Revista Jurídica Cesumar
setembro/dezembro 2019, v. 19, n. 3, p. 705-725
DOI: 10.17765/2176-9184.2019v19n3p705-725

BIG DATA E A PROTEÇÃO DO DIREITO À PRIVACIDADE NO CONTEXTO DA SOCIEDADE DA INFORMAÇÃO

Marcelo Guerra Martins[*]
Leonardo Felipe de Melo Ribeiro Gomes Jorgetto[**]
Alessandra Cristina Arantes Sutti[***]

RESUMO: O presente trabalho analisa o quadro normativo da proteção ao direito constitucional à privacidade e sua possível violação em relação ao uso do Big Data, descrevendo-se as características dessa tecnologia. O tema é examinado com base no direito europeu (o *General Data Protection Regulation*, adotado pelo Parlamento Europeu em abril de 2016), e no direito brasileiro, com incursões pelo Marco Civil da Internet (lei 12.965/2014) e pela recente Lei Geral de Proteção de Dados (lei 13.709/2018) que, dentre diversas medidas, criou a Autoridade Nacional de Proteção de Dados, criou diversas obrigações a empresas que colhem dados pessoais em ambientes virtuais, estabelecer direitos aos titulares desses dados, bem como implantou um sistema de responsabilidade administrativa e judicial específico para a área.

PALAVRAS-CHAVE: Sociedade da informação; Big data; Privacidade; Proteção de dados.

BIG DATA AND PROTECTION OF PRIVACY RIGHTS WITHIN INFORMATION SOCIETY

ABSTRACT: Protection norms on privacy guaranteed by the Brazilian Constitution and their possible violation with regard to the usage of Big Data are analyzed. The technology´s characteristics are also provided. The theme is analyzed according to

[*] Doutor em Direito do Estado pela Universidade de São Paulo (2010). Docente da Graduação e do Mestrado em Direito do Centro Universitário das Faculdades Metropolitanas Unidas, São Paulo. Juiz Federal em São Paulo, Brasil. E-mail: mgmartin@alumni.usp.br.

[**] Mestre em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas. Docente da Graduação em Direito do Centro Universitário das Faculdades Metropolitanas Unidas, São Paulo, Brasil.

[***] Mestranda em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas. Docente de Direito Empresarial da Escola de Negócios do Centro Universitário das Faculdades Metropolitanas Unidas, São Paulo, Brasil.

European law, General Data Protection Regulation, by the European Parliament in April 2016), and to Brazilian law, with investigation on the Internet Civil Mark (Law 12.965/2014) and the recent General Law for Data Protection (Law 13.709/2018) which, among other things, established the National Authority for Data Protection. It also established rules for companies that collect personal data from virtual sites, rights of data owners and implanted a system of administrative and juridical accountability.

KEY WORDS: Information society; Big data; Privacy; Protection of data.

BIG DATA Y PROTECCIÓN DEL DERECHO A LA PRIVACIDAD EN EL CONTEXTO DE LA SOCIEDAD DE LA INFORMACIÓN

RESUMEN: En el presente estudio se analiza el cuadro normativo de la protección al derecho constitucional a la privacidad y su posible violación en relación al uso del Big Data, describiéndose las características de esa tecnología. El tema es examinado con base en el derecho europeo (y General Data Protection Regulation, adoptado por el Parlamento Europeo en abril de 2016), y en el derecho brasileño, con incursiones por el Marco Civil de la Internet (Ley 12.965/2014) y por la reciente Ley General de Protección de Datos (Ley 13.709/2018) que, entre distintas medidas, creó la Autoridad Nacional de Protección de Datos, creó diversas obligaciones a empresas que recolectan datos personales en ambientes virtuales, establecer derechos a los titulares de esos datos, así como implantó un sistema de responsabilidad administrativa y judicial específico para el área.

PALABRAS CLAVE: Sociedad de la información; Big data; Privacidad; Protección de datos.

INTRODUÇÃO

A humanidade vive o que se tem denominado de Sociedade da Informação, ou seja, um período em que a troca de dados, as informações e o conhecimento vêm ocorrendo em nível mundial, a velocidades antes nunca concebidas e a custos cada vez menores. Esse fenômeno informacional influencia o modo como as pessoas vivem e se relacionam, o que, por conseguinte, desafia legisladores e operadores do direito a darem uma resposta satisfatória a novas necessidades e conflitos que inevitavelmente vão surgindo.

O desafio é enorme, visto que, de um modo geral, o direito tende a se mostrar estático e pouco ágil em incorporar conjunturas que se transformam com

rapidez, o que requer atenção pronta dos juristas, principalmente quando estiverem em cena direitos fundamentais, cuja proteção deve ser igualmente plena dentro dos diversos tipos de ambientes digitais.

Nesse passo, os direitos da personalidade, que foram firmemente fixados com a Declaração Universal dos Direitos Humanos em 1948 e, entre nós, definitivamente acolhidos e positivados pela Carta Magna de 1988, requerem atenção primordial, notadamente no que concerne ao conceito de privacidade no contexto próprio da Sociedade da Informação.

