uno strumento che rafforza la posizione di proprietari e imprenditori, cosi sottratti a continui e sostanziali controlli da parte della collettività."

A "privacidade", portanto, literalmente constituiu uma privação, separação da esfera mais importante da vida humana: a pública. Em Atenas, a esfera pública foi incorporada em eclésia ou assembleia de todos os cidadãos masculinos livres. No entanto, como já foi referido acima, entrar na arena pública também requeria do indivíduo que fosse proprietário (de casa), o que possibilitou a "vida privada"[108].

Em 1953, uma teoria, chamada de teoria dos círculos concêntricos da esfera da vida privada (ou Teoria das Esferas da Personalidade), foi elaborada pelos alemães Heinrich Hubmann e Heinrich Henkel[109].

Tal teoria preconiza a existência de três níveis distintos de proteção da vida privada. São três círculos concêntricos que tratam da privacidade de forma ampla: o círculo da vida privada em sentido estrito, o círculo da intimidade e, no meio, o círculo do segredo. Isso levando em consideração que o direito à privacidade seria aquele que possibilita ao seu titular reservar sua própria vivência para si mesmo e também possibilita que controle quais membros da sociedade terão ou não acesso a ela.

A respeito da teoria dos círculos concêntricos, Sônia Vieira ensina, de forma resumida, que:

> Por esta teoria, as esferas individual e privada integram a vida privada. A esfera individual, responsável pela proteção à honra, tem como manifestações mais importantes o direito ao nome e a reputação. A esfera privada tem por

---

[108] NIGER, Sergio. *Le Nuove Dimensioni Della Privacy: Dal Diritto Alla Riservatezza Alla Protezione Dei Dati Personali,* Padova: Cedam, 2006, p. 3.
"Nell'antichità greca, quindi, l'aspetto deprivazione della "privacy" presente nella parola stessa, era ritenuto predominante. Significava letteralmente uno stato di privazione che poteva toccare anche facoltà più alte e più umane. Un uomo che vivesse solo una vita privata e che, come lo schiavo, non potesse accedere alla sfera pubblica o che, come il barbaro, avesse scelto di non istituire un tale dominio, non era pienamente umano".
La "privacy", quindi, costituiva letteralmente una privazione, la separazioni dall'ambito più importante della vita umana: quello pubblico. Ad Atene la sfera pubblica si incarnava nell'ecclesia o assemblea di tutti i cittadini maschi liberi. Tuttavia, come già evidenziato in precedenza, per scendere nell'arena pubblica occorreva anche essere proprietari di beni (casa), condizione che rendeva possibile la "vita privata", ossia appartarsi.
[109] HUBMANN, Heinrich. *Das persönlichkeitsrecht*. Münster: Böhlau-Verlag, 1953.

> objetivo a proteção contra a indiscrição. Na esfera individual o cidadão do mundo acha-se relacionado com seus semelhantes; na esfera privada, ao contrário, o cidadão acha-se na intimidade ou no recato, em seu isolamento moral, convivendo com a própria individualidade[110].

Nesse sentido, Paulo José da Costa Jr. preleciona que a esfera mais externa seria a esfera privada *stricto senso* (*Privatsphäre*): "*nela estão compreendidos todos aqueles comportamentos e acontecimentos que o indivíduo não quer que se tornem do domínio público*"[111].

Dessa forma, o círculo mais amplo diz respeito à vida privada em sentido estrito, em que repousam as relações interpessoais mais rasas, nas quais não há um amplo grau de conhecimento da vida alheia. Nessa situação, ainda que o acesso ao público seja restrito, seu grau de limitações é o menor dentre as três esferas.

Assim, o interesse público pode ser motivo plausível para sua violação. É neste círculo que repousa, por exemplo, o sigilo de dados telefônicos (acesso à relação de ligações efetuadas e recebidas), que pode ser quebrado pelo Poder Judiciário ou por Comissão Parlamentar de Inquérito. Nesta esfera, encontram-se os episódios de natureza pública que envolvam o indivíduo, extensíveis a um círculo indeterminado de pessoas.

O círculo do meio, ou a segunda esfera, seria a da intimidade (*Vertrauensphäre/Vertrauensphäre*). Dela participam aquelas pessoas nas quais o indivíduo deposita certa confiança e mantém amizade: "*Fazem parte desse campo conversações ou acontecimentos íntimos, dele estando excluídos não só o* quivis ex populo*, como muitos membros que chegam a integrar a esfera pessoal do titular do direito à intimidade*"[112].

---

[110] VIEIRA, Sônia Aguiar do Amaral. Inviolabilidade da vida privada e da intimidade pelos meios de comunicação. São Paulo: Juarez de Oliveira, 2002. p. 17.
[111] COSTA JR., Paulo José da. *O direito de estar só: tutela penal da intimidade*. 2ª ed. São Paulo: Revista dos Tribunais, 1995. p. 29.
[112] *Idem.* p. 30.

Em outras palavras, neste círculo estão incluídas as informações mais restritas sobre o ser humano, compartilhadas com reduzido número de pessoas de seu ambiente familiar, amigos íntimos e profissionais que têm conhecimento das informações em razão do ofício (a exemplo de psicólogos, padres e advogados).

É neste círculo que se encontram protegidos o sigilo domiciliar, profissional e das comunicações telefônicas (i.e., "grampo"), que sofrem restrições mais agudas para sua exposição, a exemplo da última, cuja quebra só pode ser decretada por decisão judicial fundamentada.

Por derradeiro, temos a esfera do segredo (*Geheimsphäre*):

> (…) ela compreende aquela parcela da vida particular que é conservada em segredo pelo indivíduo, do qual compartilham uns poucos amigos, muito chegados. Dessa esfera não participam sequer pessoas da intimidade do sujeito. Consequentemente, a necessidade de proteção legal contra a indiscrição, nessa esfera, faz-se sentir muito mais intensa[113].

Por fim, o segredo é o círculo mais restrito das esferas da privacidade *lato sensu,* no qual são guardadas as informações mais íntimas do indivíduo, que, muitas vezes, não são compartilhadas com outros indivíduos e sobre as quais o interesse público não poderá se imiscuir, a exemplo da opção sexual, filosófica e religiosa.

Em complementação, Rodotà ensina que a privacidade hoje não se baseia mais no eixo "pessoa – informação – segredo", mas sim no eixo "pessoa – informação – circulação – controle".[114]

---

[113] *Ibidem.* p. 31.

[114] RODOTÀ, Stefano. *Tecnologie e diritti,* Bologna: Il Mulino, 1995, p. 102. No original: "Nel diritto al rispetto alla vita privata e familiare si manifesta soprattutto il momento individualistico, il potere si esaurisce sostanzialmente nell'escludere interferenze altrui: la tutela è statica, negativa. La protezione dei dati, invece, fissa regole sulle modalità del trattamento dei dati, si concretizza in poteri di intervento: la tutela è dinamica, segue i dati nella loro circolazione. (...) Si evidenzia bene qui il punto d'arrivo di una lunga evoluzione del concetto di *privacy*, dall'originaria definizione come diritto ad essere lasciati soli fino al diritto

Dessa forma, o direito à privacidade não pode mais ser compreendido unicamente como o direto de ser deixado em paz (liberdade negativa), mas sim como a possibilidade de obter controle da própria vida privada (liberdade positiva).

Neste sentido, o autor ensina que, no direito à vida privada e familiar, manifesta-se o momento individualista; o poder do indivíduo é amplamente exaurido pela exclusão da interferência dos outros: a proteção é estática, negativa.

A proteção de dados, por outro lado, estabelece regras sobre como os dados são processados. O indivíduo está no poder da intervenção: a proteção dos dados é dinâmica, ou seja, segue os dados em sua circulação. O ponto aqui é a longa evolução do conceito de privacidade, desde a definição original, como o direito de ser deixado sozinho, até o direito de manter o controle de suas informações e de determinar as formas de construir sua própria esfera[115].

Conclui-se que a privacidade diz respeito aos aspectos mais ocultos do indivíduo, resguardando as informações pessoais, dentre as quais algumas podem tocar o interesse público (intimidade), e outras dizem respeito exclusivamente ao titular (segredo). Portanto, à medida que a informação está mais próxima do centro do círculo, maior a proteção de acordo com a doutrina alemã. Apesar de estar positivada na Constituição Federal a proteção à intimidade, não se nota a diferença conceitual da teoria dos círculos concêntricos.

Nada obstante à proteção de dados pessoais estar próxima ao conceito de privacidade, eles não se confundem. A privacidade está relacionada com a informação pessoal, pois, quanto maior o grau de privacidade, menor a difusão de dados pessoais e vice-versa. Ainda assim, por não se confundirem, pode-se dizer que a privacidade, em decorrência do seu caráter amplo, muitas vezes leva a uma dificuldade de elaboração de uma resposta clara, harmônica e rápida aos problemas relacionados à sua violação.

---

a mantenere il controllo delle proprie informazioni e di determinare le modalità della costruzione della propria sfera privata.

[115] RODOTÀ, Stefano. *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice della privacy*. In Europa e diritto privato, 2004, 1-11. p. 3.

Neste sentido, há quem diga que, por não ter "nada a esconder", a privacidade talvez seja um direito não tão importante, que deve ser mitigado para justificar a segurança nacional e a chamada "guerra ao terror". Porém, Daniel Solove ensina que tal colocação não se verifica, pois parte de falsas assunções sobre a privacidade e seus valores. O autor nos ensina que

> o argumento do "nada para esconder" fala a alguns problemas, mas não aos outros. Na verdade, ele representa uma forma singular e estreita de conceber a privacidade, e acaba ganhando por excluir outros problemas (muitas vezes, levantados em programas de vigilância governamental e de *data mining)*. Quando encarado de forma direta, o argumento do "nada a esconder" pode se mostrar convincente, pois o debate fica concentrado unicamente em sua compreensão estreita da privacidade. Mas, quando confrontado com a pluralidade de questões de privacidade envolvidas pela coleta de dados do governo e seu uso além da vigilância e divulgação, o argumento do "nada para esconder", no final, não acrescenta nada (tradução livre).[116]

A proteção de dados pessoais, enquanto direito individual, por outro lado, tem um caráter mais objetivo, pois ela visa proteger o dado em si e, por meio dele, a pessoa, o que acaba facilitando o trabalho do julgador. O direito à proteção de dados pessoais foi definido na Convenção 108 do Conselho da Europa: "informação pessoal é qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação"[117]. De acordo

---

[116] SOLOVE, Daniel J., *I've Got Nothing to Hide and Other Misunderstandings of Privacy.* George Washington University Law School, 44 San Diego L. Rev. 745 (2007), p. 772. No original: "The nothing to hide argument speaks to some problems, but not to others. It represents a singular and narrow way of conceiving of privacy, and it wins by excluding consideration of the other problems often raised in government surveillance and data mining programs. When engaged with directly, the nothing to hide argument can ensnare, for it forces the debate to focus on its narrow understanding of privacy. But when confronted with the plurality of privacy problems implicated by government data collection and use beyond surveillance and disclosure, the nothing to hide argument, in the end, has nothing to say

[117] UE, Convenção nº 108 – Convenção para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais, de 28 de janeiro de 1981.

com a Diretiva 2016/680, atualmente em vigor, "*os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável*"[118].

O Marco Civil da Internet também garante a proteção aos dados pessoais em seu artigo 3º, III. O desenvolvimento da proteção de dados pessoais como um direito da personalidade autônomo, com instrumentos legais de proteção próprios, fornece maior garantia de proteção aos dados pessoais e demonstra como tal instituto vai além da sua caracterização como proteção à privacidade.

Deve-se observar que a proteção de dados pessoais, consubstanciada na garantia de controle do indivíduo sobre as próprias informações, é uma característica generalizada das diversas legislações sobre o tema. A expressão "autodeterminação informativa" [119] (ou autodeterminação informacional[120]), consolidada no direito alemão ("liberdade informática" no direito espanhol), demonstra a importância que alcançou a proteção de dados pessoais.

Nas palavras do doutrinador de Perez Luño, a liberdade informática tem aspectos positivo e negativo (como mencionado acima)[121]. O autor afirma que a liberdade informática, assim como a liberdade política, apresenta dois aspectos: um é o aspecto negativo que se traduz no direito de manter privadas de domínio público informações de caráter pessoal, privado o reservado; o outro é o positivo, implica no exercício do direito ao controle dos dados pessoais que ultrapassam a esfera da privacidade para compor elementos do *input* de um programa eletrônico.

---

[118] UE, Diretiva n. 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[119] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, Rio de Janeiro: Renovar, 2006, p. 211: "A autodeterminação informativa, de fato, surgiu basicamente como uma extensão das liberdades presentes nas leis de segunda geração, e são várias as mudanças específicas nesse sentido que podem ser identificadas na estrutura destas novas leis. O tratamento dos dados pessoais era visto como um processo, que não se encerrava na simples permissão ou não da pessoa para a utilização de seus dados pessoais, porém procurava fazer com que a pessoa participasse consciente e ativamente nas fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros; estas leis incluem também garantias específicas, como o dever de informação".

[120] BIONI, Bruno. *Autodeterminação informacional… Op. Cit.*

[121] PÉREZ LUÑO, Antonio-Enrique, *Informática y Libertad. Comentario al Artículo 18.4 de la Constitución Española.* In: Revista de Estudios Políticos (Nueva Época), nº 24, pág. 4, Centro de Estudios Constitucionales, Madrid, 1981.

A liberdade informática em sua acepção positiva, portanto, é estranha ao reconhecimento do direito a conhecer, corrigir, cancelar ou adicionar dados em uma ficha pessoal contida em um registro informático.

> Deve-se ter em mente que, na prática, os aspectos negativo e positivo da liberdade informática são complementares, já que o exercício pleno deste direito consiste na faculdade de intervir nos bancos de dados não apenas para limitar o uso dos dados, proibindo sua difusão, mas também para construir uma atividade de inspeção, verificação ou cancelamento. No que se verifica uma correspondência com o direito de solicitar a retificação na informação publicada nos meios de comunicação[122].

Pérez Luño também afirma que os direitos fundamentais diretamente relacionados com a personalidade da pessoa (como honra, nome, imagem, privacidade, intimidade) não podem ser vistos como categorias estanques devendo ser tutelados a partir de uma perspectiva exclusiva, sempre que houver necessidade.

No caso dos dados pessoais, há necessidade de uma proteção que considere as interações e conexões sociais do seu titular. Expõe-se, portanto, a necessidade de se reconhecer o direito à

---

[122] PÉREZ LUÑO, Antonio-Enrique. Derechos humanos, Estado de Derecho y Constitución. 9. ed. Madri: Editorial Tecnos, 2005, p. 339.
No original: *"En efecto, como acertadamente se ha puesto en evidencia, la libertad informática, al igual que la libertad política, presenta dos aspectos: uno, es de significación negativa y se traduce en el derecho a no hacer de dominio público ciertas informaciones de carácter personal, privado o reservado; el otro, es positivo e implica el ejercicio de un derecho al control de los datos concernientes a la propia persona que han rebasado la esfera de la privacy para devenir elementos del input de un programa electrónico. La libertad informática en su aceptación positiva entraña, por tanto, el reconocimiento del derecho a conocer, corregir, cancelar o añadir datos en una ficha personal contenida en un registro informático. Si bien, debe tenerse presente que en la práctica ambos aspectos negativo y positivo de la libertad informática son complementarios, ya que el ejercicio pleno de este derecho consiste en la facultad de intervenir sobre los bancos de datos no sólo para limitar su uso prohibiendo la difusión de sus informaciones, sino también para desarrollar una actividad de inspección, verificación o cancelación, en la que se ha visto una correspondencia con lo que supone el derecho a la rectificación en las informaciones publicadas en los medios de comunicación".*

autodeterminação informativa, como uma categoria de direito fundamental[123], como se verá posteriormente.

A captação automatizada de dados pessoais do usuário, para as mais amplas atividades, ocorre durante quase todo o período de acesso deste à internet, seja por meio de redes sociais, ferramentas de pesquisa ou *sites* de compartilhamento de informações, o que torna tal atividade uma atividade de risco. Este risco se revela na possibilidade de tais dados pessoais serem expostos ou utilizados de forma indevida ou abusiva, ou ainda, na sua incorreção, caracterizando uma representação em desacordo com a realidade do seu titular.

Diante de tal situação, se mostra necessário o uso de mecanismos que possibilitem que o titular dos dados tenha controle sobre quais dados a seu respeito são captados e de que forma tais dados serão usados (seja para pesquisa de *marketing*, traçar perfil do cliente, venda de dados para terceiros). Dados pessoais são expressão direta da personalidade do indivíduo, e, por isso, a proteção de dados é considerada um direito e instrumento para proteção da pessoa humana.

2.1.1. Proteção de dados pessoais antes do Marco Civil da Internet

Na Constituição Federal há reconhecimento do direito geral à intimidade e à vida privada, explicitado por disposições que modificaram o sistema de proteção dos direitos fundamentais, especialmente o direito à intimidade[124]. Os incisos X, e XIII do artigo 5º da Constituição Federal trazem indiretamente disposições sobre dados pessoais

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à

---

[123] *Idem.* p. 339.
[124] SAMPAIO, José Adércio Leite. Direito à intimidade e a 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. 478.

> liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> (...)
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> (...)
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Verifica-se que a Constituição trata de proteção de dados ao tratar do direito fundamental à intimidade, estabelecendo a inviolabilidade dos dados. Mais adiante, no artigo 5º do texto constitucional, surge a possibilidade de defesa dos dados por meio do *habeas data, n*o art. 5º LXXII. Tal ação garante o conhecimento de informações relativas ao indivíduo, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, bem como a retificação de dados.

A esse respeito, ensinam Antônia Klee e Guilherme Martins:

> O habeas data tem por objeto a proteção dos indivíduos contra: a) os usos abusivos e nocivos de registros pessoais coletados por meios fraudulentos, desleais ou ilícitos; b) a introdução dos dados sensíveis nos registros; c) a conservação de dados falsos ou com fins diversos dos autorizados em lei [125].

---

[125] KLEE, Antônia Espínola Longoni e 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. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira. Direito e Internet III: Marco Civil da Internet III – tomo II. São Paulo: Quartier Latin, 2015, p. 291.

Posteriormente, o *habeas data* foi regulamentado pela Lei 9.507/1997 (Lei de Acesso à Informação), que disciplina o seu rito processual e regula o direito de acesso à informação dos indivíduos.

Logo no paragrafo único do art. 1º da Lei 9.507/1997, é definido como de caráter publico "*todo o registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam do uso privativo do órgão ou entidade produtora ou depositária das informações*".

Também em vigência, a Lei 9.296/96 trata da interceptação de comunicações telefônicas. A lei aborda, inclusive da interceptação do fluxo de comunicações em sistemas de informática e telemática para prova em investigação criminal e em instrução processual penal. A interceptação dependerá de ordem judicial, sob segredo de justiça e em autos apartados[126].

Após a exposição de fotos íntimas da atriz Carolina Dieckmann, foi aprovada a Lei 12.737/2012 que criminaliza a violação de dispositivos informáticos com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita[127].

Outro dispositivo infraconstitucional que trata de dados pessoais é a Lei do Cadastro Positivo, Lei 12.414/2011. Ela foi criada para disciplinar a formação de banco de dados formados sob um conjunto relativo a operações financeiras e de adimplemento para fins de concessão de crédito. Em seu texto, há regras específicas sobre a formação e consulta a bancos de dados com informações de

---

[126] Art. 1º. A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. Parágrafo único: O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.
Art. 8°. A interceptação de comunicação telefônica, de qualquer natureza, ocorrerá em autos apartados, apensados aos autos do inquérito policial ou do processo criminal, preservando-se o sigilo das diligências, gravações e transcrições respectivas

[127] Art. 154 - A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, veja-se:

> Art. 2º Para os efeitos desta Lei, considera-se:
>
> I - banco de dados: conjunto de dados relativo a pessoa natural ou jurídica armazenados com a finalidade de subsidiar a concessão de crédito, a realização de venda a prazo ou de outras transações comerciais e empresariais que impliquem risco financeiro;
>
> Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei.
>
> (...)
>
> § 3º Ficam proibidas as anotações de:
>
> I - informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e
>
> II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

Da mesma forma, o Código de Defesa do Consumidor apresenta proteção aos dados pessoais dos consumidores, criando regras sobre como os cadastros dos consumidores devem ser feitos, qual o direito ao acesso às informações desses cadastros, bem como possibilidade de correção nos dados:

> 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.
>
> § 1º 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.
>
> § 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
>
> § 3º 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.

Há, ainda, o Decreto 7.962 de 2013, que regulamenta o Código de Defesa do Consumidor para dispor sobre a contratação no meio eletrônico. Estabelece que as informações devem ser claras, o atendimento facilitado ao consumidor e o direito de arrependimento deve ser respeitado. Dispõe ainda que os dados do consumidor deverão ser tratados de forma segura e eficaz:

> Art. 3º Os sítios eletrônicos ou demais meios eletrônicos utilizados para ofertas de compras coletivas ou modalidades análogas de contratação deverão conter, além das informações previstas no art. 2º as seguintes:
> (...)
> VII - utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor.

O Código Civil, como mencionado acima, não se concentra no tratamento de dados pessoais, porém traz disposições relativas à proteção da imagem e intimidade em seus artigos 20 e 21. Assim, apesar de os dados pessoais não serem abordados de forma explicita, pode-se dizer o Código Civil poderá ser usado em situações em que haja violação à proteção de dados pessoais, já que elas, muitas vezes, vêm acompanhadas de violações à imagem e à intimidade.

> Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.
>
> Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

Outra questão que resvala na discussão proposta no presente trabalho são as biografias não autorizadas. A esse respeito, o Plenário do Supremo Tribunal Federal julgou, por unanimidade, procedente a Ação Direta de Inconstitucionalidade (ADI) 4815 e declarou inexigível a autorização prévia para a publicação de biografias[128].

---

[128] A ministra Cármen Lúcia utilizou o instituto da interpretação conforme a Constituição da República em relação aos artigos 20 e 21 do Código Civil, em consonância com os direitos fundamentais à liberdade de expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença de pessoa biografada, relativamente a obras biográficas literárias ou audiovisuais (ou de seus familiares, em caso de pessoas falecidas).

Por fim, interessante anotar a decisão do Superior Tribunal de Justiça que declarou não existir uma garantia constitucional de inviolabilidade dos dados registrados em um computador (*Habeas Corpus* 83.168-1, Ministro Relator Sepúlveda Pertence, data do julgamento 02.02.2007). O Ministro afirmou, em sua decisão, que não houve violação ao art. 5º, XII da Constituição porque "*não houve quebra do sigilo das comunicações de dados (interceptação das comunicações), mas sim a apreensão da base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial*".

A opinião do relator, seguida por maioria, é de que o inciso XII protegeria a inviolabilidade e o sigilo da comunicação dos dados, mas não os dados em si. A decisão foi proferida com base nos seguintes ensinamentos de Tércio Sampaio Ferraz:

> A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação[129].

Em conclusão, pode-se observar que há necessidade latente de lei única para tratar todos os assuntos relacionados à proteção de dados, bem como a revogação das demais, especialmente as relacionadas ao direito privado, para que seja diminuída a confusão na orientação dos consumidores.

Na ADI 4815, a Associação Nacional dos Editores de Livros (ANEL) sustentava que os artigos 20 e 21 do Código Civil conteriam regras incompatíveis com a liberdade de expressão e de informação.

A ministra Cármen Lúcia destacou que a Constituição prevê, nos casos de violação da privacidade, da intimidade, da honra e da imagem, a reparação indenizatória, e proíbe "*toda e qualquer censura de natureza política, ideológica e artística"*. Assim, uma regra infraconstitucional (Código Civil) não pode abolir o direito de expressão e criação de obras literárias. "*Não é proibindo, recolhendo obras ou impedindo sua circulação, calando-se a palavra e amordaçando a história que se consegue cumprir a Constituição"*, afirmou. *"A norma infraconstitucional não pode amesquinhar preceitos constitucionais, impondo restrições ao exercício de liberdades*".

[129] FERRAZ, Tércio Sampaio. *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito do Estado de São Paulo,* vol.88, 1993, p. 447e

2.1.2. Proteção de Dados na União Europeia

Antes de voltarmos ao Brasil para falar do Marco Civil da Internet, é interessante, neste momento, traçar um ligeiro perfil da proteção de dados na Europa. Inicialmente, surgiu na Alemanha, em 1970, a Lei de Hesse, a primeira lei sobre o assunto. Posteriormente, em 1977, foi aprovado o Ato Federal de Proteção de Dados na Alemanha (chamada *Bundesdatenschutzgesetz*, BDSG), para muitos, a mais importante lei de proteção aos dados pessoais. Essa lei sofreu alterações, mas traçou um perfil inicial no mundo a respeito da proteção de dados pessoais.

Em 1973, a Suécia implementou uma lei de proteção de dados pessoais, seguida das leis da Dinamarca, Áustria, França, Noruega e Luxemburgo, todas em 1978. Esse momento da década de 70 é nomeado por Mayer-Schönberger como a primeira geração de normas de proteção de dados pessoais. Elas surgem para limitar a atuação da administração pública e das empresas privadas na criação de bancos de dados e seu processamento eletrônico.[130] Nesse aspecto, o autor comenta que diversas leis dessa década têm perspectiva funcional com o intuito de controlar os bancos de dados de forma preventiva.

Posteriormente, essas normas demonstram fragilidade, abrindo espaço para uma nova geração de leis. A segunda geração de normas buscava tratar prioritariamente o direito à privacidade e não de quais formas os bancos de dados poderiam ou não existir, como na primeira geração.

Como consequência, a privacidade informacional foi inserida nos textos das Constituições da Áustria, Espanha e de Portugal. As normas de segunda geração têm como atributo a possibilidade de concordância do indivíduo no processo de coleta e de processamento de dados, por meio de seu consentimento. Igualmente, dá-se ao indivíduo um poder de decisão para intervir no domínio de sua própria privacidade informacional[131].

---

[130] MAYER-SCHÖNBERGER, Viktor. *Generational Development of Data Protection in Europe*. In: Technology and Privacy: The New Landscape. Massachusetts: The MIT Press, 2001. p. 221.
[131] *Idem*, p. 227.

Nesse contexto, porém, verifica-se que, caso o indivíduo não consinta com o fornecimento de dados, poderá ser excluído do contexto social. Assim, a proteção de dados pessoais como liberdade individual pode oferecer ao indivíduo a possibilidade de não conceder informações a seu respeito que lhe são solicitadas. Mas qual será o custo disso? É aceitável que a proteção de dados pessoais possa ser exercida apenas por eremitas? Será que há garantia da proteção de dados quando a proteção se dá somente em relação àqueles que serão necessariamente excluídos da sociedade?[132]

Em 1981, O Conselho da Europa assinou a Convenção 108 do Conselho da Europa para proteção das pessoas singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais. Trata-se do primeiro instrumento internacional juridicamente vinculativo em relação aos dados pessoais. Visa garantir *"a todas as pessoas singulares (...) o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de caráter pessoal*".

Posteriormente, surgiu a terceira geração de leis de proteção de dados pessoais. Ela foi iniciada pela decisão do tribunal alemão, em 1983, que declarou a inconstitucionalidade da "Lei do Censo"[133]. Mencionada lei previa a obrigatoriedade do fornecimento de dados pessoais, sem sua adequada proteção. Na situação, o tribunal reinterpretou a lei de proteção de dados pessoais alemã e declarou que os cidadãos possuem o direito à autodeterminação informativa, radicalizando a ideia do consentimento do indivíduo no processamento de seus dados[134].

Porém, mais uma vez, o ideal de controle das informações pessoais, fundado na ideia de autodeterminação informativa, provou-se não ser suficiente. Isso porque, de maneira semelhante à segunda geração das normas de proteção aos dados

---

[132] *Ibidem*, p. 228.

[133] Por meio da decisão, foi garantido o direito de autodeterminação dos indivíduos no sentido de poder controlar e fiscalizar o levantamento de seus dados pessoais e relativos à sua vida privada. Ressaltou-se a ideia de que toda pessoa precisaria permanecer, para o efetivo desenvolvimento livre e responsável de sua personalidade, em uma espécie de "espaço interno", no qual ela domina e controla a si própria e do qual ela possa se retirar sem sofrer influências externas. Tal espaço deveria permitir que se ficasse em paz e que se aproveitasse um direito de estar só.

[134] MAYER-SCHÖNBERGER, Viktor. *Op. Cit.,* p. 228.

pessoais, os indivíduos não estavam dispostos a arcar com os custos sociais (de exercer o seu direito e não fornecer dados pessoais) para, por consequência, serem privados do acesso a bens e serviços ou a benefícios[135].

Por fim, a quarta geração de normas procurou resolver esses problemas apresentados pelas gerações anteriores de duas formas: (i) por meio do fortalecimento da posição dos indivíduos, tornando mais efetivo o seu autocontrole sobre os dados pessoais, e (ii) em alguns casos, retirando da esfera de controle do indivíduo o poder de decisão sobre o compartilhamento de dados em relação a determinados assuntos que, por serem muito delicados e terem potencial de acarretar discriminação, não podem estar na esfera de disposição individual[136].

Em 1995, foi regulamentada a proteção de dados pessoais nos países membros da União Europeia, por meio da Diretiva 95/46/CE, que delimitou e fixou parâmetros para o levantamento, o processamento, a utilização, o armazenamento e a circulação de dados pessoais no âmbito dos países componentes. Está no seu cerne a participação do indivíduo no processo de tratamento dos dados pessoais.

O conceito de dados pessoais foi definido no artigo 2º "a" da Diretiva 95/46/CE, substituída em 27 de abril de 2016 pelo Regulamento Geral sobre a Proteção de Dados:

> a) "dados pessoais": toda informação concernente a uma pessoa física identificável ou identificada (pessoa interessada); é reputada identificável uma pessoa que possa ser identificada, diretamente ou indiretamente, especialmente por um número de identificação ou um dentre vários elementos específicos, próprios a sua identidade física, econômica, cultural ou social.

---

[135] *Idem*., p. 232.
[136] *Ibidem.* p. 233.

Ademais, o Regulamento Geral sobre a Proteção de Dados, em linhas gerais, apresenta princípios que devem ser observados na legislação pelos Estados-Membros para garantir o direito à proteção de dados, bem como limites e exceções ao tratamento de dados pessoais.

Além disso, em caso de tratamento de dados sensíveis, o Regulamento Geral sobre a Proteção de Dados determina que este está condicionado ao consenso expresso e informado do indivíduo. O Regulamento Geral sobre a Proteção de Dados possibilita que os cidadãos proíbam a utilização de seus dados para fins de realização de *marketing* direto.

O Regulamento Geral sobre a Proteção de Dados continua em vigor. Porém, tendo em vista o avanço tecnológico, foram criadas novas Diretivas sobre proteção de dados, a saber: Diretiva 2002/58/CE, relativa à privacidade, conhecida como *ePrivacy Directive* (alterada em 2009), a Diretiva 2006/24/CE, relativa à conservação de dados (declarada inválida pelo Tribunal de Justiça da União Europeia em 2014, devido à sua interferência na vida privada e na proteção de dados pessoais), e a Diretiva 2009/136/CE (conhecida como *Privacy and Eletronic Communication Directive*).

A Diretiva 2002/58/CE procurou regulamentar a proteção de dados especialmente nos serviços de comunicação eletrônica, tendo em vista o avanço que estava sofrendo no mundo. Ela fornece instrumentos que permitem adequação de suas diretrizes à realidade tecnológica que surgiu com a comunicação em rede.

Posteriormente, foi aprovada a Diretiva 2009/136/CE cujos pontos principais são gerar confiança no ambiente online, qualidade na prestação de serviços na internet, criar harmonia entre as regras dos Estados-Membros da União Europeia, garantir acesso à internet e às comunicações eletrônicas a todos cidadãos, com destaque para os portadores de necessidades especiais e, especialmente relacionado com o presente projeto, impor aos provedores de acesso à internet e aplicativos de internet a obrigação de adotar medidas para evitar que sejam instalados *spywares* nas máquinas dos usuários. A Diretiva ainda estimula a cooperação entre os Estados-Membros para o combate de *spams* ilícitos e de *spywares* entre os Estados-Membros.

Mais recentemente, houve a Reforma da Proteção de Dados, que entrou em vigência em maio de 2018, após três anos de debates. Por meio dela, entraram em vigor o Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, bem como a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de crimes ou execução de sanções penais e à livre circulação desses dados.

Uma das mais importantes mudanças trazidas com a Reforma determina que os *data controllers* devem notificar a autoridade supervisora de qualquer vazamento de dados no prazo 72 horas (se possível). Foram positivados o direito ao esquecimento e outros. Importante novidade também é a obrigatoriedade de adoção do *privacy by design* pelas empresas, como, por exemplo a utilização de técnica de pseudônimos, auditorias e treinamento de equipe.

Esse é o quadro geral legal na União Europeia, que certamente sofrerá ainda muitas alterações, considerando a volatilidade do tema em si.

2.2. Dados pessoais e o Marco Civil da Internet

A sociedade brasileira clamava há anos para que fosse aprovada lei que regulamentasse o uso da internet, desde que se verificou o risco que o tratamento dos dados pessoais poderia representar.

A jurisprudência e a doutrina até então estavam cuidando de regular determinadas situações e tentando reduzir os abusos criados na internet, aplicando o direito à privacidade ao caso concreto de violação de dados pessoais. Já havia sido iniciado o processo de construção do direito à proteção dos dados pessoais. Porém, pela falta de lei específica e mesmo de orientação uniforme dos tribunais, as decisões destoavam de juízo para juízo. Inegavelmente, este panorama de insegurança jurídica não é algo que

contribui para a sociedade como um todo e tampouco ao desenvolvimento da internet no Brasil.

Para especialistas, a jurisprudência estava ainda cambaleante no que dizia respeito ao entendimento das novas tecnologias da sociedade da informação. Citam-se casos diversos: em uma decisão específica, uma ordem judicial proibiu um cidadão de publicar comentários contestando a criação de três torres com 162 apartamentos em São Paulo. Outra decisão judicial impediu um advogado de acessar qualquer rede social, após este ter feito críticas à atuação de um membro do Ministério Público.

Diante de tal instabilidade, o Marco Civil da Internet foi discutido e elaborado, de forma democrática e aberta, tornando-se a lei que estabelece princípios, garantias, direitos e deveres para o uso da internet. Assim, foi publicada no Diário Oficial da União de 24 de abril de 2014 a Lei 12.965, que estabelece regras gerais para utilização da internet no Brasil. A lei entrou em vigor em junho de 2014, após decorridos 60 dias da sua publicação oficial. O Marco Civil da Internet trouxe diversas inovações, dentre as quais as mais importantes encontram-se abaixo relacionadas.

O ponto mais importante do Marco Civil para o presente estudo é a novidade que a lei trouxe ao positivar o princípio da proteção de dados pessoais na internet (artigo 3º, III da Lei). Até o implemento da lei, os dados eram coletados, tratados e vendidos quase que instantaneamente e sem limitações expressas, porém, com a inovação legal, pode-se afirmar que as informações dos usuários não podem ser usadas para um fim diverso daquele para que foram fornecidas.

Logo, a lei estabelece que, desde que haja consentimento livre, expresso e informado do usuário, o provedor poderá fornecer a terceiros os seus dados pessoais, registros de conexão e de acesso a aplicações de internet (artigo 7º, VII). A lei institui, ainda, que os contratos deverão conter, de forma destacada das demais cláusulas, o consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais dos usuários (artigo 7º, IX).

Vale adiantar que tal situação causará dificuldade do ponto de vista prático. A exigência de "consentimento livre, expresso

e informado" pode trazer certos problemas no caso concreto, posto que é difícil delimitar com precisão que tipo de manifestação de vontade pode ser considerada como detentora de todas essas características.

O Marco Civil da Internet também apresentou alguns conceitos, como o dos provedores. A Lei os divide em (i) provedores de conexão e (ii) provedores de aplicação.

Os primeiros, segundo Marcel Leonardi são denominados provedores de acesso[137], sendo classificados como fornecedores de serviços que possibilitem o acesso de seus consumidores à internet. Estes provedores são os responsáveis pela conexão da internet e desenvolvem função de intermediários entre o usuário e a rede.

Os provedores de aplicação, por outro lado englobam os provedores de correio eletrônico, de hospedagem e de conteúdo, sendo que:

> Provedor de correio eletrônico fornece (...) serviços que consistem em possibilitar o envio de mensagens do usuário a seus destinatários, armazenar as mensagens enviadas a seu endereço eletrônico até o limite de espaço disponibilizado no disco rígido de acesso remoto e permitir, somente ao contratante do serviço, o acesso ao sistema e às mensagens, mediante o uso de um nome de usuário e senha exclusivos.
>
> (...)
>
> Provedor de hospedagem é a pessoa jurídica que fornece o serviço de armazenamento de dados em servidores próprios de acesso remoto, possibilitando o acesso de terceiros a esses dados, de acordo com as condições estabelecidas com o contratante do serviço. (...)

---

[137] LEONARDI, Marcel. Responsabilidade *Civil dos Provedores de Serviços de Internet*, São Paulo: Juarez de Oliveira, 2005, p. 21.

> Provedor de conteúdo é toda pessoa natural ou jurídica que disponibiliza na Internet as informações criadas ou desenvolvidas pelos provedores de informação, utilizando para armazená-las servidores próprios ou os serviços de um provedor de hospedagem. [Por outro lado,] o provedor de informação é toda pessoa natural ou jurídica responsável pela criação das informações divulgadas através da Internet. É o efetivo autor da informação disponibilizada por um provedor de conteúdo. Dessa forma, o provedor de conteúdo pode ou não ser o próprio provedor de informação, conforme seja ou não o autor daquilo que disponibiliza[138].

As aplicações de internet são definidas pelo Marco Civil da Internet como o conjunto de diversas funcionalidades acessíveis por meios de terminais conectados à internet. O Marco determina, em seu artigo 15, que esse tipo de provedor (de aplicação) é aquele "*constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos*".

Acrescente-se, ainda, que o artigo 10 da lei determina que os provedores devem observar sigilo em relação aos registros de conexão e de acesso a aplicações de internet, dados pessoais e conteúdo de comunicações privadas dos usuários. O texto legal também estabelece que o provedor responsável pela guarda somente poderá disponibilizar registros de conexão e de acesso a aplicações de internet e conteúdo de comunicações privadas mediante ordem judicial (artigo 10, parágrafos 1º e 2º, artigo 13, parágrafo 5º e artigo 15, parágrafo 3º).

Ademais, conforme determina o artigo 8º, parágrafo único, são reputadas nulas de pleno direito as cláusulas contratuais que violem a garantia do direito à privacidade e à liberdade de expressão nas comunicações dos usuários, tais como aquelas que

---

[138] *Idem*., p. 22-25.

impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas via internet.

No mesmo artigo que reconhece a proteção de dados pessoais como um princípio, o Marco Civil indica que tal proteção deve se dar nos termos da Lei (art. 3º, III). Ou seja, faz referência à criação de uma lei específica para tratamento dos dados pessoais, deixando evidente que não foi intuito do legislador esgotar o tema.

Uma alteração muito criticada está relacionada à responsabilidade dos provedores por conteúdo de terceiros. A lei prevê que o provedor somente poderá ser responsabilizado por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial, ou da notificação em caso de material reproduzindo sexo ou nudez, não tomar as medidas necessárias para tornar indisponível o conteúdo indicado como infringente (artigos 19, 20 e 21).

Em outras palavras: excepcionados casos em que haja conteúdo sexual ou nudez, o provedor só será obrigado a retirar conteúdo da internet após ordem judicial. Desta forma, caberá ao juízo decidir, no caso concreto, quando a retirada de conteúdo é admissível e quando não é – algo muito criticado pela doutrina especializada, a exemplo de Renato Ópice Blum[139].

Essa mudança ganha importância, pois, até o advento do Marco Civil da Internet, o Superior Tribunal de Justiça entendia que provedores de aplicações que mantivessem serviços de redes sociais deveriam retirar, em até 24 horas do recebimento da notificação, publicações ofensivas à pessoa mediante mero pedido desta, sob pena de responder na esfera civil pelos danos morais causados, adotando o modelo norte-americano denominado "*notice and takedown*"[140].

---

[139] UOL. *Especialistas apontam pontos falhos no marco civil em audiência no Senado*. Disponível em: <http://tecnologia.uol.com.br/noticias/redacao/2014/04/15/especialistas-apontam-pontos-falhos-no-marco-civil-em-audiencia-no-senado.htm>. Acesso em: 06.jul.15.

[140] REsp 1193764/SP, Rel. Ministra Nancy Andrighi, Terceira Turma, julgado em 14/12/2010 e AgRg no REsp 1309891/MG, Rel. Ministro Sidnei Beneti, Terceira Turma, julgado em 26/06/2012.

2.3. Princípios relacionados aos dados pessoais

Canotilho[141] estabelece diversos princípios relativos à proteção de dados pessoais. De acordo com o autor, para que a proteção aos direitos de personalidade dos usuários da internet seja respeitada, se faz fundamental que os princípios elencados sejam observados.

O primeiro princípio citado por Canotilho é a publicidade. Para o autor é necessário que o *site* deixe claro o compartilhamento de informações, com o usuário tendo conhecimento concreto sobre a criação e manutenção de registros informáticos pelo *site* que está acessando.

Outro princípio citado por Canotilho é a justificação social. Ele explica que é fundamental que o uso de arquivos, bases de dados e bancos de dados tenha objetivos geral e específico claramente definidos e que estes estejam de acordo com os interesses sociais.

Por sua vez, a transparência está diretamente relacionada à publicidade. Canotilho destaca a necessidade de clareza dos registros tanto quanto às espécies e categorias de informações quanto ao tempo de tratamento dessas informações.

Destaca-se, ainda, como princípio a especificação de finalidades, que deve ocorrer logo no momento da captura dos dados. Além disso, deve haver uma limitação na captura desses dados, restringindo-se aos dados necessários para finalidades específicas já citadas. Neste ponto têm-se os princípios da necessidade e da proporcionalidade.

Canotilho cita também o princípio da fidelidade, que diz que os dados devem ser exatos, completos e atuais e o princípio da limitação da utilização dos dados, que devem ser utilizados exclusivamente para persecução das finalidades que foram especificadas previamente à coleta. O autor também menciona as garantias de segurança do usuário contra perda, destruição e/ou acesso de terceiros aos seus dados. O responsável pelo site que

---

[141] CANOTILHO, J.J. Gomes. *Constituição* da *República Portuguesa anotada,* vol. 1. São Paulo, AT, 1ª Ed., 2007, p. 550.

recolheu dados do usuário também é responsável por esses dados, sendo impostos a ele deveres legais e deontológicos.

Por fim, Canotilho cita o princípio de limitação do tempo, que impõe o cancelamento dos dados, assim que a finalidade a que eles se propunham for atendida.

Nesse mesmo sentido, Danilo Doneda cita cinco princípios a serem seguidos, tendo como base a Convenção de Strasbourg e as *guidelines* da OCDE: princípio da publicidade; princípio da exatidão; princípio da finalidade; princípio do livre acesso e princípio da segurança física e lógica[142].

O princípio da publicidade, conforme Danilo Doneda, ocasiona a necessidade de conhecimento público da existência de um banco de dados, sendo necessária autorização prévia do usuário para a captura dos dados.

O princípio da exatidão, por sua vez, diz respeito ao princípio da fidelidade citado por Danilo Doneda: os dados armazenados devem ser fieis à realidade, exigindo cuidado e correção, além de atualização constante dos dados.

O princípio da finalidade apresenta-se como de grande importância, visto que se fundamenta na restrição da transmissão de dados pessoais a terceiros, devendo sempre obedecer especificamente à finalidade informada a usuário no momento de captura dos dados.

Enquanto isso, o princípio do livre acesso, como o próprio nome sugere, trata-se da possibilidade do usuário de ter acesso ao banco de dados em que suas informações estão armazenadas, com controle sobre elas, podendo, inclusive, obter cópia desses registros.

Finalmente tem-se, na visão de Danilo Doneda, o princípio da segurança física e lógica, devendo os dados serem protegidos contra os riscos de extravio, destruição, modificação, transmissão ou acesso não autorizado.

---

[142] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law [EJJL*], v. 12, n. 2, p. 91-108, 2011.

Como se verifica, portanto, em geral, trata-se de uma sistematização de princípios similar dos dois autores.

2.4. Proteção de dados pessoais e direitos da personalidade

A conceituação dos direitos da personalidade é uma problemática que há tempos tem sido debatida entre estudiosos do Direito Civil. Existem, é fato, elementos mínimos sobre o assunto para traçar alguns caracteres comuns que permitem realizar um corte epistemológico sobre o assunto.

Os direitos da personalidade, como definidos por Antonio Carlos Morato, "v*ersam sobre a própria pessoa e seus reflexos e são reconhecidos à pessoa humana e atribuídos à pessoa jurídica*"[143]. O autor continua: *"os direitos da personalidade nada mais são do que a proteção aos direitos do ser humano sob o enfoque privado*"[144].

Adriano de Cupis que aos direitos da personalidade "*é reservado para esses direitos subjetivos, cuja função, em relação à personalidade, é especializada, constituindo o ´mínimo´ necessário e indispensável do seu conteúdo*"[145].

José Serpa, por sua vez, ensina que os direitos da personalidade:

> são como projeções de certos atributos, que adornam e dignificam a pessoa humana. Nos substanciais direitos privados da personalidade, ao lado de seu caráter absoluto, sobressai a essencialidade lapidarmente descrita por Adriano de Cupis. Esta essencialidade, bem entendida como necessariedade, participa da própria natureza do ser humano, sendo, pois, inatos

---

[143] MORATO, Antonio Carlos. Quadro geral dos direitos da personalidade. *Revista da Faculdade de Direito (USP),* v. 106-107, p. 121-158, 2012, p. 124.
[144] *Ibidem*. p. 130.
[145] CUPIS, Adriano de. *Il Diritto della* personalità*,* Milano: Giuffré, 1982. p. 13.
No original: "*è riservata a quei diritti soggettivi, la cui funzione, rispetto alla personalità, si specializza, costituendo il 'minimum' necessario e imprescindibile del suo contenuto*".

> os direitos inerentes eis que nascem e morrem com a pessoa humana, sendo destinados, como magistralmente exalta Orlando Gomes, a resguardar a eminente dignidade humana[146].

Já Orlando Gomes aborda o tema da seguinte maneira:

> Sob a denominação de direitos da personalidade, compreendem-se os direitos personalíssimos e os direitos essenciais ao desenvolvimento da pessoa humana, que a doutrina moderna preconiza e disciplina no corpo do Código Civil como direitos absolutos, desprovidos, porém, da faculdade de disposição. Destinam-se a resguardar a eminente dignidade da pessoa humana, preservando-a dos atentados que pode sofrer por parte dos outros indivíduos[147].

Anderson Schreiber, em excelente monografia sobre o tema, define a expressão como sendo

> empregada na alusão aos atributos humanos que exigem especial proteção no campo das relações privadas, ou seja, na interação entre particulares, sem embargo de encontrarem também fundamento constitucional e proteção nos planos nacional e internacional[148].

Como é possível verificar dos conceitos acima coletados, os direitos da personalidade têm como centro gravitacional o indivíduo. Com efeito, são direitos que exsurgem da condição existencial do indivíduo, independendo da vontade de seus titulares para existirem juridicamente.

Trata-se da estrutura jurídica da pessoa, ou seja, de direitos que decorrem diretamente da condição de ser humano do seu

---

[146] de SANTA MARIA, José Serpa. *Direitos da Personalidade e a Sistemática Civil Geral,* São Paulo: Editora Julex Livros Ltda., 1987, p. 31.
[147] GOMES, Orlando. *Introdução ao Direito Civil*, 11ª. ed., Rio de Janeiro, Forense, 1996, p.130.
[148] SCHREIBER, Anderson. Direitos da personalidade. São Paulo: Atlas, 2011, p.13

titular. Nesta condição, os direitos da personalidade são inatos, de sorte que prescindem de qualquer manifestação de vontade para sua existência ou seu exercício. Neste sentido, ensina Paulo Mota Pinto:

> Tais direitos são, portanto, essenciais, uma vez que a própria personalidade humana quedaria descaracterizada se a proteção que eles concedem não fossem reconhecida pela ordem jurídica. São, por outro lado, direitos gerais, isto é, direitos de que são titulares todos os seres humanos, não estando essa titularidade ligada a um grupo, classe ou categoria específica de homens (característica, esta, que é a decorrente óbvia de, por um lado, se reconhecer a qualidade de pessoa a todos e de, por outro lado, estes direitos serem essenciais).[149]

Na mesma toada, Bittar ensina que os direitos da personalidade são inatos ao ser humano, em suas palavras:

> [...] Entendemos que os direitos da personalidade constituem direitos inatos — como a maioria dos escritores ora atesta —, cabendo ao Estado apenas reconhecê-los e sancioná-los em um ou outro plano do direito positivo — em nível constitucional ou em nível de legislação ordinária —, e dotando-os de proteção própria, conforme o tipo de relacionamento a que se volte, a saber: contra o arbítrio do poder público ou as incursões de particulares[150].

Ademais, são universais, posto que toda pessoa natural pode exercê-los em sua total extensão. Existe debate acerca da titularidade de direitos da personalidade por pessoas jurídicas. Isso

---

[149] PINTO, Paulo Mota. Notas sobre o direito ao livre desenvolvimento da personalidade e os direitos de personalidade no direito português, *in*: A constituição concretizada – construindo pontes com o público e o privado. Porto Alegre: Livraria do Advogado, 2000. p. 63.

[150] BITTAR, Carlos Alberto. Os direitos da personalidade, 7ª ed., Rio de Janeiro: Forense Universitária, 2004, p. 7.

porque há quem entenda que essas entidades são mera ficção legal, não sendo dotadas de existência senão por previsão legal.

Milita em prol desse entendimento uma interpretação do artigo 52 do Código Civil[151], que estende a essas entidades tão somente a proteção desses direitos, limitando-os ainda ao que for aplicável. Desta forma, as pessoas jurídicas não seriam titulares dos direitos da personalidade, mas tão somente poderiam invocar instrumentos jurídicos de proteção desses direitos, cabendo, ainda, ao aplicador da lei decidir quais direitos podem ser estendidos às pessoas jurídicas em cada caso concreto.

Em sentido diverso, o Superior Tribunal de Justiça possui entendimento sumulado[152] no sentido da possibilidade de pessoas jurídicas sofrerem danos morais. Frise-se que a premissa básica para se reconhecerem os danos morais é a existência de direitos da personalidade a serem violados.

De outro lado, por serem inerentes à pessoa e prescindirem de um ato volitivo para sua existência, os direitos da personalidade são oponíveis *erga omnes*, ou seja, o titular do direito pode buscar tutela contra qualquer um que tenha violado seus direitos.

O ordenamento jurídico confere um amplo sistema de proteção aos direitos da personalidade, em especial depois do advento do Código Civil de 2002. Neste diploma,[153] foi previsto um sistema que permite, ao titular dos direitos da personalidade, buscar tutela jurisdicional preventiva, de forma a evitar a ocorrência de um dano, pleiteando a imposição de ações ou omissões de quem quer que ameace esses direitos, sem prejuízo da tradicional tutela repressiva mediante indenização por danos morais.

---

[151] Art. 52. Aplica-se às pessoas jurídicas, no que couber, a proteção dos direitos da personalidade.

[152] STJ Súmula nº 227 - 08/09/1999 - DJ 20.10.1999 - Pessoa Jurídica - Dano Moral. A pessoa jurídica pode sofrer dano moral.

[153] 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.

Os direitos da personalidade são, ainda, por força de lei,[154] irrenunciáveis e intransmissíveis. A letra da lei, neste quesito, é categórica e, em certa medida, descolada da realidade. Com efeito, ao buscar proteger o indivíduo das suas próprias escolhas, a escolha do legislador[155] acabou por criar problemas que surgem em casos concretos que esbarram nessa norma. Segundo Anderson Schreiber, "*em uma série de situações não previstas em lei, mas socialmente admitidas, as pessoas desejam e aceitam limitar, pontualmente, o exercício de algum atributo da própria personalidade*"[156].

Em resposta a essa problemática, a doutrina acabou por amenizar o rigor legislativo, construindo teses que admitem a restrição ou alienação parcial de direitos da personalidade, desde que restritas no tempo e na extensão, assim como sempre vinculadas ao melhor interesse da pessoa, no que tem especial aplicação a noção de dignidade humana. Sobre o assunto, novamente recorre-se às palavras de Anderson Schreiber:

> Para analisar a legitimidade das autolimitações ao exercício dos direitos da personalidade, não há fórmula matemática, mas há alguns aspectos que devem ser levados necessariamente em conta. Em primeiro lugar, é de se examinar sua duração e alcance. Qualquer autolimitação de caráter irrestrito ou permanente não deve ser admitida, por se equiparar à renúncia
> [...]
> Qualquer limitação voluntária do exercício de um direito da personalidade deve estar vinculada, como já se destacou, a um interesse direto e imediato do próprio titular[157].

Por fim, deve ser destacado que os direitos da personalidade são ampliativos. Isso quer dizer que não há um rol

---

[154] Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.
[155] Interessante notar que, em certos casos, alguns diplomas legislativos admitem a restrição a esses direitos. Os mais interessantes são a lei de transplantes de órgãos (Lei nº 9.434, de 4 de fevereiro de 1997) e a lei de proteção de direitos autorais (Lei nº 9.610, de 19 de fevereiro de 1998), que excepcionam esta regra, permitindo, desde que dentro de certos limites, a restrição ao direito à integridade física e à titularidade dos direitos autorais, respectivamente.
[156] SCHREIBER, Anderson. *Direitos da Personalidade.* 2ª ed. São Paulo: Atlas, 2013, p. 27.
[157] *Ibidem*.

exaustivo elencando todos, apesar de existirem alguns que são sempre inerentes. Considerando que eles decorrem da própria condição do ser humano, é inviável exigir que o legislador os reconheça de forma definitiva, posto que, a cada dia, novas questões surgem, nos campos filosófico, sociológico, antropológico, psicológico, dentre outros, que alteram a essência do ser humano, cabendo ao legislador saber detectar e criar as normas jurídicas que sejam necessárias para preservar esse núcleo duro da existência humana.

A discussão sobre os dados pessoais e sua correta alocação jurídica não foge ao campo de discussão dos direitos da personalidade. Com efeito, os problemas jurídicos atrelados aos dados pessoais surgiram, num primeiro momento, ligados à privacidade — que é um dos mais tradicionais direitos da personalidade —, pois se objetivava proteger o indivíduo contra exposições indevidas dos fatos que integram a vida privada e a intimidade.

Contudo, com o advento da tecnologia, em especial a internet, os dados pessoais passaram a se desvincular de questões ligadas somente à privacidade. Com efeito, em certo ponto, a coleta e a manipulação de dados por meio cibernético passou a configurar um risco que não necessariamente se relacionava somente com a exposição indevida de fatos da vida do indivíduo, mas sim com a possibilidade de mau uso daqueles para finalidades diversas das incialmente autorizadas, ou mesmo para fins ilícitos, como manipulação política ou indução comercial.

Os dados pessoais revelam o vínculo da informação pessoal com o seu titular, acabam por tornar visível diretamente algo sobre o indivíduo titular. Pierre Catala apontou, em 1983, que um dado é pessoal quando o objeto da informação é a própria pessoa, e, assim, trata-se de atributo da personalidade, considerando as características dos direitos da personalidade acima expostos.

Catala aponta também que, ainda que a pessoa em questão não seja a criadora da informação, no sentido de tê-la concebido voluntariamente, ela é a titular legítima de seus elementos, ou seja, dos fatos da vida que representam. O seu vínculo com o indivíduo é por demais estreito para que fosse de outra forma. Assim,

quando o objeto da informação é um sujeito de direito, a informação é um atributo da personalidade[158].

Desta forma, considerando a classificação jurídica dos dados pessoais como direitos da personalidade, é relevante destacar que o mundo jurídico não pode deixar esta discussão à margem do sistema. O uso de instrumentos cada vez mais eficientes na coleta de dados pessoais coloca essas questões no centro dos debates jurídicos, merecendo atenção tanto da doutrina quanto de julgadores e demais aplicadores da lei, inclusive a administração pública.

2.4.1. Eficácia horizontal dos direitos fundamentais

Os direitos fundamentais, enquanto conceito jurídico, não possuem univocidade na definição. A determinação do que sejam esses direitos, ou de quais objetos devem proteger, varia conforme o tempo, o lugar e as posições pessoais do intérprete da norma. Tal fato revela, por si só, a multidimensionalidade das questões que surgem do problema.

De uma forma sucinta, pode-se entender que os direitos fundamentais são aqueles direitos, reconhecidos na estrutura do Estado por norma constitucional fundamental, como sendo os direitos básicos do indivíduo enquanto merecedor de proteção estatal. Não se confundem, mas sim complementam os direitos da personalidade acima delineados, posto que derivam de fontes jurídicas distintas e possuem papéis diferentes no sistema de proteção do indivíduo.

Enquanto os direitos da personalidade derivam de normas constitucionais ou infraconstitucionais, podendo ser reconhecidos e protegidos por meio de sistemas que o legislador ordinário crie, os direitos fundamentais são reconhecidos necessariamente no sistema constitucional, de forma expressa ou implícita, cabendo ao legislador ordinário tão somente aparelhar o Estado para tornar efetivos estes direitos.

---

[158] CATALA, Pierre. *Ebauche d'une théorie juridique de l'informati*on, in: Informatica e Diritto, ano IX, jan-apr. 1983, p. 20 (tradução livre).

Os direitos da personalidade visam resguardar o mínimo da condição do ser humano, tendo como objeto aqueles direitos que protegem bens essenciais a este mister, como o corpo, a integridade física, a honra, a privacidade, dentre outros.

Nesse sentido, Lima ensina que o direito geral de personalidade pode ser visto como um direito subjetivo e também como uma cláusula geral:

> Portanto, entendemos que o direito geral de personalidade pode ser visto como um direito subjetivo na medida em que gera uma pretensão, no sentido jurídico, de forma que seu titular pode exigir *erga omnes* uma conduta normativa positiva ou negativa. É uma cláusula geral na medida em que confere ao operador do direito maior flexibilidade para que o intérprete analise os argumentos e fatos caso a caso, definindo o conteúdo da norma subjacente[159].

Já os direitos fundamentais, sem conflitar com os direitos da personalidade, configuram o mínimo de direitos que serão objeto de proteção estatal. Cumpre ressalvar que, em determinados casos, os direitos da personalidade são direitos fundamentais, como é o caso da privacidade, dos direitos de autor, dentre outros que exigem efetiva ação estatal para proteção.

Por fim, é interessante destacar que os direitos da personalidade, em última instância, representam sempre uma projeção do maior direito fundamental de todos: a dignidade da pessoa humana, insculpida na cabeça do artigo 5º da Constituição Federal.

Diante de todo o exposto, fica evidenciado que, pela tradição dos conceitos, os direitos fundamentais formam um conjunto de determinações ao Estado, enquanto garante de direitos, e os direitos da personalidade, em regra, são oponíveis contra qualquer pessoa que os viole ou ameace violar.

---

[159] LIMA, Cíntia Rosa Pereira de. *A imprescindibilidade... Op. Cit*. p. 80

A interação entre esses conceitos, acima demonstrada, por outro lado, deixa evidente que nem todo direito fundamental será exclusivamente oponível ao Estado. Os entendimentos recentes sobre o assunto têm quebrado essa divisão científica e atribuído o que se convencionou chamar de "eficácia horizontal" a esta categoria de direitos.

Ora, não somente o Estado pode lesar os direitos fundamentais por ação ou omissão. Tome-se como exemplo a liberdade de pensamento[160]. Trata-se de comando tradicionalmente voltado ao Estado, com fins a evitar censuras calcadas exclusivamente na ideologia daqueles que detêm o poder.

Contudo, é evidente que, em várias ocasiões particulares, podem também lesar este direito, como quando grupos particulares buscam frustrar manifestações de outros particulares em via pública, feitas de forma regular. Nesses casos, o Estado também deve agir, para fins de garantir outros bens, inclusive a segurança pública e a ordem jurídica. Contudo, do particular que lesa o direito de seu igual, também deve ser exigido comportamento respeitoso dos direitos fundamentais, cabendo ao lesado exigir também a observância do Estado Democrático de Direito.

A discussão sobre a proteção dos dados pessoais também se passa nesta esfera. Os grandes atores na coleta e tratamento de dados pessoais são empresas particulares, que se utilizam de diversos recursos de tecnologia para captar esses dados e transformá-los, de diversas formas, em algo rentável. Como será demonstrado neste trabalho, essas práticas devem encontrar limites, justamente quando confrontadas com direitos fundamentais e direitos da personalidade dos titulares dos dados pessoais.

Como será colocado abaixo, os dados pessoais estão passando a configurar um direito fundamental autônomo, justamente enquanto projeção direta da dignidade da pessoa humana e, somando-se a isso o fato de que grande parte das infrações a esse direito provêm de entes privados, a discussão sobre a existência, extensão e aplicabilidade da eficácia horizontal dos direitos fundamentais ganha especial relevância.

---

[160] Art. 5º, IV - é livre a manifestação do pensamento, sendo vedado o anonimato;

2.4.2. Direito à proteção de dados como um direito fundamental

A problemática jurídica ligada aos dados pessoais tem estreita vinculação com o direito fundamental à privacidade e, recentemente, tem inclusive ultrapassado esta esfera, colocando em questão o direito fundamental à autodeterminação informativa (ou informacional) do indivíduo.

Os problemas que derivam dos dados pessoais ligam-se, em larga escala, à deturpação da utilização dos dados pessoais por particulares que os captam, e nem sempre de maneira lícita[161], frustrando aspecto crucial da esfera de direitos individuais.

É interessante destacar que não se trata também de uma questão meramente contratual entre o titular dos dados pessoais e aquele que coleta e trata esses dados. Nem sempre existe contrato entre essas partes e, muitas vezes os dados pessoais são coletados e infringem a esfera subjetiva de direitos do seu titular, merecendo resposta jurídica à altura.

Como acima colocado, os direitos fundamentais derivam de proteção constitucional, seja por reconhecimento expresso no texto, seja por dedução lógico-jurídica de valores que decorrem das normas e princípios previstos no texto fundamental. Os dados pessoais, como acima exposto, podem ser classificados como direitos da personalidade, pois, em essência, visam à proteção da dignidade da pessoa humana na sua dimensão existencial e, ainda, têm vida própria dentro da conceituação de direito fundamental pois devem existir, também, ações estatais que visem à proteção desses direitos. Isso posto, é acertado considerar que os dados pessoais caminham para serem considerados direitos fundamentais *per se*, desvinculando-se dos demais direitos que lhe deram origem.

Nesse sentido, Lima ensina que o direito à proteção de dados pessoais, conforme a doutrina de Stefano Rodotá, deve ser tutelado como um direito fundamental:

> No que tange ao direito brasileiro, podemos afirmar que o direito à proteção

---

[161] Nesse trabalho também são tratados, de forma mais detalhada, os maiores problemas ligados à utilização dos dados pessoais dos indivíduos e usuários da internet, de forma que, para evitar repetições, remete-se à leitura do trecho para mais detalhes.

> dos dados pessoais diz respeito às regras de conduta impostas para o tratamento dos dados que consiste em operação ou conjunto de operações, automatizadas ou não, que permitam a coleta, o armazenamento, a organização, a consulta, a modificação, a classificação, o cancelamento, a transmissão ou a difusão, bem como outras condutas com estas relacionadas a depender da evolução tecnológica.
>
> Segundo a opinião de Stefano Rodotà, o direito à proteção dos dados pessoais é muito importante no contexto da atual sociedade informacional em razão dos riscos que ela oferece como destacados *supra*, e por isso tal direito deve ser tutelado como um direito fundamental[162].

Há a necessidade de uma proteção desses direitos que considere as interações e conexões sociais do seu titular. Expõe, portanto, a necessidade de se reconhecer o direito à autodeterminação informativa como uma categoria de direito fundamental[163], como se verá posteriormente.

Com efeito, o direito à proteção dos dados pessoais compreende a possibilidade de controlar de que forma dados sobre um determinado indivíduo são coletados e de que forma são tratados. Questões complexas exsurgem desta colocação, pois se trata de uma faceta da personalidade que é a autodeterminação informativa, a qual faz parte da liberdade individual de fazer as escolhas sobre seus próprios dados de maneira livre e consciente.

---

[162] LIMA, Cíntia Rosa Pereira de. *A imprescindibilidade... Op. Cit.* p.114.

[163] PÉREZ LUÑO, Antonio-Enrique. Informática y Libertad. Comentario al Artículo 18.4 de la Constituición Española. In: *Revista de Estudios Políticos* (Nueva Época), nº 24, pag. 4, Centro De Estudos Constitucionales, Madrid, 1981.

2.5. Outras considerações relacionadas ao Marco Civil da Internet

Outras considerações a respeito do Marco Civil da Internet podem ser relevantes no desenvolvimento deste trabalho. A exemplo, o art. 7º estabelece as garantias dos usuários ao dispor que o acesso à internet é essencial ao exercício da cidadania. Elas são:

> 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.

O mencionado artigo repete alguns direitos assegurados pelo Código de Defesa do Consumidor, como o direto de ter acesso a informações claras e completas constantes dos contratos de pregação de serviço. Porém, menciona de maneira expressa a proteção de dados pessoais.

Como se verifica, a lei dispõe que, salvo mediante consentimento livre, expresso e informado, os dados pessoais não podem ser fornecidos a terceiros, excetuadas as hipóteses previstas em lei (inciso VII). Ademais, determina a necessidade de clareza das informações a respeito da "coleta, uso, armazenamento, tratamento e proteção" dos dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta, não sejam ilegais e estejam especificadas em contrato (inciso VIII).

Dessa forma, determina expressamente a necessidade de obediência ao princípio da finalidade da coleta de dados pessoais por parte dos fornecedores. A coleta e o tratamento de dados pessoais são legais somente para as atividades declaradas na lei.

A lei também fala em direito ao esquecimento quando propõe o direito à exclusão definitiva dos dados pessoais, a pedido do usuário titular, ao término das relações entre as partes (inciso X).

Ademais, conforme determina o artigo 8º, parágrafo único, são reputadas nulas de pleno direito as cláusulas contratuais que violem a garantia do direito à privacidade e à liberdade de expressão nas comunicações dos usuários, tais como aquelas que impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas via internet ou, em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

Mais adiante, o artigo 10 do Marco Civil da Internet, institui que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet[164], bem como de dados pessoais e do conteúdo de comunicações privadas, *"devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas"*.

Os provedores de aplicações de internet — pessoas jurídicas que exerçam essa atividade de forma organizada, profissionalmente e com fins econômicos — deverão manter armazenados, pelo período de seis meses, sob sigilo, em ambiente

---

[164] O registro de conexão é o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP. Já registro de acesso a aplicações é o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

controlado e de segurança, conforme regulamento a ser editado, os respectivos registros de acesso a aplicações de internet, isto é, o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP (artigo 15[165]).

Já o provedor da conexão deverá guardar sigilosamente os registros de conexões, em ambiente controlado e seguro, pelo prazo de um ano, não podendo transferir a responsabilidade para terceiro. Em ambos os casos, uma ordem judicial poderá permitir a guarda dos dados por período maior do que o estipulado em lei (artigos 13[166] e 15).

Lamentavelmente, nada obstante os avanços apresentados pela lei, houve verdadeiro retrocesso no que diz respeito ao direito do usuário de ter retirado determinado conteúdo do ar (note que, nesses casos, o imperativo é a rapidez para a retirada de conteúdos).

A jurisprudência do Superior Tribunal de Justiça havia firmado entendimento (anterior ao Marco Civil da Internet) no sentido de que os provedores de aplicações deveriam retirar, em até 24 horas do recebimento da notificação, as publicações ofensivas à pessoa mediante mero pedido desta, sob pena de responder na esfera civil pelos danos morais causados.

Porém, com o advento da lei, o mero pedido não é mais suficiente para a retirada de conteúdo[167] (exceto nos casos em haja

---

[165] Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

[166] Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

[167] Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

Nesse sentido, segue julgado ilustrativo:

nudez não autorizada (vide artigo 21[168]). Ademais, o entendimento que havia sido firmado não se restringia a casos de retirada de conteúdos ofensivos postados por usuários em redes sociais, mas era aplicado também para *blogs* mantidos por determinado provedor de aplicações, que deveriam retirar do ar os conteúdos ofensivos, independentemente de decisão judicial.

Verifica-se que, com o intuito de assegurar a liberdade de expressão e impedir a censura, houve uma alteração que não é benéfica ao consumidor. No atual contexto, o provedor de aplicações de internet somente será responsabilizado na esfera civil por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para tornar indisponível o conteúdo.

Entende-se que o Marco Civil deveria privilegiar mecanismos que dispensam o caminho judicial para que se possa evitar a propagação de uma determinada lesão a direito de personalidade. Ademais, houve, em verdade, um retrocesso na proteção do consumidor, isentando de responsabilidade os provadores de conexão por danos decorrentes de conteúdo gerado por terceiros.

Esperar uma ordem judicial para remover um conteúdo não é compatível com a velocidade que as informações circulam na

---

"AGRAVO REGIMENTAL EM RECURSO ESPECIAL. DIREITO DO CONSUMIDOR. PROVEDOR. MENSAGEM DE CONTEÚDO OFENSIVO. REGISTRO DE NÚMERO DO IP. DANO MORAL. NÃO RETIRADA EM TEMPO RAZOÁVEL.
1 – Na linha dos precedentes desta Corte, o provedor de conteúdo de internet não responde objetivamente pelo conteúdo inserido pelo usuário em sítio eletrônico, por não se tratar de risco inerente à sua atividade. Está obrigado, no entanto, a retirar imediatamente o conteúdo moralmente ofensivo, sob pena de responder solidariamente com o autor direto do dano. Precedentes. 2 – No caso dos autos o Tribunal de origem entendeu que não houve a imediata exclusão do perfil fraudulento, porque a Recorrida, por mais de uma vez, denunciou a ilegalidade perpetrada mediante os meios eletrônicos disponibilizados para esse fim pelo próprio provedor, sem obter qualquer resultado. 3 – Agravo Regimental a que se nega provimento".
(AgRg no REsp 1309891/MG, Rel. Ministro Sidnei Beneti, Terceira Turma, julgado em 26/06/2012)

[168] Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

internet. A noção de tempo no mundo virtual não é a mesma do mundo real, sendo muito provável o perecimento de um direito.

Outro potencial retrocesso é o Projeto de Lei 215 de 2015, também chamado de "PL Espião", de autoria do Deputado Hildo Rocha (PMDB-MA), que pretende reduzir os direitos e garantias apresentados pelo Marco Civil da Internet. O projeto foi aprovado na forma de substitutivo (compilados pelos projetos de lei 1.547 e 1.589 de 2015) pela Comissão de Constituição e Justiça no dia 6 de setembro de 2015.

O Deputado Hildo Rocha acredita que tais medidas são válidas, independentemente de quão duras sejam, e que "quem for inocente não precisa ter medo. Os bandidos é que estão com seu traseiro apertado, com medo desse projeto"[169]. Verifica-se, portanto, o argumento do "I've got nothing to hide" criticado por Daniel Solove, conforme acima exposto.

De maneira geral, o PL Espião surgiu com o intuito inicial de punir com maior rigor os crimes contra a honra cometidos na internet. O projeto é confuso na abordagem dos conceitos jurídicos que propõe e vai no sentido contrário das discussões realizadas em fóruns públicos a respeito dos dados pessoais, aparentemente em total desconhecimento do avanço dos debates em torno de uma Lei de Proteção de Dados Pessoais.

Em linhas gerais, o PL Espião propõe a exigência, aos provedores de conexão, site ou aplicativo, de que estes coletem os chamados "dados cadastrais" e guardem pelo prazo de um a cinco anos, a depender de a internet ser móvel ou banda larga. Por outro lado, os provedores de aplicações não estão obrigados a efetuar ou manter qualquer tipo de cadastro.

O PL também propõe a ampliação de dados que podem ser acessados sem ordem judicial, ou seja, caso solicitadas tais informações, deverão ser entregues às autoridades para apuração de crimes contra a honra (artigos 7º, § 3º[170], 23-A e 23-B[171] do PL).

---

[169] GIZMODO, *Os problemas do "PL Espião" que muda o Marco Civil para punir calúnias na internet.* Disponível em http://gizmodo.uol.com.br/giz-explica-pl-espiao/, Acesso em 14.3.16.

[170] Art. 7º O § 3º do art. 10 da Lei nº 12.965, de 23 de abril de 2014, passam a vigorar com a seguinte redação: Art. 10. .....

Enfim, observando brevemente as propostas estabelecidas pelo projeto, fica justificado o apelido "PL Espião"; isso porque o projeto coloca um contexto de maior vigilância e monitoramento de internautas a despeito de qualquer suspeita prévia. O projeto foi aprovado na forma de substitutivo (compilados pelos projetos de lei ns. 1.547 e 1.589 de 2015) pela Comissão de Constituição e Justiça dia 6 de setembro de 2015.

2.6. Estudo das versões do projeto de lei de proteção de dados pessoais

Problemas relacionados à privacidade e à coleta e tratamento de dados pessoais no âmbito da internet têm sido debatidos em diversas esferas, acadêmicas e institucionais, ante a multiplicação de problemas atrelados e a popularização de diversos meio, pela internet de compartilhamento de dados.

É certo que a legislação brasileira atual não desconhece a importância do tema da proteção dos dados pessoais, de sorte que

---

§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação, endereço completo, telefone, CPF, conta de e-mail, na forma da lei, pelas autoridades que detenham competência legal para sua requisição, cabendo aos provedores, obrigatoriamente, a adoção de providências de coleta, obtenção, organização e disponibilização dos referidos dados cadastrais de modo a atender o aqui disposto, se e quando por elas requisitados.

[171] Art. 23-A. Observado o disposto neste artigo, a autoridade policial ou o Ministério Público poderão requerer, ao responsável pela guarda, dados cadastrais, no âmbito adequadamente restrito à investigação, para instruir inquérito policial ou procedimento investigatório instaurado para apurar a prática de crime contra a honra cometido com o emprego de equipamento, aparelho, dispositivo ou outro meio necessário à realização de telecomunicação, ou por aplicação de internet, independentemente do meio empregado, desde que o referido requerimento esteja pautado em informações publicadas ou disponibilizadas ao público em geral pelo próprio investigado ou acusado, ou qualquer outro usuário.

§ 1º O requerimento será formulado somente se houver fundados indícios da ocorrência do crime e quando a prova não puder ser feita por outro meio disponível, sob pena de nulidade da prova produzida.

§ 2º O inquérito policial de que trata o caput será concluído no prazo de trinta dias, se o indiciado estiver preso, e de noventa dias, quando solto.

§ 3º Compete ao requerente tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário.

Art. 23-B. Constitui crime requerer ou fornecer registro de conexão ou registro de acesso a aplicação de internet em violação das hipóteses autorizadas por lei.

Pena: reclusão, de dois a quatro anos, e multa.

diversos diplomas em vigor cuidam de trazer regras, ainda que setoriais, acerca da proteção dos dados pessoais. São exemplos o Código de Defesa do Consumidor, a Lei de Cadastro Positivo, inclusive o próprio Código Civil de 2002, ao tratar da privacidade, também afeta, indiretamente a tutela dos dados pessoais, conforme explicado acima.

Do debate referente à proteção de dados pessoais, surgiram três propostas legislativas para consolidação dos direitos dos usuários da internet e dos deveres dos provedores de serviços, de forma a conferir algum grau de estabilidade jurídica a essas relações e permitir o justo equilíbrio entre esses agentes.

A primeira proposta é proveniente do Poder Executivo, consolidada no Projeto de Lei n° 5.276/2016, atualmente em trâmite legislativo perante a Câmara dos Deputados. Este projeto teve origem em interessante processo de audiência pública organizado pelo Ministério da Justiça, no qual, por meio de plataforma acessível *online*, foi possível coletar diversos comentários e sugestões do público em geral, que foram compilados de forma a aperfeiçoar as disposições da lei. O mencionado projeto tramitava em regime de urgência perante a Câmara dos Deputados, porém, em 6 de setembro de 2016, foi cancelado tal regime e o projeto passou a tramitar em regime de prioridade.

A segunda proposta é proveniente do Senado Federal e é uma consolidação dos projetos de lei 330/2013, de autoria do Senador Antônio Carlos Valadares, e 181/2014, de autoria do Senador Vital do Rêgo, ambos atualmente em trâmite na Comissão de Assuntos Econômicos da referida Casa Legislativa sob a relatoria do Senador Ricardo Ferraço. Estes projetos também passaram por audiências públicas na casa legislativa e foram unificados pelo Senador Aloysio Nunes, que apresentou um projeto substitutivo, de forma que todos os projetos tramitam em conjunto.

Por fim, a terceira proposta é proveniente da própria Câmara dos Deputados, materializada no projeto de lei no. 4.060/2012, de autoria do deputado Milton Monti, atualmente em trâmite perante as comissões da Casa legislativa em rito ordinário.

Dessa forma, tem-se três principais proposições em trâmite, que tratam do tema em variações quanto ao grau e extensão

da proteção conferida, cada um com suas peculiaridades, as quais devem ser efetivamente sopesadas quando do processamento deles perante as Casas Legislativas do Congresso Nacional.

Neste trabalho, o recorte analítico para cada um dos projetos será centrado na extensão atribuída ao conceito de dados pessoais e dados anônimos, assim como a respeito do consentimento do usuário para os procedimentos de coleta e tratamento dos referidos dados e aos sistemas de controle atribuídos por cada projeto para a utilização destes.

2.6.1.1. Extensão dos conceitos de dados pessoais e dados anônimos

Uma das questões essenciais a serem tratadas pelos projetos de proteção de dados, o conceito de dados pessoais é trazido expressamente por cada uma das três leis em comento, contudo de formas diversas.

O projeto de lei da Câmara dos Deputados optou pela adoção do conceito mais restritivo de dados pessoais. O artigo 7º, I do projeto tem a seguinte redação: "*Art. 7°. Para os fins da presente lei, entende-se como: I – dado pessoal: qualquer informação que permita a identificação exata e precisa de uma pessoa determinada."*

Ao se referir a "identificação exata e precisa", o autor do projeto deixou clara a opção técnica feita pela restrição do alcance da aplicabilidade da lei somente àquelas hipóteses nas quais o usuário seja plenamente identificado de imediato, constando dados suficientes para precisar sua individualização à margem de qualquer dúvida, sem necessidade de concorrer qualquer outra forma de individualização.

Obviamente uma restrição desta envergadura tornará inaplicável, em uma grande parte das situações, a proteção da lei. Com efeito, são várias as situações nas quais não é possível identificar uma pessoa de forma precisa e exata de pronto, com base nos dados fornecidos, ou seja, são situações nas quais o usuário é tão somente identificável.

Desta forma, uma considerável base de indivíduos será alijada da proteção da lei, pois os dados disponíveis, apesar de não os tornarem plenamente identificados, os tornam identificáveis. A utilização indiscriminada desses dados será juridicamente viável, deixando os direitos individuais dessas pessoas a descoberto da legislação.

De outro lado, o projeto de lei enviado pelo Poder Executivo e aquele elaborado no Senado Federal optaram pela noção mais ampliada de dados pessoais, estendendo-a para abranger, além dos dados que permitam a identificação direta de uma pessoa, também aqueles que a tornem identificável. Assim, dispõe o texto do projeto proposto pelo Poder Executivo:

> Art. 5º Para os fins desta Lei, considera-se: I – dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa.

Já a proposta do Senado Federal, de acordo com o projeto substitutivo proposto pelo Senado Aloysio Nunes, adotou o conceito que segue: "*Art. 3º Para os efeitos desta Lei, considera-se: I – dado pessoal: qualquer informação referente a pessoa natural identificável ou identificada.*"

Percebe-se que entre as duas definições dos dois projetos, existe uma equivalência, diferindo tão somente em questões de estilo que não afetam o conceito do que seria dado pessoal.

O projeto de lei do Poder Executivo adiciona, à definição em comento, em um rol exemplificativo, exemplos de dados que podem ser considerados pessoais, mantendo como característica essencial a pessoalidade dos dados, abrangendo inclusive pessoas identificáveis. De outro lado, o projeto de lei do Senado Federal utilizou-se de uma fórmula mais simples para a elaboração do conceito, deixando clara, contudo, sua opção pela ideia mais extensiva quanto aos dados pessoais. Apesar de singela, em harmonia com os demais dispositivos do projeto, a definição proposta ganha relevância, mormente por ser incisiva ao adotar a noção mais expansionista.

Outro tema importante para o estudo dos dados pessoais e, consequentemente, a ser abordado legislativamente é o conceito de dados anônimos, já tratados com mais profundidade neste trabalho. Neste mister, é interessante destacar que os projetos de lei do Senado Federal e do Poder Executivo, de forma expressa, excluem de sua incidência situações que envolvam dados anônimos ou anonimizados. O artigo 2º, §3º, III do projeto de lei do Senado Federal, neste sentido, foi assim redigido:

> Art. 2°, §3º Esta Lei não se aplica: (...)
>
> IV – à coleta e ao uso de dados anonimizados e dissociados, desde que não seja possível identificar o titular.

O projeto de lei do Poder Executivo não contém dispositivo semelhante ou análogo. Contudo, pela interpretação sistemática dos conceitos de dados pessoais e dados anônimos, assim como pelo disposto no artigo 1º do texto[172], infere-se que a diferença de tratamento entre ambos também foi adotada.

Dos três projetos em análise, somente os projetos oriundos do Poder Executivo e do Senado Federal abordaram de forma direta os dados anônimos. O projeto oriundo da Câmara dos Deputados omitiu-se quanto ao tema, de forma que, caso aprovado, será tarefa doutrinária e jurisprudencial dirimir questões que possam surgir do tema, inclusive no que tange à conceituação e tratamento da anonimização dos dados.

A proposta da Presidência da República traz o conceito de dados anonimizados no artigo 5°, IV, que assim lê:

> Art. 5º Para os fins desta Lei, considera-se:
> (...)
> IV – dados anonimizados: dados relativos a um usuário que não possa ser identificado.

A despeito da concisão do texto sobre dados anonimizados, o texto elaborado pelo Poder Executivo apresenta, em seu artigo 13, interessante disposição sobre o tema, abaixo transcrita:

---

[172] Art. 1º Esta lei dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

> Art. 13. Os dados anonimizados serão considerados dados pessoais, para os fins desta Lei, quando o processo de anonimização ao qual foram submetidos for revertido ou quando, com esforços razoáveis, puder ser revertido.

Por sua vez, o projeto de lei que se originou no Senado Federal conceituou os dados anônimos da seguinte forma:

> Art. 3º, XIV – dado anonimizado ou anônimo: dado relativo a um titular que não possa ser identificado, considerando a utilização dos meios técnicos razoáveis e disponíveis na ocasião de sua coleta ou tratamento.

Das disposições acima destacadas, fica evidente que seus autores preocuparam-se em traçar um limite entre o conceito de dados identificáveis e os dados anônimos ou anonimizados. Para este fim, ambos se socorrem da ideia de razoabilidade. Desta forma, para que um dado seja considerado identificável, pelo texto de ambos os projetos, é necessário que os esforços para identificação de um determinado usuário constante de uma base de dados anônima ou anonimizada sejam feitos dentro de certos parâmetros de razoabilidade.

A diferença entre os projetos reside na atribuição de parâmetros para que seja definido o que são tais "esforços razoáveis". Novamente, o Grupo de Pesquisa em Política Pública para o Acesso à informação, em seu relatório[173] sobre as iniciativas legislativas em comento, destaca a importância da criação de critérios menos abstratos[174] com relação à razoabilidade. Segundo o estudo:

---

[173] Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação. *Op. Cit.*

[174] No estudo mencionado, o grupo de pesquisas buscou classificar as formas de criterização do que seriam esforços razoáveis, chegando à seguinte categorização: "I - silêncio (autorregulação "total"): a legislação apenas enunciaria a razoabilidade, nada dispondo sobre critérios para a sua interpretação e/ou a respeito de um órgão regulador para a sua aplicação. Diante desse silêncio, o próprio mercado se autorregularia. Desse modo, o significado de razoabilidade corresponderia às práticas correntes do mercado sem que houvesse qualquer tipo de ingerência externa para a sua significação; II regulação *ex ante* (autorregulação "parcial" ou heterorregulação "parcial"): aprioristicamente (*ex ante*), a legislação poderia dispor quais seriam os critérios para a aferição do que venha ser razoável, como, por exemplo, o estado da arte da tecnologia e/ou a relação custo financeiro/tempo para se reverter um processo de

> Razoabilidade é um conjunto equívoco que comporta uma série de interpretações. Estabelecer critérios para demarcar uma interpretação objetiva do vocábulo e/ou indicar a quem compete o seu respectivo exercício de significação são possíveis estratégias para mitigar tal exponencialidade. Trata-se, em última análise, de fornecer elementos adicionais para orientar qual sentido deve ser empregada à terminologia em questão.

O projeto de lei do Poder Executivo solucionou a questão atribuindo esta tarefa a um órgão técnico regulador especificamente criado para desenvolver políticas públicas atreladas aos dados pessoais. O texto do artigo 13, §2° do projeto autoriza esta conclusão.

> Art. 13, §2° O órgão competente poderá dispor sobre padrões e técnicas utilizadas em processos de anonimização e realizar verificações acerca de sua segurança.

O artigo 4º traz uma série de princípios[175] que informam o sistema de proteção de dados que busca estabelecer. Obviamente

---

anonimização; II.a como os atores deveriam se comportar para fins de uma eventual autorregulação. Diferentemente da hipótese I, o mercado não seria absolutamente livre para se autonormatizar ou; II.b como o órgão regulador deveria atuar, reduzindo a sua discricionariedade na aplicação da norma; III critérios ao órgão regulador, apostando-se em uma regulação *ex post* que: III.a inviabilizaria a autorregulação do mercado, pelo menos até que sobreviesse a definição dos critérios e a sua respectiva fiscalização pelo órgão regulador; e III.b conferiria maior discricionariedade ao órgão fiscalizador, já que ele não estaria vinculado a critérios predeterminados em lei para a sua atuação – diferentemente da hipótese II.b.

[175] Art. 4º Ao tratamento de dados pessoais aplicam-se os seguintes princípios:
I – coleta, armazenamento e processamento de forma lícita, com observância do princípio da boa-fé e adstritos a finalidades determinadas, vedada a utilização posterior incompatível com essas finalidades;
II – adequação, pertinência, exatidão e atualização, periódica e de ofício, das informações;
III – conservação dos dados e identificação dos seus titulares apenas pelo período necessário às finalidades da coleta ou tratamento;
IV – acesso do titular a informações sobre o tratamento de seus dados;
V – consentimento livre, específico, inequívoco e informado do titular de dados como requisito à coleta de dados pessoais e, ainda, prévio e expresso, quando se tratar de dados sensíveis ou de interconexão internacional de dados realizada por banco de dados privado;

esses princípios podem e devem ser utilizados em cada caso concreto pelo aplicador da lei, de sorte a solucionar os diversos conflitos de interesses que possam surgir de situações ligadas à proteção dos dados pessoais.

Desta forma, fica evidenciado que os projetos de lei de regulação de dados pessoais elaborados pelo Senado Federal e pelo Poder Executivo, no que diz respeito aos temas até aqui abordados, foram mais abrangentes e, de certo modo, mais técnicos do que o projeto elaborado pelos deputados federais.

2.6.1.2. Consentimento do usuário

O consentimento, enquanto manifestação individual e positiva de vontade, desde o advento das reformas liberais tem sido um dos temas centrais no direito, em especial o direito privado.

O Código Civil Brasileiro de 2002, em especial, preocupou-se em buscar a integridade do consentimento do particular, destacando hipóteses de nulidade ou anulabilidade de negócios jurídicos em decorrência de distorções no consentimento e na projeção desta na formação de liames jurídicos entre particulares.

O tema ganhou ainda novos contornos com o advento estudos jurídicos que destacam a importância das relações que envolvem a "hegemonia diagonal", ou seja, a diferença de poder entre particulares, oriundas, normalmente de aspectos extrajurídicos,

---

VI – transparência no tratamento de dados, por meio inclusive da comunicação ao titular de todas as informações relevantes ao tratamento dos seus dados, tais como finalidade, forma de coleta e período de conservação, dentre outras;
VII – proporcionalidade no tratamento dos dados, sendo vedado o tratamento de dados que não seja adequado, necessário e proporcional à finalidade desejada ou que tenha fundamentado sua coleta;
VIII – segurança da informação, por meio do uso de medidas técnicas atualizadas e compatíveis com os padrões internacionais, que sejam aptas a proteger os dados pessoais de destruição, perda, alteração, difusão, coleta, cópia ou acesso indevido e não autorizado;
IX – prevenção, por meio da adoção de medidas técnicas adequadas para minimizar os riscos oriundos do tratamento de dados pessoais;
X – responsabilização e prestação de contas pelos agentes que tratam dados pessoais, de modo a demonstrar a observância e o cumprimento das normas de proteção de dados pessoais;
XI – o tratamento de dados pessoais deve ser compatível com as finalidades a que se destinam e com as legítimas expectativas do titular, respeitado o contexto do tratamento;
XII - tratamento dos dados pessoais limitado ao mínimo necessário e indispensável para as finalidades para que são tratados.

como poderio econômico, político ou social. Exemplos dessa evolução são o Código de Defesa do Consumidor e a Lei de Locação de Imóveis Urbanos, ambas voltadas a suprir uma desigualdade entre particulares, de sorte a manter o equilíbrio contratual e evitar distorções da vontade dos contratantes.

Contudo, por conta dos meios técnicos à disposição e pela própria dinâmica ínsita à formação contratual pela internet, a questão do consentimento há de ser revista, posto que a nova realidade, em muitas ocasiões não encontra perfeito encaixe com as figuras jurídicas já consolidadas.

Neste sentido, Newton de Lucca[176], ao abordar a questão de contratação entre ausentes e presentes e sua aplicação no âmbito de contratações telemáticas, destacou o seguinte:

> (...) não se pode tratar das características da contratação telemática com os mesmos esquemas mentais existentes na tradição jurídica doutrinária, sob pena de incidirmos em discussões absolutamente inúteis.

Sob outro prisma, o consentimento também deve ser objeto de destaque no debate sobre os dados pessoais na internet pois, como já ressaltado neste trabalho, estes últimos têm sido construídos pela doutrina como integrantes do rol dos direitos fundamentais do indivíduo, de forma autônoma e desagregada da privacidade.

A coleta e o tratamento de dados pessoais por terceiros, ainda mais de forma automatizada, deve contar com o consentimento do usuário, justamente pelo fato de integrarem o patrimônio jurídico da cidadania, enquanto direitos fundamentais. Desta afirmação, surgem questões a serem solucionadas, como a forma de externalização, e mesmo a extensão do consentimento, de forma a garantir que o indivíduo mantenha controle e ciência de toda ação que recaia sobre o seu direito à utilização dos dados pessoais.

Preliminarmente, o consentimento, para cada espécie de relação jurídica, pode ganhar diferentes contornos e formas de

---

[176]DE LUCCA, Newton. A*spectos Jurídicos da Contratação Informática e Telemática.* São Paulo: Saraiva, 2003, p. 107.

externalização, conforme as necessidades específicas de cada direito tutelado. A premissa básica que rege toda situação jurídica que envolva o consentimento é o direito que tem cada cidadão de reger sua vida e os negócios que a cercam.

O consentimento, enquanto autorização para que determinada pessoa, física ou jurídica, proceda à coleta e tratamento e dados pessoais de uma outra pessoa, pode ser tratado de formas diversas. Na condição de marco legal, uma lei que regule este assunto deve, necessariamente, abordar em que condições tal consentimento será válido, em que momento e de que forma deve se externar, além do grau de participação do titular dos dados pessoais no controle dos atos.

Considerando esses critérios, além das demais peculiaridades atinentes à internet, é possível vislumbrar que o consentimento para coleta e tratamento de dados pessoais deve guardar cinco características básicas: informado, livre, com finalidade determinada, inequívoco e específico.

Novamente, deve ser ressaltada a conceituação elaborada pelo Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação[177], que explicou a divisão acima mencionada. A primeira característica do consentimento para a coleta e tratamento de dados pessoais é a informação prévia.

A noção por trás de "consentimento informado" é a ideia básica de que, para controlar as operações realizadas com seus dados pessoais, o titular destes deve ser ciência prévia de todo o processado. Qualifica-se pelo fato de que, antes de consentir, incumbe àquele que coleta os dados pessoais levar ao conhecimento de seu titular tudo que se passará, de sorte que este último possa dar seu consentimento ou negá-lo se lhe aprouver.

A segunda característica é a liberdade. Aqui opera a mesma noção de liberdade na declaração de vontade que vige nos atos civis. Desta forma, o consentimento do titular dos dados pessoais deve ser isento de quaisquer vícios que maculem a exteriorização de sua vontade. Cabe uma análise casuística, para, diante dos elementos do caso concreto, ser precisado se houve ou não

---

[177] Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação. *Op. Cit.*

frustração do intento do titular. Essas duas características são o mínimo existencial do consentimento, não sendo admissível qualquer forma de consentimento que não seja minimamente livre e informado.

A terceira característica do consentimento para utilização dos dados pessoais é a especificidade finalística. Não é possível ao titular de dados pessoais conferir liberdade à outra parte para fazer o que bem entender com os dados. O consentimento deve ser dado dentro da realidade da prestação de serviços contratada.

Obviamente, não é possível elencar todo e qualquer ato autorizado. Contudo, o instrumento que materializar o consentimento deve conter um direcionamento mínimo para que seja possível ao titular dos dados pessoais controlar de forma eficaz o que ocorre com esses dados.

Em quarto lugar, o consentimento dado para coleta e tratamento de dados pessoais não pode ser duvidoso, devendo ser inequívoco. Isso não quer dizer que seja necessário ser expresso, podendo ser tácito, desde que revestido de certeza mínima sobre a vontade do titular dos dados pessoais.

Por fim, o consentimento deve ser específico e expresso. Assim, na materialização deste, o titular dos dados pessoais a serem coletados e tratados deve manifestar de forma detalhada e precisa com quais atos consente, sendo o máximo da participação e controle que o titular teria no processo. Não seriam válidos quaisquer atos praticados sem que o titular dos dados pessoais a eles expressamente anua.

O tema não passou despercebido pelos autores dos projetos em comento, tendo sido abordado pelos três textos, em graus diferentes de detalhes e formas diversas de tratamento do assunto.

O projeto da Câmara dos Deputados, em seu artigo 15, de um lado reconhece a autodeterminação do indivíduo em relação aos seus dados pessoais, de outro lado, de forma um tanto lacônica, adotou um sistema de *opt-out*. Por este sistema, em regra, a coleta e o tratamento dos dados pessoais são livres, não dependendo do consentimento. Caberia ao titular dos dados pessoais, manifestar de forma expressa sua intenção de restringir a disposição dos seus dados pessoais.

O texto do artigo do projeto é o seguinte:

> Art. 15. O Titular tem direito a autodeterminação das informações e dados pessoais prestados ou coletados, por qualquer meio.
> Parágrafo Único. O tratamento de dados e o envio de comunicações comerciais ou sociais é permitido, salvo se o titular solicitar o bloqueio do tratamento dos seus dados ou tiver manifestado diretamente ao responsável pelo envio a opção de não recebê-la.

O texto proposto pela Câmara dos Deputados traz duas exceções à regra, em situações nas quais o sistema é o *opt-in*, sendo necessária a autorização prévia do usuário para a coleta e tratamento dos dados pessoais. São os casos de menores de idade e dos dados pessoais sensíveis[178].

> Art. 12. O início do tratamento de dados pessoais sensíveis, quando não solicitado pelo titular, somente ocorrerá mediante autorização deste, por qualquer meio que permita a manifestação de sua vontade, ou na hipótese de imposição legal.
> Art. 17. O tratamento de dados pessoais de crianças somente será possível mediante o consentimento dos seus pais, responsáveis legais ou por imposição legal.

Ainda, o artigo 18 do texto também expressa que é ilícito o uso de coação ou dolo para as operações abrangidas pelo projeto. Trata-se aqui de uma obviedade, posto que seria inadmissível qualquer lei que autorizasse essas práticas.

Assim, a Câmara dos Deputados, no seu projeto de lei, propõe que o consentimento seja meramente despido de vícios, adotando tão somente um sistema básico de proteção que, em

---

[178] Cabe destacar que a noção de "dados sensíveis" no projeto da Câmara dos Deputados é trazida pelo Art. 7º, IV, que assim dispõe: Art. 7º Para os fins da presente lei, entende-se como: IV - dados sensíveis: informações relativas à origem social e étnica, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas do titular;

diversas ocasiões, poderá deixar descoberto o titular dos dados pessoais, que se verá na necessidade de recorrer a outros sistemas normativos, como o Código de Defesa do Consumidor.

Por sua vez, o sistema proposto no substituto do projeto de lei do Senado Federal adota o sistema de proteção máxima ao titular dos dados pessoais. Com efeito, o texto remete expressamente a um consentimento "livre, específico, inequívoco e informado" a ser concedido pelo titular dos dados pessoais.

O texto do projeto a esse respeito é o seguinte:

> Art. 6º São direitos básicos do titular: (...)
>
> IV – consentimento livre, específico, inequívoco e informado sobre coleta, armazenamento e tratamento de dados pessoais, que deverá sempre ocorrer de forma destacada;
>
> Art. 12. O tratamento de dados pessoais somente pode ser realizado nas seguintes hipóteses:
>
> I – mediante consentimento livre, específico, inequívoco e informado concedido pelo titular dos dados;

O artigo 13 do projeto também vem corroborar e especificar qual o conteúdo do consentimento a ser prestado, nestes termos: "*Art. 13. O consentimento do titular deve ser prestado de forma apartada do restante das declarações e dizer respeito a finalidade legítima, específica e delimitada.*"

Desta forma, é evidenciada a tendência do projeto de qualificar o consentimento do titular dos dados pessoais. Como se vê, este deve ser, inclusive específico, sendo dever daquele que pretender a utilização destes dados informar detalhadamente ao seu titular quais serão e qual a destinação dos dados pessoais que forem coletados, que deve manter coerência com as atividades.

Já o projeto do Poder Executivo tem uma proposta semelhante à que trazem os Senadores. Contudo, dista do projeto apresentado por estes últimos ao não mencionar, dentre as características do consentimento para coleta e tratamento de dados pessoais, que este seja específico. O texto que traz é o seguinte:

> Art. 5º. Para os fins desta Lei, considera-se:
>
> (...)
>
> VII – consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
>
> Art. 7°. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I – mediante o fornecimento pelo titular de consentimento livre, informado e inequívoco

O tratamento conferido pelo Poder Executivo no seu projeto é dotado de um grau intermediário de participação do titular dos dados pessoais. A desnecessidade de atribuição específica dos dados pessoais que são objeto do consentimento é, de fato, um fator que reduz a possibilidade de controle do titular destes.

Contudo, o projeto do Poder Executivo aborda, de forma expressa, que a finalidade dos dados deve ser determinada quando da expedição do consentimento livre[179]. Com este elemento, é possível ao titular dos dados pessoais efetuar um controle do uso destes pelo método finalístico, buscando proibir que aquele que faz uso dos dados se afaste do que foi autorizado.

2.6.1.3. Sistemas de controle ("freios e contrapesos")

Outro tema de especial relevância para fins de construção legislativa de um marco civil de proteção de dados pessoais é a criação de mecanismos que permitam ao titular destes dados fazer sustar de forma eficaz o abuso na utilização dos dados, considerando-se os parâmetros consentidos quando do início da coleta dos dados, conforme acima exposto. Trata-se de conferir efetividade jurídica aos direitos dos titulares de dados pessoais,

---

[179] Ao definir o que é consentimento livre, o projeto de autoria do Poder Executivo optou por arrolar certos vícios do consentimento, remetendo o intérprete aos conceitos estabelecidos no Código Civil para este ofício (i.e. o consentimento não poderá ser obtido mediante erro, dolo, coação, estado de perigo ou simulação).

consagrados pelo sistema normativo desde a Constituição Federal e o sistema normativo internacional até os projetos em discussão.

Na relação que se estabelece entre o titular dos dados pessoais e o fornecedor de serviços pela internet que pretende sua coleta e tratamento, o primeiro sistema de limites à atuação destes é o consentimento do usuário. Com efeito, o usuário, ao consentir de maneira livre e informada, efetua um controle, ainda que de forma precária, sobre aquela atividade.

De outro lado, considerando a natureza dos interesses em jogo, conforme já discorrido anteriormente neste trabalho[180], é inviável considerar que o consentimento seja definitivo ou eterno. O controle do usuário deve, inclusive, abranger a possibilidade de se retratar de seu consentimento a qualquer momento, de sorte que lhe seja concedido controle total sobre seus dados pessoais, enquanto integrantes da personalidade humana.

Desta forma, os projetos de lei ora sob análise não são isentos a esta discussão, sendo que todos eles trazem também dispositivos neste sentido, conferindo aos titulares dos dados pessoais instrumentos jurídicos que permitam a cessação da coleta e do tratamento destes dados quando bem lhe aprouverem.

O projeto de lei da Câmara dos Deputados traz os seguintes dispositivos a esse respeito:

> Art. 13. O tratamento de dados pessoais ou a sua interconexão respeitará a lealdade e boa fé, de modo a atender aos legítimos interesses dos seus titulares, lhes devendo ser garantido sempre o direito ao bloqueio do registro, salvo se necessário para cumprimento de obrigação legal ou contratual.
> Art. 15. O Titular tem direito a autodeterminação das informações e dados pessoais prestados ou coletados, por qualquer meio.
> Art. 19. O titular poderá, a qualquer momento, requerer o bloqueio do tratamento de seus

[180] Neste sentido, é salutar mencionar o que diz o artigo 11 do Código Civil: Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

> dados pessoais, salvo se a manutenção do tratamento for necessária à execução de obrigações legais ou contratuais.

Estes dispositivos, conforme o texto proposto, têm condições de conferir um mínimo existencial de garantias a direitos da personalidade atrelados aos dados pessoais, instrumentalizando a defesa destes direitos.

Por sua vez, o projeto do Poder Executivo também tratou do tema, conferindo ao titular dos dados pessoais o direito de revogar o consentimento dado a qualquer momento, desde que o faça mediante manifestação expressa. Os dispositivos que fundamentam essa conclusão são:

> Art. 9º: (...)
> §5º O consentimento pode ser revogado a qualquer momento, mediante manifestação expressa do titular.
> Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
> (...)
> IV – comunicação do titular, inclusive no exercício do seu direito de revogação do consentimento, conforme art. 9º, §5º.

O projeto do Poder Executivo Federal traz um capítulo inteiro que detalha os direitos dos titulares dos dados pessoais, também informando os meios para efetivar estes direitos. Destacam-se as seguintes disposições:

> Art. 18 (...)
>
> §2º: Os direitos previstos neste artigo serão exercidos mediante requerimento do titular a um dos agentes de tratamento, que adotará imediata providência para seu atendimento.
>
> Art. 20. O titular dos dados tem direito a solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive as decisões destinadas a definir o seu perfilo ou avaliar aspectos de sua personalidade.

Já o projeto do Senado Federal também aborda a exclusão do consentimento como forma de controle da atuação do agente que colete e trate dados pessoais. Da mesma forma considerando-a um direito do titular, é expresso neste sentido, embora de forma não tão incisiva quanto o que propõe o Poder Executivo. É o texto: "*Art. 16. O tratamento de dados pessoais será encerrado: IV - mediante solicitação do titular, ressalvadas as demais previsões legais."*

Neste aspecto, o projeto substitutivo do Senado é mais conciso do que os outros dois, posto que trata do assunto em somente um dispositivo. Contudo, em decorrência das demais disposições da lei, o sistema protetivo se aperfeiçoa, pois outras ferramentas são colocadas à disposição do titular dos direitos pessoais.

Em um terceiro ponto relevante, observando a tendência legislativa e jurisprudencial de valorizar a solução de conflitos por meio de tutela transindividual, os três textos ora analisados reconhecem a natureza de direito coletivo dos interesses dos usuários e autorizam a tutela dos direitos destes pela via coletiva, por meio de ações civis públicas, termos de ajustamento de conduta, dentre outros instrumentos. Trata-se de forma eficaz de balancear o poder que detêm aqueles que coletam dados pessoais sobre os direitos dos titulares destes. Também implica conferir mais efetividade à tutela, que é sempre melhor protegida quando se engajam atores com poder político, como o Ministério Público ou associações de defesa do consumidor.

Neste sentido, o texto da Câmara dos Deputados dispõe:

> Art. 22. Sem prejuízo das sanções cabíveis, os órgãos e entidades previstos no artigo 82 da Lei 8.078/90, além das associações legalmente constituídas há pelo menos 1 (um) ano, poderão promover a celebração de Compromissos de Ajustamento de Conduta (CAC) com responsáveis que incorram em infração às normas desta lei, visando a adoção de medidas corretivas que considerem necessárias para reverter os efeitos danosos que a conduta infratora tenha causado e para evitar que esta se produza novamente no futuro.

Por sua vez, o texto do projeto enviado pelo Poder Executivo Federal preconiza que:

> Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo individual ou coletivamente, na forma do disposto na Lei 9.507, de 12 de novembro de 1997, nos artigos 81 e 82 da Lei nº 8.078, de 11 de setembro de 1990, na Lei nº 7.347, de 24 de julho de 1985, e nos demais instrumentos de tutela individual e coletiva.

Ainda, o Senado Federal propõe o seguinte texto:

> Art. 11. Em caso de violação desta Lei, o titular poderá pleitear os seus direitos perante as autoridades administrativas competentes e o Poder Judiciário.
>
> Parágrafo único. A defesa dos interesses e dos direitos estabelecidos nesta Lei poderá ser exercida administrativamente ou em juízo, individual ou coletivamente, na forma da lei.

Sobrepondo-se os três textos, para efeitos comparativos, é possível vislumbrar que o que trouxe o texto do Poder Executivo é tecnicamente mais elaborado que os demais e faz referência direta às fontes legislativas que regem o processo coletivo. Contudo, os outros textos trazem, ainda, referências sólidas ao sistema de defesa de direitos individuais e coletivos, trazendo a robustez desse tipo de tutela também ao mundo dos dados pessoais.

Por fim, não é escopo deste trabalho esgotar a análise do tema pertinente aos projetos de lei, posto que muitos outros dispositivos em cada um dos textos merecem destaque.

Com efeito, cada um deles traz um rol, mais ou menos extenso, de regras e princípios invocáveis para a regulamentação da coleta e do tratamento de dados pessoais no âmbito da internet, sempre com o escopo definido de coibir abusos e proteger os direitos dos usuários.

É possível vislumbrar que o trabalho legislativo preocupou-se com questões que vão desde o consentimento do titular, aqui tratado, passando pelo direito à obtenção de informação,

até a estipulação de obrigações pertinentes à própria administração pública. Neste último tema, é interessante destacar que a administração pública, de acordo com a maioria das propostas, terá papel fundamental na defesa dos direitos dos titulares de dados pessoais, elaborando normas e padrões técnicos que permitam o respeito aos direitos destes. Desta forma, remete-se à leitura de trabalhos mais específicos sobre o assunto, posto que aqui foram selecionados pontos específicos dos textos legislativos que dizem respeito ao tema desta dissertação.

CAPÍTULO 3: ANONIMATO NA INTERNET

A discussão sobre o anonimato não trata apenas da liberdade para se manifestar com uma máscara ou sem identificação na internet, mas também de atribuir limites ao monitoramento de qualquer atividade *online* e dar ao usuário controle dos seus dados.

Paul Ohm afirma que cientistas da computação minaram nossa fé no poder da anonimização (nome de técnicas para proteger a privacidade de indivíduos em grandes bancos de dados), que teoricamente seria capaz de excluir informações coletadas dos usuários como nomes e números de segurança social (*social security number*). Esses cientistas demonstraram que muitas vezes tais dados podem ser reidentificados ou desanonimizados com incrível facilidade[181].

No mesmo sentido, conforme mencionado na introdução, para Paul Schwartz e Daniel Solove, dados pessoais (identificados) dizem respeito a uma pessoa específica enquanto dados identificáveis (anônimos) sugerem a relação do dado com uma pessoa determinada. No caso dos dados anônimos a conexão (entre o dado e a pessoa) ainda não ocorreu, porém, há a possibilidade de ocorrência de tal conexão a qualquer momento por meios que transformem tais dados anônimos em dados pessoais[182].

Da mesma forma, os integrantes do Grupo de Pesquisa em Políticas Públicas Para o Acesso à Informação da Universidade de São Paulo destacam, em estudo publicado no ano de 2015, que a existência de dados anônimos, ou não identificáveis é algo impossível do ponto de vista da ciência da análise de dados[183].

---

[181] OHM, Paul. *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* UCLA Law Review, vol. 57, 2010. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006. Acesso em 15.mar.2017. p. 1701.

182 SCHWARTZ, Paul; SOLOVE, Daniel J. The PII Problem: privacy and a new concept of personally identifiable information. 86 N.Y.U. L.Q. Rev. 1814 (2011). Disponível em http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2638&context=facpubs Acesso em 03.mar.2017 p. 1873 e 1874. No original: "Identified information already refers to a specific person, while identifiability suggests that such a connection has not yet occurred, but is possible

[183] Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação. *Op.Cit.*

Nesse sentido, deve-se observar que, para que haja real proteção dos dados pessoais, os dados pessoais identificados e identificáveis (anônimos) deverão ser protegidos, seja porque (i) os processos de anonimização são reversíveis, ou (ii) os dados considerados anônimos podem deixar de ser por meio de processos de reidentificação e desanonimização do usuário.

Conforme dispõe Mariana Cunha e Melo[184], existem três motivos para se identificar a relevância da discussão sobre o anonimato na internet: (i) evitar a vigilância dos usuários; (ii) para que os usuários tenham controle do fluxo de informações sobre si mesmos; e (iii) para fomentar o fórum público da internet.

O direito de evitar a vigilância e a possibilidade de vigilância é extremamente relevante no contexto da sociedade informacional, que está progressivamente mais e mais implicado em iniciativas de vigilância absoluta. É importante notar que "*ainda que não haja efetiva vigilância sobre todas as pessoas a todo o tempo, a possibilidade de vigilância provoca efeitos no comportamento das pessoas e na sua percepção de liberdade*"[185].

A esse respeito, Danilo Doneda ensina que a perda de controle da pessoa sobre o que sabe em relação a ela mesma ocorre diuturnamente no contexto em que os dados pessoais passam a ser os intermediários entre a pessoa e a sociedade. Em última análise, a perda desse controle representa uma diminuição da própria liberdade[186].

Além disso, Mariana Cunha Melo afirma que o anonimato na internet também tem um viés de empoderamento, que é permitir o controle do fluxo de informações sobre si. Trata-se de dar aos usuários o poder de proteger seus próprios dados da vigilância privada ou do Poder Público: essa é uma das funções mais poderosas do anonimato na internet.

No atual contexto em que estamos inseridos, isto é, sem que haja verdadeiramente a possibilidade de anonimato na internet, a

---

184 MELO, Mariana Cunha e. *Anonimato, proteção de dados e devido processo legal: por que e como conter uma das maiores ameaças.* Disponível em https://itsrio.org/wp-content/uploads/2017/03/Mariana-Cunha-e-Melo-V-Revisado.pdf Acesso em 02.fev.2017 p. 2

185 *Idem.* p. 3

186 DONEDA, Danilo. *A proteção de dados pessoais nas relações de... Op. Cit.* p 84.

vigilância continuar a existir de forma devastadora. Nesse sentido, Ascensão ensina que, em termos gerais, a sociedade informacional nasce com uma ínsita contradição fundamental: o acesso amplo ao conteúdo produzido mas, em contrapartida, um profundo desequilíbrio no que diz respeito ao domínio da informação[187].

Por fim, Mariana Cunha Melo ensina que muitas ideias são objeto de represália no grande mercado de ideias que é a internet:

> internet é considerada o grande mercado de ideias hoje, um fórum público. Muitas ideias e opiniões, contudo, são objeto de represálias de todas as formas – inclusive pela violência física. Nesse sentido, vale registrar o trabalho de ONGs como a Association for Progressive Communications (APC), que combate violência contra mulheres na internet, da Derechos Digitales, que promovem campanhas para o uso seguro da internet para fins de propagação de ideias, da Electronic Frontier Foundation e da Access Now, duas das maiores organizações mundiais de defesa dos direitos civis na internet. Em muitos casos, esconder a identidade dos ativistas é a primeira fronteira de defesa contra violência na internet. Há, portanto, um interesse na defesa do anonimato na internet – ao menos em alguma medida e em certas circunstâncias[188].

Dessa forma, considerando sua relevância, a discussão sobre o anonimato deverá ser aprofundada para que se tenha consciência do que sua ausência causa de efeitos na sociedade.

3.1. Definição de anonimato

Kathleen Wallace, professora de filosofia, ensina que "*ser anônimo é ser não identificável sob algum ponto de vista ou em*

---

[187] ASCENSÃO, José de Oliveira. *O direito.... Op. Cit.*

[188] MELO, Mariana Cunha e. *Anonimato, proteção de dados e devido processo legal: por que e como conter uma das maiores ameaças.* Disponível em https://itsrio.org/wp-content/uploads/2017/03/Mariana-Cunha-e-Melo-V-Revisado.pdf Acesso em 02.fev.2017 p. 2

algum contexto"[189]. A autora continua afirmando que a definição de anonimato é cumulativa já que a afirmação acima deve ser complementada pela:

> (...) não coordenabilidade de características, constituindo relação entre pessoa anônima e outros, em que a primeira é conhecida apenas por meio de traços que não são coordenáveis com outros que permitam a identificação da pessoa como um todo[190].

Para Maria Helena Diniz, o conceito de anonimato pode ser conceituado da seguinte forma:

> 1. Ato de escrever anonimamente, ou seja, sem identificação, passando os direitos autorais ao editor. 2. Condição do autor de algum escrito não assinado. 3. Condição de alguém que, tendo nome, o oculta. 4. Causa de apreensão policial de impresso que exprima o exercício de liberdade de manifestação do pensamento e de informação sem conter a identificação de seu autor. 5. Abuso de liberdade de pensamento que pode ser punido criminalmente. 6. Ação de uma pessoa que, ao ocultar seu nome, vem a atacar outra, injuriando-a, caluniando-a ou difamando-a, procurando esquivar-se, assim, da responsabilidade[191].

Pode-se dizer, portanto, que o anonimato pressupõe uma relação social. O anonimato pode ser implementado para tornar impossível ou muito difícil descobrir o verdadeiro autor de uma mensagem.

---

[189] WALLACE, Kathleen A. *Anonymity. Ethics and information technology,* Dordrecht, v. 1, n. 1. ,p. 23.
No original: "To be anonymous is to be non-identifiable in some respect or context".
[190] Idem. p. 24..
No original: "(…) anonymity is noncoordinatability of traits in a given respect. In other words, one has anonymity or is anonymous when others are unable to relate a given feature of the person to other characteristics. For example, the Unabomber was anonymous when he was known only as 'sender-of-bombs-to-computer-scientists' and that trait could not be related to (coordinated with) other traits such as name, address, social security number, and so on, such that the person as such could be identified".
[191] DINIZ, Maria Helena. Dicionário Jurídico. 2ª ed. rev., atual. e aum. São Paulo: Saraiva, 2005.

Ainda de acordo com Wallace[192], o anonimato pode se apresentar sob aspectos positivo e negativo. No ponto de vista positivo, destaca-se o encorajamento à liberdade de expressão, promovendo a proteção do autor de reações negativas, além de favorecer a proteção de dados pessoais. Sob o ponto de vista negativo, o anonimato pode ser utilizado para realização de dados ilícitos, tornando impunes autores de crimes virtuais ou de discursos de ódio.

Ou seja, o anonimato e o pseudônimo podem ser utilizados simplesmente como forma de exercício da cidadania ou para prejudicar terceiros. Também pode, em determinados casos, ser desejável para uma pessoa e não desejável para outra pessoa, no seguinte sentido: uma empresa pode, por exemplo, não gostar que um funcionário divulgue informações sobre práticas impróprias dentro da empresa, mas a sociedade como um todo pode achar importante que essas práticas impróprias sejam publicamente expostas.

Nada obstante a discussão sobre o conceito de anonimato ser relevante sob o aspecto de tratamento automatizado de dados pessoais na internet, a literatura tem demonstrado ceticismo, já que grande parte dos dados pessoais podem ser reidentificados ou associados entre si para chegar ao indivíduo na ponta.

Neste sentido, ensinam Vitaly Shmatikov e Arvind Narayanan:

> Algoritmos de reidentificação são agnósticos quanto à semântica dos elementos de dados. Acontece que existe um amplo espectro de características humanas que permitem a reidentificação dos dados, como: preferências de consumo, transações comerciais, navegação na web, históricos de pesquisa, e por aí vai. Suas duas principais propriedades são que (1) eles são razoavelmente estáveis através do tempo e de contextos, e que (2) os atributos de dados correspondentes são suficientemente

[192] WALLACE, Kathleen A. *Anonymity... Op. Cit. p. 23.*

> numerosos e apurados para que seja muito improvável encontrar duas pessoas similares[193].

3.2. Anonimização e a desanonimização pela reidentificação de dados

A anonimização e a possibilidade de desanonimização por meio da reidentificação de dados são fatores que precisam ser estudados quando o assunto se volta para o anonimato e a proteção de dados pessoais na internet.

A anonimização dos dados é definida como uma técnica que busca proteger dados, excluindo ou criptografando informações de identificação pessoal de um banco de dados, ou seja, abrange uma diversidade de métodos que podem ser usados para converter dados pessoais em dados anonimizados. Essa técnica é executada com a finalidade de proteger as atividades privadas de um indivíduo ou empresa, mantendo a integridade dos dados coletados e compartilhados. Teoricamente, a partir da anonimização de dados os registros individuais não podem ser vinculados de volta a um indivíduo.

O Grupo de Ensino e Pesquisa em Inovação da FGV afirma que a anonimização dos dados obriga o seu tratamento de modo que não seja possível a guarda de referências individualizadas em relação a nenhuma pessoa natural em específico:

> Trata-se de elemento frequentemente tido como essencial à garantia do direito à privacidade, uma vez que obriga o tratamento de dados de modo que ele não guarde mais referências individualizadas a nenhuma pessoa natural em específico. No entanto, a própria possibilidade de anonimização total e irreversível de dados pessoais é tecnicamente questionável, uma vez que a emergência de novas técnicas de engenharia reversa pode reverter esse tipo de tratamento, possibilitando a identificação de indivíduos específicos. Nesse sentido, mesmo

---

[193] SHMATIKOV, Vitaly e NARAYANAN, Arvind. *Privacy and Securiry: Myths and Fallacies of "Personally Identifiable Information.* p .26. Disponível em http://www.cs.utexas.edu/users/shmat/shmat_cacm10.pdf Acesso em 6.mar.2017.

> anonimizados, tais dados continuariam a ser pessoais, pois ainda seriam referentes a pessoas identificáveis, ainda que não identificadas.[194]

Como anteriormente afirmado, infelizmente a proteção dos dados na internet ainda está concentrada em apenas três pilares: o consentimento livre e esclarecido, a possibilidade de exclusão dos dados e a anonimização dos dados.

O consentimento livre e esclarecido está relacionado à livre escolha individual (desde que esclarecida), o sistema *opt out* prevê a possibilidade de exclusão dos dados e a anonimização se utiliza de mecanismos que podem desconectar informações de interesse dos dados que realmente identificam as pessoas.

Neste sentido, Cíntia Rosa Pereira de Lima esclarece as três medidas não passam de uma falácia, já que nenhuma delas garante verdadeiramente a proteção de dados pessoais[195]. Em relação à anonimização, a autora afirma que "*é possível, através de associações e tratamento de dados, partir de um dado anônimo e chegar a informações pessoais que revelem opção sexual, filiação partidária, convicções religiosas e etc.*"

Tais informações são as relacionadas ao que se chama de dado sensível. Apesar de não haver ainda uma definição legal sobre o que são dados sensíveis, a prática do direito criou essa categoria apartada definida por Danilo Doneda como sendo um conjunto de informações que poderiam se prestar à utilização discriminatória ou lesiva ao indivíduo, veja-se:

---

[194] Grupo de Ensino e Pesquisa em Inovação FGV. U*m novo mundo de dados*. Disponível em https://direitosp.fgv.br/sites/direitosp.fgv.br/files/arquivos/unmd_policy_paper_fgv.pdf Acesso em 10.dez.2017. p.11.

[195] LIMA, Cíntia Rosa Pereira de. *A imprescindibilidade... Op Cit.* p. 51.
Veja-se: "Contudo, tais medidas não nos parecem suficientes. Primeiro porque o consentimento, que deve ser livre e informado, não o é tendo em vista os longos termos e condições utilizados pelas grandes empresas que inviabilizam o real conhecimento pelos indivíduos que anuem sem saber ao certo com o quê.
Segundo porque o sistema *opt out*, muitas vezes, é utilizado justamente para continuar rastreando as atividades dos indivíduos.
E, terceiro, porque já é cediço que a anonimização de dados na economia informacional é uma falácia já que é possível, através de associações e tratamento de dados, partir de um dado anônimo e chegar a informações pessoais que revelem opção sexual, filiação partidária, convicções religiosas e etc."

> informações que que, se conhecidas e processadas, prestariam-se a uma potencial utilização discriminatória ou lesiva, particularmente mais intensa e que apresentaria maiores riscos potenciais que a média. Alguns destes dados seriam as informações sobre raça, credo político ou religioso, opções sexuais, histórico médico ou dados genéticos de um indivíduo[196].

Nesse sentido, fica evidente que a violação de dados sensíveis é muito mais prejudicial para o indivíduo, podendo gerar danos intensos a ele, sendo que o mau uso desses dados pode gerar maiores possibilidades de discriminação do indivíduo[197].

Os dados pessoais (sensíveis ou não) que teoricamente são anônimos podem ser reidentificados com incrível facilidade. A literatura sobre o tema sempre aponta três grandes casos a esse respeito: (i) divulgação pelo Estado de Massachusetts de dados anonimizados relacionados à saúde de seus funcionários; (ii) AOL em 2006; (iii) Netflix em 2006.

A Comissão de Seguros do Estado de Massachusetts teve uma ideia brilhante em meados da década de 1990: decidiu divulgar dados anônimos sobre funcionários do Estado que mostravam suas visitas ao hospital. O objetivo era ajudar os pesquisadores e o Estado passou o tempo removendo os identificadores óbvios (como nome, endereço e número da Segurança Social). Mas uma estudante de pós-graduação em informática viu uma chance de fazer uma análise sobre os limites da anonimização[198].

---

[196] DONEDA, Danilo. *Da privacidade... Op. Cit*. p. 160/161

[197] *Idem.* p. 163.

[198] MONTJOYE, Yves-Alexandre de. *Unique in the… Op. Cit…*

Comentando o caso da divulgação de dados pela Comissão de Seguros do Estado de Massachusetts, Yves-Alexandre de Montjoye et. al. afirmam: *"A simply anonymized dataset does not contain name, home address, phone number or other obvious identifier. Yet, if individual's patterns are unique enough, outside information can be used to link the data back to an individual. For instance, in one study, a medical database was successfully combined with a voters list to extract the health record of the governor of Massachusetts. In another, mobile phone data have been re-identified using users' top locations. Finally, part of the Netflix challenge dataset was re-identified using outside information from The Internet Movie Database".*

Latanya Sweeney solicitou uma cópia dos dados e foi trabalhar em sua busca de "reidentificação". Não foi difícil. O professor de direito Paul Ohm descreve o trabalho de Latanya Sweeney:

> No momento em que foram lançados os dados, William Weld, então governador de Massachusetts, assegurou ao público que eles protegeriam a privacidade do paciente, já que haviam excluido os identificadores. Em resposta, a estudante de pós-graduação, Sweeney, começou a procurar os registros do hospital do próprio governador nos dados disponibilizados. Ela sabia que Governor Weld residia em Cambridge, Massachusetts, uma cidade de 54.000 habitantes e sete códigos postais. Por vinte dólares, ela comprou os roteiros de eleitores completos da cidade de Cambridge, um banco de dados contendo, entre outras coisas, o nome, endereço, CEP, data de nascimento e sexo de cada eleitor. Ao combinar esses dados com os registros do disponibilizados, Sweeney encontrou o Governor Weld com facilidade. Apenas seis pessoas em Cambridge compartilharam sua data de nascimento, apenas três deles homens, e apenas ele morava no CEP. Em um floreio teatral, Sweeney enviou os registros de saúde do governador (que incluiu diagnósticos e prescrições) em seu escritório [199].

Além disso, em 2000, Latanya demonstrou que 87% de todos os norte-americanos poderiam ser identificados de maneira exclusiva usando apenas três bits de informação: código postal, data de nascimento e sexo[200].

Da mesma forma, quando os pesquisadores da AOL lançaram um conjunto de dados massivo de consultas de pesquisa, primeiro eles anonimizavam os dados retirando os IDs de usuários e

---

[199] OHM, Paul. *Broken... Op. Cit.* p. 1719.

[200]SWEENEY, Latanya. Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000. Disponivel em https://dataprivacylab.org/projects/identifiability/paper1.pdf. Acesso em 05.mar.2018.

endereços IP. Quando a Netflix disponibilizou para estudos um enorme banco de dados de recomendações de filmes, ela retirou as informações obviamente identificáveis dos dados. Ainda assim, os cientistas da computação conseguiram identificar usuários individuais utilizando os dados supostamente anonimos.

No caso da AOL, o problema era que os IDs de usuários foram removidos, mas foram substituídos por um número que identificou de forma exclusiva cada usuário. Isso parecia uma boa ideia na época, pois permitiu que os pesquisadores usassem os dados para ver a lista completa das consultas de busca de uma pessoa, mas também criou problemas. Essas listas completas de consultas de pesquisa eram tão completas que os indivíduos podiam ser rastreados simplesmente com base no que buscavam. Como observa Paul Ohm, isso ilustra uma realidade central da coleta de dados: os dados podem ser úteis ou perfeitamente anônimos, mas nunca os dois[201].

Quando a Netflix disponibilizou para estudos um enorme banco de dados de recomendações de filmes, ela retirou as informações obviamente identificáveis dos dados. Ainda assim, os cientistas da computação conseguiram identificar usuários individuais utilizando os dados supostamente anonimos. O caso Netflix ilustra outro princípio, que é o de que os dados em si podem parecer anônimos, mas quando eles são emparelhados com outros dados existentes, a reidentificação torna-se possível. Cientistas da computacao, filtrando as recomendações de filmes encontrados no Internet Movie Database (IMDB) com os dados da Netflix; foram capazer de identificar com facilidade os usuários a partir dos dados disponibilzados pelo Netflix.

Um estudo mais recente realizado por Yves-Alexandre de Montjoye et. al demonstraram como os dados anonimizados de uma empresa de telefonia europeia (provavelmente uma na Bélgica) poderiam ser reidentificados com 95% de precisão, com apenas quatro pontos de dados sobre cada pessoa (diga-se que, com apenas

---

[201] OHM, Paul. Broken.. Op. Cir. p. 1704.
No original: "This research unearths a tension that shakes a foundational belief about data privacy: Data can be either useful or perfectly anonymous but never both".

dois pontos de dados, mais da metade dos usuários no conjunto poderia ser reidentificado). [202]

Tais resultados são, obviamente, problemáticos em um mundo onde o Facebook. por exemplo[203], conserva dados por anos, realizando a anonimização depois de um certo período de tempo, mas mostrando reticência para excluí-lo completamente. A ciência da reidentificação mina a fé que colocamos na anonimização e perturba o panorama da política de privacidade, escreve Paul Ohm. E continua, afirmando que a fé que temos na anonimização é grande,

A ciência da reidentificação mina a fé que colocamos na anonimização e perturba o panorama da política de privacidade, escreve Paul Ohm. E continua, afirmando que a fé que temos na anonimização é grande,

> pois os tecnólogos contam com ela para justificar o compartilhamento de dados de maneira indiscriminada e o armazenamento de dados perpétuo, ao mesmo tempo prometendo aos seus usuários (e ao mundo) que eles estão protegendo sua privacidade. Os avanços na reidentificação de dados expõem essas promessas (de anonimização) como muitas vezes ilusórias [204].

Para os usuários, a perspectiva de vazamento secreto para o público cresce à medida que proliferam bancos de dados. Aqui está o cenário do pesadelo de Paul Ohm, que afirma que *"para quase*

---

[202] MONTJOYE, Yves-Alexandre de, César A. Hidalgo, Michel Verleysen & Vincent D. Blonde. *Unique in the Crowd: The privacy bounds of human mobility*. Scientific Reports 3, Article number: 1376 (2013) doi:10.1038/srep01376. Disponível em https://www.nature.com/articles/srep01376. Acesso em 25.mar.2017.

[203] FACEBOOK, Como faço para gerenciar ou excluir informações sobre mim? Disponível em https://www.facebook.com/privacy/explanation Acesso em 08.dez.2017.
Em sua página de política de dados, a rede social afirma o seguinte: "Nós armazenamos dados pelo tempo necessário para fornecer produtos e serviços para você e outras pessoas, inclusive as descritas acima. As informações associadas à sua conta serão mantidas até que ela seja excluída, a menos que não precisemos mais dos dados para fornecer produtos e serviços"

[204] *Idem.* p. 1704.
No original: "Reidentification science disrupts the privacy policy landscape by undermining the faith we have placed in anonymization. This is no small faith, for technologists rely on it to justify sharing data indiscriminately and storing data perpetually, while promising users (and the world) that they are protecting privacy. Advances in reidentification expose these promises as too often illusory".

todas as pessoas na terra, há pelo menos um fato sobre ele armazenado em alguma base de dados que pode ser considerada a 'base de dados da ruína'" caso algum adversário tenha acesso a tais informações [205].

Neste sentido, Cory Doctorow ensina que, quando uma regulamentação vem faceiramente determinar que alguns dados são "anônimos" ou mesmo "pseudônimos", essa regulamentação está gritantemente desconectada das melhores teorias de que dispõe a ciência da computação.[206]Assim, deve-se observar que quaisquer dados teoricamente podem ser anonimizados na tentativa de que seu titular não seja identificado, porém, na prática, não é isso o que ocorre. Por isso, dados pessoais identificados e identificáveis deverão ser protegidos quando sobrevier uma lei de proteção de dados no Brasil.

3.3. Métodos para anonimização de dados

A anonimização de dados ocorre em diversos contextos. Um exemplo recorrente trata da situação em que um hospital pretende compartilhar dados específicos de seus pacientes sem que estes possam ser identificados individualmente. Nesse momento, os técnicos de informática se valem da chamada anonimização, na tentativa de que os sujeitos não sejam identificados.

Em linhas gerais, existem duas estratégias para a anonimização de dados pessoais. A primeira é baseada na supressão e a segunda parte da ideia da generalização[207,208].

---

[205] *Ibidem*. p. 1748.
No original: For almost every one of us, then, we can assume a hypothetical database of ruin, the one containing this fact but until now splintered across dozens of databases on computers around the world, and thus disconnected from our identity. Reidentification has formed the database of ruin and given our worst enemies access to it.
[206] DOCTOROW, Cory. Data protection in the EU: the certainty of uncertainty. *Guardian.* Disponível em https://www.theguardian.com/technology/blog/2013/jun/05/data-protection-eu-anonymous Acesso em 03.mar.2017.
No original: "When a regulation asserts that some data is 'anonymous', it is disconnected from the best theories in computer science".
[207] SWEENEY, Latanya. *Achieving k-anonymity privacy protection using generalization and suppression.* International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 571- 588.

Latanya Sweeney ensina a diferença entre os dois métodos. A supressão altera atributos com o objetivo de remover as ligações entre os dados e o indivíduo. Pode ser obtida por meio (i) da adição de ruído e (ii) da permutação dos dados entre si. A generalização, por outro lado, altera os atributos, modificando a escala ou a ordem de magnitude dos dados. A agregação junta uma pessoa com outros indivíduos, de forma que o grupo resultante de indivíduos acaba compartilhando o mesmo valor de atributos. [209].

3.4. A diferença entre desindexação de dados e anonimização e breves comentários sobre ao direito ao esquecimento

Quando o assunto se volta para o compartilhamento de informações na internet e a proteção dos dados pessoais, é necessária a digressão sobre o direito à sua desindexação. Diferentemente da anonimização dos dados, a desindexação está diretamente relacionada à remoção e bloqueio de resultados de pesquisa na internet.

Desta forma, entende-se como direito à desindexação de dados o direito de exigir a remoção e o bloqueio de dados dos motores de busca relacionados a *sites* que contenham dados de uma pessoa física ou jurídica, sejam esses inverídicos ou que se caracterizem como invasão de privacidade.

Descrevendo o problema, trata-se de um direito do indivíduo de não mais ser lembrado por algum fato ocorrido em seu passado, como por exemplo, no caso de um indivíduo ter cometido um crime de grande repercussão nacional há dez anos e a mídia fazer ressurgir a notícia, relembrando à sociedade o fato ocorrido e, ainda, permitindo que seja encontrado facilmente na internet cada vez que alguém colocar palavras em *sites* de busca que remontem ao assunto.

---

[208] A.H.M. Sarowar Sattara, Jiuyong Lia , Xiaofeng Dinga, Jixue Liua , Millist Vincenta. *A General Framework for Privacy Preserving Data Publishing*. School of Information Technology and Mathematical Science, University of South Australia, Mawson Lakes, SA-5095, Australia. p. 2-3.

[209]SWEENEY, Latanya. *Achieving.. Op. Cit.* p. 572.

No original: *"Generalization involves replacing (or recoding) a value with a less specific but semantically consistent value. Suppression involves not releasing a value at all. While there are numerous techniques available , combining these two offers several advantages".*

Essa lembrança fará ressurgir tudo o que foi vivido pelo indivíduo, bem como a imagem negativa frente à sociedade, podendo ele, com isso, ter a sua dignidade ferida por um fato que poderia ter sido esquecido.

É justamente disso que trata o caso emblemático que ganhou grande repercussão: Google Inc., Google Spain Sl. Vs Agencia Española de Protección de Dados (AEPD), Mario Costeja González, em 2014. Referente caso ficou notório, pois o Sr. González pleiteou a desindexação de matérias do jornal La Vanguardia que haviam sido publicadas em 1998. Elas noticiavam o leilão de um imóvel (de propriedade de González) em hasta pública para o pagamento de dívida com a Seguridade Social. O Tribunal determinou que o Google removesse dos resultados de busca os resultados que associavam o Sr. González às matérias que veiculavam seu débito. Após seu pedido contra o jornal ter sido negado pela Agencia Española de Protección de dados (AEDP), o Sr. Mario Costeja González recorreu da decisão. No Acórdão, o Tribunal de Justiça da União Europeia determinou que fossem desindexados *links* que veiculassem informações pessoais dos motores de busca.[210]

---

[210] UE, Tribunal de Justiça da União Europeia. Google Spain, Google Inc. Contra Agencia Española de Protección de dados (AEDP), Mario Costeja González, 13 de maio de 2014, processo c-131/12. Disponível em: http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d2dc30d5fe90ba6179b14238af0fae643c9fa1b9.e34KaxiLc3qMb40Rch0SaxyKaNb0?doclang=PT&text=&pageIndex=1&part=1&mode=DOC&docid=152065&occ=first&dir=&cid=100417 Acesso em 15.2.2017. No original:

96 - Atendendo ao exposto, no âmbito da apreciação dos pedidos apresentados contra um tratamento como o que está em causa no processo principal, importa designadamente examinar se a pessoa em causa tem o direito de que a informação sobre a sua pessoa deixe de ser associada ao seu nome através de uma lista de resultados exibida na sequência de uma pesquisa efetuada a partir do seu nome. A este respeito, importa sublinhar que a constatação desse direito não pressupõe que a inclusão da informação em questão na lista de resultados cause prejuízo à pessoa em causa.

97 - Na medida em que a pessoa em causa pode, tendo em conta os seus direitos fundamentais nos termos dos artigos 7º e 8º da Carta, requerer que a informação em questão deixe de estar à disposição do grande público através da sua inclusão numa lista de resultados deste tipo, há que considerar, como resulta, designadamente, do n. 81 do presente acórdão, que esses direitos prevalecem, em princípio, não só sobre o interesse económico do operador do motor de busca mas também sobre o interesse desse público em encontrar a referida informação durante uma pesquisa sobre o nome dessa pessoa. No entanto, não será esse o caso se se afigurar que, por razões especiais como, por exemplo, o papel desempenhado por essa pessoa na vida pública, a ingerência nos seus direitos fundamentais é justificada pelo interesse preponderante do referido público em ter acesso à informação em questão em virtude dessa inclusão.

A Analisando a literatura publicada, o que se verifica é um entendimento de que o direito à desindexação faz parte do direito ao esquecimento[211]. Conforme matéria com entrevista concedida por Julia Powles, o direito à desindexação seria uma categoria do direito ao esquecimento:

> Esse direito [à desindexação], oponível a ferramentas de busca, destina-se a resolver o problema do "eterno" presente na Internet, isto é, a dificuldade de se "deixar para trás" acontecimentos do passado. Trata-se da

98 - Tratando-se de uma situação como a que está em causa no processo principal, que diz respeito à exibição, na lista de resultados que o internauta obtém ao efetuar no Google Search uma pesquisa a partir do nome da pessoa em causa, de ligações a páginas de arquivos em linha de um jornal que contém anúncios que mencionam o nome dessa pessoa e que respeitam a uma venda de imóveis em hasta pública decorrente de um arresto com vista à recuperação de dívidas à Segurança Social, há que considerar que, tendo em conta o caráter sensível, para a vida privada dessa pessoa, das informações contidas nesses anúncios e o facto de a sua publicação inicial remontar há 16 anos, a pessoa em causa tem comprovadamente direito a que essas informações já não sejam associadas ao seu nome através dessa lista. Por conseguinte, na medida em que, no caso em apreço, não parece haver razões especiais que justifiquem um interesse preponderante do público em ter acesso a essas informações no âmbito dessa pesquisa, o que, todavia, cabe ao órgão jurisdicional de reenvio verificar, a pessoa em causa pode, ao abrigo dos artigos 12º, alínea b), e 14º, primeiro parágrafo, alínea a), da Diretiva 95/46, exigir a supressão das referidas ligações dessa lista de resultados".

99 - Resulta das considerações precedentes que há que responder à terceira questão que os artigos 12º, alínea b), e 14º, primeiro parágrafo, alínea a), da Diretiva 95/46 devem ser interpretados no sentido de que, no âmbito da apreciação das condições de aplicação destas disposições, importa designadamente examinar se a pessoa em causa tem o direito de que a informação em questão sobre a sua pessoa deixe de ser associada ao seu nome através de uma lista de resultados exibida na sequência de uma pesquisa efetuada a partir do seu nome, sem que, todavia, a constatação desse direito pressuponha que a inclusão dessa informação nessa lista causa prejuízo a essa pessoa. Na medida em que esta pode, tendo em conta os seus direitos fundamentais nos termos dos artigos 7º e 8º da Carta, requerer que a informação em questão deixe de estar à disposição do grande público devido à sua inclusão nessa lista de resultados, esses direitos prevalecem, em princípio, não só sobre o interesse económico do operador do motor de busca mas também sobre o interesse desse público em aceder à referida informação numa pesquisa sobre o nome dessa pessoa. No entanto, não será esse o caso se se afigurar que, por razões especiais como, por exemplo, o papel desempenhado por essa pessoa na vida pública, a ingerência nos seus direitos fundamentais é justificada pelo interesse preponderante do referido público em ter acesso à informação em questão, em virtude dessa inclusão.

[211]MELO, Mariana Cunha. O significado do Direito ao Esquecimento. *Jota*, 22.nov.2016. Disponível em https://www.jota.info/artigos/o-significado-direito-ao-esquecimento-22112016 Acesso em 01.mar.2018. "Mais recentemente, o direito ao esquecimento passou a ser relacionado a outra matéria: o suposto direito à remoção de resultados de busca na internet. Nesse segundo sentido – podemos chama-lo procedimental –, o direito de ser esquecido é também chamado de direito de ser desindexado, em alusão à remoção dos links impugnados do index de possíveis resultados de busca".

> remoção de resultados de busca contendo informações desatualizadas, irrelevantes ou imprecisas sobre alguém, quando essas informações não forem de interesse público. Para este direito, Powles propõe sua segmentação em categorias mais específicas e claras com o propósito de facilitar a harmonização dos critérios adotados pelos tribunais para separar os casos em que as informações deverão ser removidas ou desindexadas daqueles em que isso não deverá ocorrer[212].

O direito ao esquecimento tem sido motivo de grandes discussões na doutrina e na jurisprudência brasileira, tendo sido utilizado como um meio de proteger direitos fundamentais do indivíduo, como o direito à dignidade da pessoa humana[213], o direito de personalidade, o direito à honra e o direito à privacidade. As discussões pairam em torno do conflito entre dois direitos, de um lado o direito à liberdade de informação e de outro o direito ao esquecimento.

Pode-se dizer que o direito ao esquecimento, apesar de estar previsto no ordenamento brasileiro, está implícito no princípio da dignidade da pessoa humana, garantido pela Constituição Federal, pois se trata basicamente do direito do indivíduo de ter acontecimentos do seu passado esquecidos e não mais veiculados no meio social, visto que a lembrança de fatos passados pode acarretar ao indivíduo intimidações, ameaças, coações, enfim, uma série de afrontas à dignidade por um episódio que já havia sido olvidado e foi trazido à tona novamente.

---

[212] [#1][especial] o que é o direito ao esquecimento? *INTERNETLAB pesquisa em direito e tecnologia,* 2017 Disponível em http://www.internetlab.org.br/wp-content/uploads/2017/01/ENTREVISTA_JULIA_POWLES_v04.pdf Acesso em 03.dez.2017.

[213] VI Jornada de Direito Civil do Conselho da Justiça Federal (CJF): "Enunciado n. 531 – A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento. Artigo: 11 do Código Civil. Justificativa: 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 exdetento 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".

Acerca da tutela da dignidade da pessoa humana, José Miguel Garcia Medina ensina que:

> O art. 1º, III da CF estabelece a dignidade da pessoa humana como um dos fundamentos da República Federativa do Brasil. (…) Trata-se, pois, de princípio de aceitação universal: a dignidade humana é o eixo em torno do qual deve girar todo o sistema normativo, núcleo fundamental dos direitos fundamentais[214].

Assim, conforme demonstrado por José Miguel Garcia Medina, ao se utilizar a técnica do sopesamento com base no princípio da proporcionalidade, a dignidade da pessoa humana deve prevalecer frente aos demais princípios, com exceção do direito à vida, que consiste em um direito maior. Logicamente, cada caso deve ser analisado, já que, em torno da dignidade da pessoa humana, existem outros direitos que fazem parte de sua tutela.

As polêmicas que giram em torno do direito ao esquecimento estão relacionadas ao conflito existente entre este e o direito à informação. De acordo com Gustavo Tepedino[215] , o direito ao esquecimento foi mencionado pela primeira vez nos Estados Unidos, mais especificamente na cidade de Boston, quando, no início do Século XX, o advogado Samuel Warren, descontente com matérias que vinham sendo divulgadas sobre a beleza de sua esposa, levantou em juízo o direito de "ser deixado em paz" (*right to be alone*), como uma derivação ao direito à intimidade.

A Constituição Federal do Brasil, ao estabelecer o direito à intimidade e à vida privada, não deixou claros os direitos que podem decorrer destes. Este problema foi instaurado em decorrência do fato da a carta não ter citado exceções referentes ao direito à informação, deixando espaço para conflitos entre direitos.

---

[214] MEDINA, José Miguel Garcia. *Novo Código de Processo Civil Comentado.* São Paulo: Revista dos Tribunais, 2017. p. 30.

[215] TEPEDINO, Gustavo. *Temas de direito civil.* 2 ed. Rio de Janeiro/São Paulo: Renovar, 2001. p.

Edilson Farias[216] disserta acerca do direito à informação afirmando que se trata de um direito subjetivo fundamental, estando consubstanciado na liberdade de pensamento, bem como no direito de dar e receber uma informação. Todavia, em alguns casos, o direito ao esquecimento deve prevalecer sobre o direito à informação, como bem exemplifica Claudio Luiz Bueno Godoy: um indivíduo que cumpriu pena privativa de liberdade precisa que seu direito ao esquecimento seja preservado em prol da função principal da pena, que é a ressocialização — desde que não se trate de um assunto de relevante conhecimento social[217], veja-se:

> 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 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 o exemplo nazista, citado por Costa Andrade. Aliás, pelo contrário, esses são casos que não devem mesmo ser esquecidos[218].

Destacando o entendimento jurisprudencial do Supremo Tribunal de Justiça (STJ) tem-se o argumento do Ministro Luís Felipe Salomão:

> [...] não se pode, pois, nestes casos, permitir a eternização da informação. Especificamente no que concerne ao confronto entre o direito de informação e o direito ao esquecimento dos condenados e dos absolvidos em processo

---

[216] FARIAS, Edilson Pereira de. *Colisão de direitos: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informaçã*o. 2 ed. Porto Alegre: Sergio Antonio Fabris Editor, 2000.
[217] GODOY, Claudio Luiz Bueno de. *A liberdade de imprensa e os direitos da personalidade.* São Paulo: Atlas, 2001, p. 89-90
[218] *Idem.*

> criminal, a doutrina não vacila em dar prevalência, em regra, ao último[219].

No julgamento do recurso especial supramencionado, foi estabelecida a tese de que as pessoas têm o direito de serem esquecidas pela imprensa e pela opinião pública[220]. Nas palavras de Rodotá: *"qual dignidade restará a uma pessoa tornada prisioneira de um passado que está todo nas mãos de outros, frente a que resta resignar-se de ter sido expropriado?"*[221]

3.5. Dificuldade da tomada de decisões no contexto do tratamento automatizado de dados

Dino Pedreschi afirma que vivemos em tempos de oportunidades sem precedentes de detecção, armazenamento e análise de dados sobre atividades humanas com extrema precisão e resolução, no nível da sociedade.[222] Tal situação possibilita, cada vez mais, que sejam utilizados os dados pessoais dos usuários (nos mais diversos fins) para gerar renda com a monetização de dados pessoais, ou seja, a atribuição de valor monetário aos dados pessoais.

Neste sentido, Bruno Bioni, ao mencionar a possibilidade de antever e prever comportamentos ou propensões dos usuários (que a mineração de dados pessoais possibilita) para sujeitá-los a decisões automatizadas, afirma que *"coletam-se, cada vez mais,*

---

[219] Brasil, Superior Tribunal de Justiça. Julgamento do Recurso Especial n. 1.334.097, 4ª Turma, Relator Ministro Luís Felipe Salomão.

[220]Em 2012, no julgamento do caso Xuxa contra Google (Recurso Especial 1.316.921–RJ) o STJ decidiu que caso o usuário queira retirar da internet conteúdo que considere violador de seus direitos, ele deverá buscar diretamente o provedor da informação, ou seja, aquele que publicou e/ou mantém a informação disponível, uma vez que os provedores agem como "meros fornecedores de meios físicos, que servem apenas como intermediários, repassando mensagens e imagens transmitidas por outras pessoas e que, portanto, não as produziram nem sobre elas exerceram fiscalização ou juízo de valor, não podendo ser responsabilizados por eventuais excessos e ofensas à moral e à honra de outros." Mais recentemente, em 2016, o entendimento foi reiterado no AgInt no Recurso Especial 1.593.873 – SP, julgado em novembro de 2016

221 RODOTÁ, Stephano. *A vida... Op. Cit.* p. 239.

[222] PEDRESCHI, Dino. Big data mining, fairness and privacy: A vision statement towards an interdisciplinary roadmap of research. In *Privacy Observatory Magazine*, Issue 1. Disponível em https://openaccess.leidenuniv.nl/bitstream/handle/1887/46938/ArtikelMODAPmetPedreschietal(2011).pdf?sequence=1 Acesso em 02.fev.2017. p. 1.

informações sobre um indivíduo a fim de compor um perfil detalhado seu para alimentar análises preditivas a seu respeito".[223]

Nesse contexto, deve-se lembrar as lições de Eli Pariser sobre *"filter bubble"* que cada usuário tem na internet.[224] Tal filtro é criado por um algoritmo que leva em consideração as atividades do usuário na internet; porém, esse mesmo usuário não tem o menor poder de controle sobre o que entra ou não nesse filtro.

Ainda, Pariser ensina que os algoritmos que definem as escolhas para os indivíduos o fazem somente com base no que se considera relevante. Dessa forma, os sensos de vida pública, de responsabilidade e sensibilidade dos usuários são totalmente excluídos da vida deles em sua navegação. Ou seja, a atenção é dirigida de forma que o usuário não note que a informação existe. Assim, é importante que ele saiba quais informações ficam para fora de tais filtros para que possa controlar o tipo de informação que receberá.

> Essa distorção é uma das dificuldades geradas pelos filtros personalizados. Tal qual uma lente, o filtro transforma inevitavelmente o mundo que vivenciamos, determinando o que vemos e o que não vemos. Ela interfere na inter-relação ente nossos processos mentais e o ambiente externo. Em certos casos, pode atuar como uma lente de aumento, sendo muito útil quando queremos expandir a nossa visão sobe uma área específica do conhecimento. No entanto, os filtros personalizados podem, ao mesmo tempo, limitar a variedade de coisas às quais somos expostos, afetando assim o modo como pensamos e aprendemos.[225]

Associado a isso, deve-se levar em consideração que os algoritmos muitas vezes não são corretos. Sim, os algoritmos decidem quem vai receber um empréstimo, quem vai ser selecionado para uma entrevista de emprego, quem vai ter direito a determinado

---

[223] BIONI, Bruno. Autodeterminação informacional... Op. Cit. p. 248
[224] PARISER, Eli. *O filtro invisível: o que a internet está escondendo de você.* Rio de Janeiro: Zahar, 2012, 2012, p. 77
[225] PARISER, Eli. *O filtro... Op. Cit.* p. 77

seguro e quanto pagará por ele, e muito mais.... e o pior: eles podem estar errados.

É o que ensina Cathy O'Neil, matemática e engenheira de dados que cunhou um termo para esses algoritmos (secretos, importantes e nocivos): "armas de destruição em matemática". A autora ensina que os indivíduos são avaliados com fórmulas secretas que eles não entendem e que geralmente não têm como ser contestadas.

> O problema surge quando os algoritmos estão errados. Para construir um algoritmo você precisa de duas questões: (i) dados (passado) e (ii) definição de sucesso (aquilo que se está procurando com o algoritmo). Treinamos um algoritmo procurando, calculando. O algoritmo descobre o que está associado com o sucesso, qual situação leva ao sucesso.
>
> Algoritmos são opiniões embutidas num código. Bem diferente do que a maioria de nós pensa sobre os algoritmos. Achamos que os algoritmos são objetivos, verdadeiros e científicos. Esse é um truque de *marketing*. É também um truque de *marketing* intimidar vocês com algoritmos, fazê-los acreditar nos algoritmos ou ter medo deles porque acreditamos na matemática, e temos medo dela. Muita coisa pode dar errado quando confiamos cegamente no *big data*.
>
> Os algoritmos não tornam as coisas justas se forem aplicados de forma cega e displicente. Não tornam as coisas justas. Eles repetem nossas práticas passadas, nossos padrões. Eles automatizam o *status quo*. Isso seria ótimo se tivéssemos um mundo perfeito, mas não temos. E mais: a maioria das empresas não inclui os litígios constrangedores, mas os cientistas de dados dessas empresas são orientados a seguirem os dados, a terem rigor. Pensem no que isso significa. Como todos somos tendenciosos, significa que poderiam estar codificando sexismo ou qualquer outro tipo de intolerância.

> O que que está havendo? Branqueamento dos dados. É um processo por meio do qual tecnólogos escondem verdades sujas dentro da caixa-preta dos algoritmos, e os chamam de objetivos, de meritocráticos. Cunhei um termo para esses algoritmos secretos, importantes e destrutivos: "armas de destruição em matemática".[226] Assim, porque os algoritmos não são confiáveis, eles deverão passar por uma auditoria.

Tudo isso gera uma violação ao direito à autodeterminação informativa,[227] um direito fundamental também violado, já que o usuário não tem o menor controle do que é feito com os seus dados. Da mesma forma, há uma violação aos direitos da personalidade, ou seja, há um impacto no livre desenvolvimento da personalidade dos usuários, isso porque eles ficam sujeitados a decisões automatizadas.

Como demonstrado, no tratamento automatizado de dados pessoais, os usuários são datificados e, com base nos estereótipos criados pelo algoritmos, são tomadas decisões, como, por exemplo, a concessão ou não de linha de crédito[228]. A categorização de pessoas, com base em seus dados pessoais,

---

[226] Cathy O'Neil at TED2017, *A era da fé cega no Big data tem de acabar*. Disponível em https://www.ted.com/talks/cathy_o_neil_the_era_of_blind_faith_in_big_data_must_end/transcript?language=pt-br Acesso em 21.12.2017.

[227] PÉREZ LUÑO, Antonio-Enrique. Derechos humanos, Estado de Derecho y Constitución. 9. ed. Madri: Editorial Tecnos, 2005, p. 339. No original: En efecto, como acertadamente se ha puesto en evidencia, la libertad informática, al igual que la libertad política, presenta dos aspectos: uno, es de significación negativa y se traduce en el derecho a no hacer de dominio público ciertas informaciones de carácter personal, privado o reservado; el otro, es positivo e implica el ejercicio de un derecho al control de los datos concernientes a la propia persona que han rebasado la esfera de la *privacy* para devenir elementos del input de un programa electrónico. La libertad informática en su aceptación positiva entraña, por tanto, el reconocimiento del derecho a conocer, corregir, cancelar o añadir datos en una ficha personal contenida en un registro informático. Si bien, debe tenerse presente que en la práctica ambos aspectos negativo y positivo de la libertad informática son complementarios, ya que el ejercicio pleno de este derecho consiste en la facultad de intervenir sobre los bancos de datos no sólo para limitar su uso prohibiendo la difusión de sus informaciones, sino también para desarrollar una actividad de inspección, verificación o cancelación, en la que se ha visto una correspondencia con lo que supone el derecho a la rectificación en las informaciones publicadas en los medios de comunicación.

[228] MAYER-SCHÖNBERGER, Viktor. CUKIER, Kenneth. *Big Data… Op. Cit.* p. 176.

demonstra o atropelo do ser humano em total afronta ao livre desenvolvimento da personalidade.

Com o intuito de solucionar a situação que pode gerar violação aos direitos da personalidade dos usuários e no livre desenvolvimento de sua personalidade, Cathy O'Neil apresenta uma solução que chama de "auditoria de algoritmos"[229] Por meio dela, os dados poderiam ser reparados para aperfeiçoar os resultados de sua aplicação:

O primeiro passo seria chegar a integridade dos dados, ou seja, retirar os vieses sociais. Para ilustrar, a autora afirma que, caso seja realizada uma pesquisa sobre qual a população que fuma maconha, deve-se ter em mente que negros são muito mais parados pela polícia do que brancos, e isso afetaria os resultados caso não fosse levado em consideração.

Conforme ensina Sata Hajam, a discriminação por meio do tratamento de dados anonimizados pode ser direta ou indireta. A discriminação direta ocorre quando as decisões são tomadas com base em atributos discriminatórios. A discriminação indireta ocorre quando as decisões são tomadas com base em atributos não

---

[229]Cathy O'Neil. *Op. Cit...* Sobre a auditoria nos dados a a autora ensina: "A boa notícia é que isso é possível. Os algoritmos podem ser questionados, e eles sempre vão nos dizer a verdade. E podemos repará-los, aperfeiçoá-los. Podemos chamar de auditoria de algoritmos, e vou mostrar como seria.
Primeiro, temos de checar a integridade dos dados. Para o algoritmo de risco de recidiva que mencionei, checar a integridade dos dados significa aceitarmos o fato de que, nos EUA, brancos e negros fumam maconha na mesma proporção, mas os negros têm muito mais chance de serem presos, quatro ou cinco vezes mais, dependendo da região. E como esse viés surge em outras categorias de crime e como justificamos isso?
Segundo, devemos pensar na definição de sucesso, auditar esse conceito. Lembram-se do algoritmo de contratação de que falei? Alguém que trabalhou por quatro anos e foi promovido uma vez? Bem, esse é um empregado de sucesso, mas é também um empregado que tem apoio da cultura da empresa. Isso pode ser bem tendencioso. Precisamos separar essas duas coisas. Deveríamos nos mirar na audição às cegas de orquestras. É quando os examinadores ficam atrás de uma planilha. O importante aí é que os examinadores decidem o que é importante e o que não é, e não se distraem com outras coisas. Quando as audições às cegas de orquestras começaram, o número de mulheres em orquestras cresceu cinco vezes mais.
Depois, temos de considerar o rigor. É aí que o modelo valor agregado para professores fracassaria imediatamente. Nenhum algoritmo é perfeito, claro, assim, temos de partir do pressuposto de que todos erram. Qual a frequência desses erros, e com quem esse modelo falha? Qual o preço desse fracasso?
E, finalmente, temos de considerar os efeitos de longo prazo dos algoritmos, os círculos viciosos que são gerados. Isso parece abstrato, mas imaginem se os engenheiros do *Facebook* tivessem considerado isso antes de decidirem nos mostrar apenas coisas que nossos amigos postam".

discriminatórios que estão fortemente correlacionados com discriminação tendenciosa.[230]

Ademais, deve-se repensar o significado de sucesso, já que ele também poderá ser alterado pela realidade no qual está inserido. Considerem-se duas pessoas, um homem e uma mulher, com a mesma idade e formação, ocupando o mesmo cargo, e o homem tem mais promoções que a mulher. Então, ele, teoricamente, tem mais sucesso, porém, não se pode perder de vista que essa definição de sucesso deverá ser mitigada caso seja verificado que homens têm mais apoio na cultura de tal empresa. Interessante notar que a mesma autora cita as "audições às cegas" de orquestras, ou seja, audições realizadas sem que o auditor saiba quem são os músicos, com enfoque total na performance do músico. Com elas, o número de mulheres em orquestras cresceu cinco vezes.

Além disso, deve ser considerado o rigor, ou seja, nenhum algoritmo é perfeito, ele deverá ser validado pela experiência humana. A autora cita como exemplo o caso em que professores estavam sendo avaliados por um algoritmo complexo e secreto, chamado "modelo de valor agregado". Após análise dos dados, Gary Rubenstein[231] descobriu que o resultado era totalmente aleatório, o algoritmo utilizado simplesmente não funcionava e nunca deveria ter sido usado para avaliar o desempenho dos professores, o algoritmo era quase um gerador aleatório de número.

Por fim, deverão ser levados em consideração os efeitos a longo prazo dos algoritmos, o que, de certa forma, corresponde àquilo que Eli Pariser trata como a distorção da realidade causada pelos filtros.

Ainda que haja uma tentativa de se humanizar e aperfeiçoar os resultados da aplicação dos algoritmos, a verdade é que eles, do modo como atuam hoje, violam os direitos da personalidade dos usuários, já que estes ficam sujeitados à decisões

---

[230] HAJAM, Sara. *Simultaneous discrimination prevention and privacy protection in data publishing and mining*. Dissertation (Doctor of philosoph in computer science), arXiv:1306.6805v1 [cs.DB] 28 Jun 2013. Disponível em https://arxiv.org/pdf/1306.6805.pdf. Acesso em 02.fev.2016. p. vi.

[231] RUBISTEIN, Gary. Analyzing Released NYC Value-Added Data. Techforus. Disponível em http://garyrubinstein.teachforus.org/2012/02/28/analyzing-released-nyc-value-added-data-part-2/ Acesso em 6.nov.2017.

automatizadas, sem que se considere o livre desenvolvimento de sua personalidade e, pior ainda, podendo gerar discriminação a determinados grupos.

CONCLUSÃO

Procurou-se investigar o conceito de anonimato e como o tratamento automatizado de dados influi em sua aplicação e existência. Levando-se em consideração (i) o alcance da internet; (ii) o volume da aquisição e compilação de dados dos usuários; e (iii) o crescimento e potencialização dos bancos de dados (como, por exemplo, o *big data*), verificou-se que, por meio do tratamento automatizado, muitas vezes os direitos dos usuários são violados, especialmente o direito à proteção de dados pessoais.

Assim, a importância do tema está associada à possibilidade de danos aos usuários da internet e à incerteza jurídica que cerca o tema, sendo necessária uma incursão sobre os diversos tópicos e conceitos, jurídicos e extrajurídicos, de sorte a construir um sólido um raciocínio sobre o tema.

No Brasil, a ausência de legislação específica que delineie os limites do que sejam os dados anônimos e a sua forma de proteção provoca insegurança jurídica para o cidadão, considerando que tal situação leva o julgador do caso concreto a utilizar-se de conceitos e proposituras nem sempre seguras e apropriadas.

Entende-se que o legislador deve buscar limites jurídicos objetivos, imperativos no trato das informações pessoais inseridas pelos usuários quando da utilização dos serviços colocados à sua disposição. Considerando os projetos de lei que estão em pauta, pode-se dizer que existe uma preocupação da população e do Poder Legislativo com a criação de lei específica sobre o tratamento dos dados pessoais capturados na internet.

Além disso, muito se questiona sobre qual o sentido do consentimento dado para autorizar o uso dos dados pessoais. Isso porque, depois de coletados os dados, os usuários não têm controle de qual será sua destinação e uso. Também não lhes é conferida a possibilidade de furtar-se a esse tratamento durante o uso da grande maioria dos *sites* e aplicações.

Ou seja: na atual conjuntura: (i) o usuário, por meio do consentimento conferido na assinatura de longos termos e condições, abre mão de saber o que ocorre com os seus dados coletados (o usuário anui sem saber ao certo com o quê) em evidente colisão com

o direito à autodeterminação informacional; ou (ii) ele fica totalmente excluído do acesso à internet por meio dos principais *sites* e redes sociais.

A atenção deverá ser redobrada quando se percebe que existência de dados anônimos ou não identificáveis é algo impossível do ponto de vista da ciência da análise de dados. O tratamento automatizado de dados pessoais não permite, em verdade, que haja anonimato dos dados pessoais (veja-se o estudo realizado por Yves-Alexandre de Montjoye *et. al* que conseguiu reidentificar dados com 95% de precisão utilizando apenas quatro pontos de dados sobre cada pessoa).

Igualmente, deverá ser questionada, inclusive, a divisão da classificação de dados entre pessoais e anônimos. Explica-se: como, na prática, não há a possibilidade de um dado pessoal se manter anônimo (levando-se em consideração as diversas técnicas para reidentificar um dado anônimo) não ha diferença entre dados pessoais e dados anonimizados, ou seja, a partir do momento em que alguém decida desanonimizá-los, os dados anônimos passarão a ser dados pessoais.

Assim, fica evidente que, ao combinar informações existentes nos dados supostamente anonimizados com informações externas, é possível, com relativa facilidade, identificar o indivíduo na ponta.

Dessa forma, levando-se em consideração a total falta de controle do usuário sobre seus dados e a rentabilidade que os dados coletados geram às empresas, é de observar com cuidado o tratamento dispendido à proteção de dados pessoais.

Um exemplo que demonstra com clareza o uso dos dados pessoais é o *profiling*, isto é, a metodologia que cria um perfil dos usuários pela coleta de dados. Com essa metodologia, presumem-se as personalidades e interesses dos usuários, com isso a tecnologia analisa os dados prevê comportamentos futuros (com base nos registros eletrônicos de hábitos de navegação associados a outra fontes de informação). O problema maior que se se vê nesse caso é a perda da autonomia do usuário, já que, após criado o perfil, são realizadas decisões automatizadas para o usuário em questão sem que ele sequer saiba o que está acontecendo.

A situação foi apontada pelos "*filter bubbles*", por meio dos quais a navegação ocorrerá de maneira individualizada, de acordo com o que a tecnologia entende ser o perfil do usuário. É evidente que tal diagramação tão individualizada transforma o mundo que cada usuário vivencia, pois acaba por determinar o que ele vê o que ele não vê durante o acesso à internet com base em decisões passadas que foram coletadas e transformadas em um perfil (isto é, por meio do tratamento de dados pessoais).

Referido filtro interfere na inter-relação entre os processos mentais dos usuários e o ambiente externo (a relação com o mundo). Assim, em certos casos, pode atuar como uma lente de aumento, ótima para quando se quer expandir a visão sobre uma área específica do conhecimento. No entanto, os filtros personalizados podem, ao mesmo tempo, limitar a variedade de coisas às quais os indivíduos são expostos, afetando, assim, o modo como eles vivem, pensam e aprendem.

A esse respeito, outra afirmação de Eric Schmidt é importantíssima para que se possa compreender o poder das informações coletadas e do perfil dos usuários: "*(...) a tecnologia será tão boa que [em breve] será muito difícil para as pessoas assistir ou consumir algo que, de certa forma, não tenha sido adaptado a elas".*[232]

Ou seja, o futuro do *Google* e demais empresas cujo maior ativo é a coleta de dados, é elaborar conteúdo, comercial ou não, específico para cada usuário com fundamento em bancos de dados. Isso deve ser observado com muito cuidado, pois, como visto, os algoritmos não são totalmente confiáveis, ou seja, nem sempre são objetivos e trazem a verdade.

Apesar de constituírem um importante ativo econômico, os dados pessoais dizem respeito a um indivíduo ou grupo de indivíduos que devem ser protegidos. Dessa forma todo cuidado é

---

[232] HOLMAN JR., Jenkins. Google and the Search for the Future. *Wall Street Journal.* Disponível em https://www.wsj.com/articles/SB10001424052748704901104575423294099527212 Acesso em 03.out.15.

No original: "The power of individual targeting — the technology will be so good it will be very hard for people to watch or consume something that has not in some sense been tailored for them".

pouco quando se trata da coleta e tratamento automatizado de dados, pois a tecnologia deve existir como uma forma de empoderamento do indivíduo e não como uma forma de limitação do livre desenvolvimento de sua personalidade.

REFERÊNCIAS BIBLIOGRÁFICAS

ARIANO, Erica. Descubra como o Big Data tem influenciado as mídias sociais. Disponível em http://www.ideiademarketing.com.br/2013/11/15/descubra-como-o-big-data-tem-influenciado-as-midias-sociais/ Acesso 06.mar.2018.

A.H.M. Sarowar Sattara, Jiuyong Lia , Xiaofeng Dinga, Jixue Liua , Millist Vincenta. *A General Framework for Privacy Preserving Data Publishing*. School of Information Technology and Mathematical Science, University of South Australia, Mawson Lakes, SA-5095, Australia.

ASCENSÃO, José de Oliveira. *Direito da Internet e da Sociedade da Informação*, Rio de Janeiro: Forense, 2002.

_____. *O direito de autor no ciberespaço. Revista Ajuris*, Porto Alegre, vol. 26, nº 80, p. 335, dez. 2000.

BALKIN, Jack M. *The Constitution in the National Surveillance State* (2008). Faculty Scholarship Series. Paper 225, p. 18 e 19. Disponível em: <http://digitalcommons.law.yale.edu/fss_papers/225>. Acesso em: 15.dez.14.

BARLOW, John Perry. *The Next Economy of Ideas*. The Wired. 2010. Disponível em http://www.wired.com/2000/10/download/. Acesso em 2.mar.2016.

BELL, Daniel. *In*: *Business and Society Review/Innovation.* Disponível em: <https://www.os3.nl/_media/2011-2012/daniel_bell_-_the_coming_of_post-industrial_society.pdf>, acesso em 20.out. 2015.

BIONI, Bruno. *Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet.* Dissertação (Mestrado), Faculdade de Direito, Universidade de São Paulo, São Paulo, 2016.

BITTAR, Carlos Alberto. Os direitos da personalidade. 7. ed. Rio de Janeiro: Forense Universitária, 2008.

CANOTILHO, J.J. Gomes. *Constituição* da *República* Portuguesa *anotada,* vol. 1. São Paulo, AT, 1a Ed., 2007.

CATALA, Pierre. *Ebauche d'une théorie juridique de l'informati*on, in: Informatica e Diritto, ano IX, jan-apr. 1983

CASTELLS, Manuel. *A Sociedade Em Rede* - Vol. I, 8ª ed. Trad. Roneide Venancio Majer. São Paulo: Paz e Terra, 2005.

_____, *Creativity, Innovation and Digital Culture. A Map of Interactions*. Disponível em https://telos.fundaciontelefonica.com/telos/articulocuaderno.asp@idarticulo=3.htm. Acesso em 4.4.2016.

_____. *The rise of the network society (Information age, v. 1)*, 2nd ed., Malden: Wiley-Blackwell, 2010.

COSTA JR., Paulo José da, O direito de estar só: tutela penal da intimidade. 2. ed. São Paulo: RT, 1995

CUPIS, Adriano de. *Il Diritto della* personalità*,* Milano: Giuffré, 1982.

DE LUCCA, Newton. Prefácio. In: LEONARDI, Marcel. *Tutela e Privacidade na Internet*. São Paulo: Saraiva, 2012.

_____. *Aspectos Jurídicos da Contratação Informática e Telemática.* São Paulo: Saraiva, 2003,

DINIZ, Maria Helena. Dicionário Jurídico. 2. ed. rev., atual. e aum. São Paulo: Saraiva, 2005.

DOCTOROW, Cory. Data protection in the EU: the certainty of uncertainty. Disponível em https://www.theguardian.com/technology/blog/2013/jun/05/data-protection-eu-anonymous Acesso em 03.mar.2017.

DONEDA, Danilo. *A proteção de dados pessoais como um direito fundamental,* Espaço Jurídico: Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

_____. *Da privacidade à proteção de dados pessoais*, Rio de Janeiro: Renovar, 2006.

_____. Reflexões sobre proteção de dados pessoais em redes sociais. Universidad de los Andes. Facultad de Derecho (Bogotá, Colombia), No. 1 Julio. Diciembre de 2012.

_____. *A proteção de dados pessoais nas relações de consumo: para além da informação creditícia.* Escola Nacional de Defesa do Consumidor. Brasília: SPE/DPDC, 2010.

FACEBOOK, *Como faço para gerenciar ou excluir informações sobre mim?* Disponível em

https://www.facebook.com/privacy/explanation. Acesso em 08.dez.2017.

FARIAS, Edilsom Pereira de. Colisão de direitos: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação. 2 ed. Porto Alegre: Sergio Antonio Fabris Editor, 2000.

FERRAZ, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito do Estado de São Paulo, vol.88, 1993.

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

GOMES, Orlando, *Introdução ao Direito Civil*, 11a. ed., Rio de Janeiro: Forense, 1996.

GRECO, Marco Aurélio. *Internet e Direito.* São Paulo: Dialética, 2000.

Grupo de Ensino e Pesquisa em Inovação FGV. U*m novo mundo de dados*. Disponível em https://direitosp.fgv.br/sites/direitosp.fgv.br/files/arquivos/unmd_policy_paper_fgv.pdf Acesso em 10.dez.2017.

Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação. *Xeque-Mate - O Tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil*. Disponível em https://gpopai.usp.br/wordpress/wp-content/uploads/2016/06/Xeque-Mate.pdf Acesso em 10.jul.16.

HAJAM, Sara. *Simultaneous discrimination prevention and privacy protection in data publishing and mining*. Dissertation (Doctor of philosophy in computer science), arXiv:1306.6805v1 [cs.DB] 28 Jun 2013. Disponível em https://arxiv.org/pdf/1306.6805.pdf. Acesso em 02.fev.2016.

HIRATA, Alessandro. O Facebook e o direito à privacidade. *Revista De Informação Legislativa,* v. 201, p. 17-27, 2014. *Disponível em* <https://www2.senado.leg.br/bdsf/bitstream/handle/id/502950/001002775.pdf?sequence=1>. Acesso em 5.mar.16.

HOLMAN JR., Jenkins. Google and the Search for the Future. *Wall Street Journal*. Disponível em https://www.wsj.com/articles/SB10001424052748704901104575423294099527212. Acesso em 03.out.1

InternetLAB, *[especial] O que são dados pessoais?,* Equipe responsável pelo conteúdo: Dennys Antonialli, Francisco Brito Cruz, Beatriz Kira, Juliana Pacetta Ruiz e Fabiane Midori Nakagawa. Disponível em http://www.internetlab.org.br/pt/opiniao/especial-o-que-sao-dados-pessoais/ Acesso em 03.dez.2017.

JEGATHEESAN, Sowmyan. Cookies Invading Our Privacy for Marketing Advertising and Security Issues. *arXiv preprint arXiv:1305.2306*, 2013.

KLEE, Antônia Espínola Longoni e 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. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira. Direito e Internet III: Marco Civil da Internet III – tomo II. São Paulo: Quartier Latin, 2015

LACE, Suzane. *The Glass Consumer: life in a surveillance society*. Bristol: Policy Press, 2005.

LANEY, Doug. 3D Data Management: Controlling Data Volume, Velocity, and Variety. Disponível em https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf Acesso em 06.mar.2017.

LEVY, Pierre. *Cibercultura: La cultura de la sociedade digital*. Rubí (Barcelona): Anthropos Editorial, México: Universidad Autónoma Metropolitana - Iztapalapa, 2007.

LEONARDI, Marcel. Responsabilidade *Civil dos Provedores de Serviços de Internet*, São Paulo: Juarez de Oliveira, 2005.

LIMA, Cíntia Rosa Pereira de; NUNES, Lydia Neves Bastos Telles (coords.). *Estudos Avançados em Direito Digital*. Rio de Janeiro: Elsevier, 2014.

_____. *A imprescindibilidade de uma entidade 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. Ribeirão Preto, 2015.

_____. *Validade e obrigatoriedade dos contratos de adesão eletrônicos (shrink-wrap e click-wrap) e dos termos e condições de uso (browse-wrap):* Um estudo comparado entre Brasil e Canadá. São Paulo: USP-SP, 2009. Tese (doutorado), Universidade de São Paulo, Faculdade de Direito.

_____; BIONI, Bruno Ricardo. A proteção dos dados pessoais na fase de coleta: apontamentos sobre a adjetivação do consentimento implementada pelo artigo 7, incisos VIII e IX do Marco Civil da

Internet a partir da human computer interaction e da privacy by default. In DE LUCCA, Newton; SIMÃO FILHO, Adalberto e LIMA, Cíntia Rosa Pereira de (coord.).*Direito & Internet III: Marco Civil de Internet* - Tomo I. Quartier Latin, 2015. p. 263-290.

LISBOA, Roberto Senise. Direito da Sociedade da Informação. *Revista dos Tribunais,* ano 95, vol. 847, maio de 2006. São Paulo: 2006.

_____. Proteção do Consumidor na Sociedade da Informação. Revista do Direito Privado da UEL, Londrina, v. 2, n. 1, p.1-27, jan/abr 2009. Quadrimestral. Disponível em: http://www.uel.br/revistas/direitoprivado/artigos/Roberto_Senise_Lisboa_Proteção_Consumi dor_Sociedade_Informação.pdf. Acesso em: 11.mai.2016.

_____. Quebra da inviolabilidade de correspondência eletrônica por violação da boa-fé objetiva. In LUCCA, Newton De e SIMÃO FILHO, Adalberto (coords.) *Direito e Internet vol. II - Aspectos jurídicos relevantes*, São Paulo: Quartier Latin, 2008.

LORENZETTI, Ricardo Luis. Comércio Eletrônico. Trad. Fabiano Menke. São Paulo: Revista dos Tribunais, 2004.

LOSANO, Mario. *A Informática Jurídica Vinte Anos Depois*, RT v. 715, fascículo I- Cível, maio de 1995.

LOUZADA, Luiza; VENTURINI, Jamila. A regulamentação de proteção de dados pessoais no Brasil e na Europa: uma análise comparativa. 2015. *3o Simpósio Internacional* LAVITS: Vigilância, Tecnopolíticas, Territórios. 13 à 15 de Maio, 2015. Rio de Janeiro, Brasil.

MANNINO, Michael V. *Projeto, Desenvolvimento de Aplicações e Administração de Banco de Dados* - 3ª ed. São Paulo: McGraw Hill Education, AMGH Editora Ltda., 2008.

MANYIKA, J., Chui,. M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H. Big data: The next frontier for innovation, competition, and productivity. McKinsey Global Institute. 2011.

MARIA, José Serpa De Santa. *Direitos da Personalidade e a Sistemática Civil Geral,* São Paulo: Editora Julex Livros Ltda., 1987.

MARQUES, Garcia; MARTINS, Lourenço. *Direito da Informática*. Coimbra: Livraria Almedina, 2000.

MAYER-SCHÖNBERGER, Viktor. *Generational Development of Data Protection in Europe*. In: Technology and Privacy: The New Landscape. Massachusetts: The MIT Press, 2001.

_____. CUKIER, Kennneth. *Big Data: a revolution that will transform how we live, work and think.* Boston: Houghton Mifflin Harcourt Publishing Company, 2013.

MEDINA, José Miguel Garcia. Novo Código de Processo Civil Comentado. São Paulo: Revista dos Tribunais, 2017.

MELO, Mariana Cunha e. O significado do Direito ao Esquecimento. *Jota*, 22.nov.2016. Disponível em https://www.jota.info/artigos/o-significado-direito-ao-esquecimento-22112016 Acesso em 01.mar.2018.

_____. *Anonimato, proteção de dados e devido processo legal: por que e como conter uma das maiores ameaças (.* Disponível em

https://itsrio.org/wp-content/uploads/2017/03/Mariana-Cunha-e-Melo-V-Revisado.pdf Acesso em 02.fev.2017

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*, São Paulo: Saraiva, 2014.

MONTEIRO, Renato Leite, *Da Proteção aos Registros, aos dados pessoais e às comunicações privadas*, *in* MASSO, Fabiano del et. al. (coord.), Marco Civil Da Internet, São Paulo: Revista dos Tribunais, 2014.

MONTJOYE, Yves-Alexandre de, César A. Hidalgo, Michel Verleysen & Vincent D. Blonde. *Unique in the Crowd: The privacy bounds of human mobility*. Scientific Reports 3, Article number: 1376 (2013) doi:10.1038/srep01376. Disponível em https://www.nature.com/articles/srep01376. Acesso em 25.mar.2017.

_____. Radaelli L., Singh V. K., Pentland A. S. *Unique in the shopping mall: On the reidentifiability of credit card metadata* Science 347 (6221), 536-539. DOI:10.1126/science.1256297 (2015). Disponível em http://science.sciencemag.org/content/347/6221/536.full?ijkey=4rZ2eFPUrlLGw&keytype=ref&siteid=sci Acesso em 25.set.2017.

NIGER, Sergio. *Le Nuove Dimensioni Della Privacy: Dal Diritto Alla Riservatezza Alla Protezione Dei Dati Personali,* Padova: Cedam, 2006.

LOUZADA, Luiza; VENTURINI, Jamila. A regulamentação de proteção de dados pessoais no Brasil e na Europa: uma análise comparativa. 2015. *3o Simpósio Internacional* LAVITS: Vigilância, Tecnopolíticas, Territórios. 13 à 15 de Maio, 2015. Rio de Janeiro, Brasil, p. 22- 39.

OHM, Paul. *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* UCLA Law Review, vol. 57, 2010. p. 1701. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006. Acesso em 15.mar.2017.

OLIVEIRA, Déborah. Big Data: *O Desafio de Garimpar Informações*. 2013, p. 1.

O'HARROW Jr., Robert, *No Place to Hide,* New York: Free Press, 2006.

OLEJNIK, Lukasz, *Real-time Bidding systems and how much are we worth*. Disponível em < http://lukaszolejnik.com/rtbdesc > Acesso em 20.mai.16.

PANCETTI, Alessandra. Privacidade na rede: questões de segurança e de direito. Site da *Organização dos Estados Ibero-Americanos.* <http://www.oei.es/divulgacioncientifica/reportajes127.htm> Acesso em 15.out.15.

PARISER, Eli. *O filtro invisível: o que a internet está escondendo de você.* Rio de Janeiro: Zahar, 2012.

PARZIALE, Lydia. *Tutorial and Technical Overview*, 8a edição. Armonk, Nova York: International Business Machines Corporation, 2006.

PEDRESCHI, Dino. Big data mining, fairness and privacy: A vision statement towards an interdisciplinary roadmap of research. In *Privacy Observatory Magazine*, Issue 1. Disponível em https://openaccess.leidenuniv.nl/bitstream/handle/1887/46938/Artike

lMODAPmetPedreschietal(2011).pdf?sequence=1 Acesso em 02.fev.2017.

PÉREZ LUÑO, Antonio-Enrique. *Informática y Libertad. Comentario al Artículo 18.4 de la Constitución Española.* In: Revista de Estudios Políticos, Nueva Época, nº 24, Centro de Estudios Constitucionales, Madrid, 1981.

_____. Derechos humanos, Estado de Derecho y Constitución. 9. ed. Madri: Editorial Tecnos, 2005.

PINTO, Paulo Mota. Notas sobre o direito ao livre desenvolvimento da personalidade e os direitos de personalidade no direito português, in A constituição concretizada – construindo pontes com o público e o privado. Porto Alegre: Livraria do Advogado, 2000.

POWELS, Julia. [#1][especial] o que é o direito ao esquecimento? *INTERNETLAB pesquisa em direito e tecnologia,* 2017 Disponível em http://www.internetlab.org.br/wp-content/uploads/2017/01/ENTREVISTA_JULIA_POWLES_v04.pdf Acesso em 03.dez.2017..

REGAN, Priscilla M. (2002) Privacy as a Common Good in the Digital World, Information, Communication & Society, 5:3,382-405, DOI: 10.1080/13691180210159328, Disponível em http://dx.doi.org/10.1080/13691180210159328, Acesso em 13.dez.2017.

RIJMENAM, Mark van. Why The 3V's Are Not Sufficient To Describe Big Data. Disponível em https://datafloq.com/read/3vs-sufficient-describe-big-data/166 Acesso em 03.mar.2017.

RODOTÀ, Stefano. *A vida na sociedade de vigilância: a privacidade hoje*. Organização, seleção e apresentação de Maria

Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

_____. *il terribile diritto, studi sulla proprietà privata*, Il Mulino, Bologna, 1981.

_____. *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice della privacy*. In Europa e diritto privato, 2004.

_____. *Tecnologie e diritti,* Bologna: Il Mulino, 1995,

RUBISTEIN, Gary. Analyzing Released NYC Value-Added Data. Techforus. Disponível em http://garyrubinstein.teachforus.org/2012/02/28/analyzing-released-nyc-value-added-data-part-2/ Acesso em 6.nov.2017.

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

SHMATIKOV, Vitaly e NARAYANAN, Arvind. *Privacy and Securiry: Myths and Fallacies of "Personally Identifiable Information.* Disponível em http://www.cs.utexas.edu/users/shmat/shmat_cacm10.pdf Acesso em 6.mar.2017.

SIMÃO FILHO, Adalberto. Dano ao consumidor por invasão do site ou da rede: inaplicabilidade das excludentes de caso fortuito ou força maior. *In*: LUCCA, Newton de e SIMÃO FILHO, Adalberto (coords.). *Direito e Internet: aspectos jurídicos relevantes.* Bauru, SP: Edipro, 2000, p. 109.

_____. BARBOSA, Kelly de Souza. Upgrade no direito de arrependimento virtual: projetos de lei 281/2012,283/2012 e 4678/2016. *Revista de direito globalização e responsabilidade nas relações de consumo,* v. 1, p. 203-224, 2017.

SETZER, Valdemar W. Dado, Informação, Conhecimento e Competência, disponível em https://www.ime.usp.br/~vwsetzer/dado-info.html, acesso em 3.mai.16.

SOLOVE, Daniel J., *I've Got Nothing to Hide' and Other Misunderstandings of Privacy*. George Washington University Law School, 44 San Diego L. Rev. 745 (2007).

STAPLES, William G., Everyday Surveillance: Vigilance and Visibility in Postmodern Life. Lanham, MD: Rowman and Littlefield, 2000.

SWEENEY, Latanya. Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000. Disponivel em https://dataprivacylab.org/projects/identifiability/paper1.pdf. Acesso em 05.mar.2018.

_____. Achieving k-anonymity privacy protection using generalization and suppression. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 571- 588.

TEIXEIRA, Tarcísio. Direito Eletrônico. São Paulo: Editora Juarez de Oliveira, 2007.

TOMIZAWA, Guilherme. *A invasão de privacidade através da internet*. Curitiba: JM, 2008.

TOSI, Emilio. *Il Contrato Virtuale – Procedimenti formativi e forme negoziali tra tipicità e atipicità*. Milão: Giuffrè Editore, 2005.

VIEIRA, Sônia Aguiar do Amaral. Inviolabilidade da vida privada e da intimidade pelos meios de comunicação. São Paulo: Juarez de Oliveira, 2002.

WALLACE, Kathleen A. Anonymity. *Ethics and information technology,* Dordrecht, v. 1, n. 1.

WALL STREET JOURNAL, Série de reportagens chamada "What They Know" ou "O que eles sabem" em tradução livre <http://online.wsj.com/public/page/what-they-know-digital-privacy.html> Acesso em 03.out.15.

WU, Tim. Network Neutrality FAQ, Disponível em http://www.timwu.org/network_neutrality.html Acesso em 03.dez.2017.

UE, Convenção nº 108 – Convenção para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais, de 28 de janeiro de 1981.

UE, Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

UE, Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016,

ZHOU, Yuchen; EVANS, David. Why aren't HTTP-only cookies more widely deployed. *Proceedings of 4th Web,* v. 2, 2010.