Assim, será inicialmente conceituado o que se entende por Big Data e sua utilização, cada vez mais constante, por diversas empresas a fim de aprimorarem seus modelos de negócios, bem como de quais maneiras o Big Data pode afetar ou até mesmo, em certas hipóteses, prejudicar os consumidores. Também será abordado o conceito de privacidade que, em face de uma nova conjuntura descortinada pela utilização em massa dos meios eletrônicos, necessita ser revisitado e aprimorado.

Igualmente será objeto de exame, sempre tendo como pano de fundo o contexto informacional já mencionado, a normatização trazida pelo *General Data Protection Regulation* (GDPR) adotado pelo Parlamento Europeu em 2016, bem como, no âmbito nacional, o Marco Civil da Internet (lei 12.965/2014) a recente Lei Geral de Proteção de Dados (lei 13.709/2018), que passará a vigorar, em sua integralidade, a partir de meados de fevereiro de 2020 e que se relaciona fortemente com o tema central ora proposto.

A metodologia empregada na elaboração do presente trabalho consiste na análise bibliográfica e normativa dos institutos jurídicos objeto do artigo, com colheita de dados feita de maneira qualitativa e resultados obtidos precipuamente por meio de indução.

1.1 SOBRE O BIG DATA

O denominado Big Data é um fenômeno típico da Sociedade da Informação e da utilização em massa de redes eletrônicas como a *internet*. Nesse campo, Pierre Lèvi enfatiza que "o surgimento do ciberespaço acompanha, traduz e promove a evolução geral da civilização. A tecnologia é produzida numa cultura, e a sociedade

é condicionada pelas tecnologias". [04]

Em se tratando Big Data, para além de uma tecnologia apropriada de captura de dados, é preciso considerar "também o crescimento, a disponibilidade e o uso exponencial de informações estruturadas e não estruturadas que caminham pela internet no âmbito da liberdade de expressão"[05].

Para além dessa concepção, é possível (e até necessário) encarar o termo Big Data não apenas como algo pertencente à informática, mas também como informações de valor econômico expressivo, ou seja, como um conjunto de dados estruturados ou não estruturados, complexos e grandiosos cujo manejo pode resultar em perspectiva de lucro do ponto de vista do *marketing*[06].

Fato é que a disponibilidade de dados estruturados e não estruturados, que servem aos mais diversos propósitos, é constantemente fornecida, muitas vezes de modo não consciente, por todos os usuários que navegam por ambientes virtuais como a *internet*. Com efeito, conforme expõe Eve Daniels:

> O Big Data está sendo gerado por tudo ao nosso redor e em todos os momentos. Cada processo digital e troca de mídia social o produz. Sistemas, sensores e dispositivos móveis podem transmiti-lo. Big Data está chegando múltiplas fontes a uma velocidade, volume e variedade alarmantes[07].

Dessa feita, podemos concluir que Big Data é o conjunto de dados fornecidos por diversas fontes, estruturados ou não, que permitem uma análise de padrões comportamentais de uma pessoa ou de um grupo de pessoas para diversos objetivos, mormente econômicos. Muito embora a definição da IBM nos traga os vetores de velocidade, volume e variedade (os denominados três V's do Big Data), não se pode ignorar um outro vetor, o vetor do valor (ou veracidade).

[04] LÉVY, Pierre. Cyberculture. Trad. p/ inglês de Robert Bononno. Minneapolis: University of Minnesota Press, 2001, p. 7. No original: "The emergence of cyberspace accompanies, translates, and promotes the general evolution of civilization. A technology is produced within a culture, and a society is conditioned by its technologies".

[05] SIMÃO FILHO, Adalberto; SCHWARTZ, Germano André Doederlein. "Big Data" big problema! paradoxo entre o direito à privacidade e o crescimento sustentável, p. 10. *In*: RIBEIRO, Diógenes Vicente Hassan; SCHWARTZ, Germano André Doederlein (org.). Teorias sociais e contemporâneas do direito. Florianópolis: CONPEDI, 2016.

[06] Vide: INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA). Big Data: impacts and benefits, 2013.

[07] Business must look at data's big picture to take advantage of analytics. IBM Systems Magazine, julho de 2015. O texto original é o seguinte: "Big data is being generated by everything around us at all times. Every digital process and social media exchange produces it. Systems, sensors and mobile devices transmit it. Big data is arriving from multiple sources at an alarming velocity".

Nessa definição, temos o volume como representativo da quantidade de dados desenvolvidos, cujas unidades variam de MB, GB, TB, PB, EB, ZB até YB[08], assim correspondendo: 1MB = 1024KB; 1GB = 1024MB; 1TB = 1024GB; 1PB = 1024TB; 1EB = 1024PB; 1ZB = 1024EB; e 1YB = 1024ZB[09]. Já a velocidade se refere à rapidez com que esses dados são desenvolvidos e modificados, enquanto que a variedade se refere às diversas fontes de dados (voz, vídeos, textos e outros).

O último vetor pode ser denominado de veracidade ou valor, mas tem a mesma raiz, visto que a própria IBM usa o termo 'veracidade' como forma de imprimir valor aos dados, isto é, esse último vetor se refere ao valor enquanto dado verídico e, portanto, passível de valor utilitário[10].

É inegável que a informação tem hoje um valor econômico expressivo e o processo de criação e processamento de dados acaba por ser um empreendimento em si, cujos procedimentos muitas vezes podem invadir esferas de direitos, em especial o direito à privacidade. Na verdade, uma das características da Sociedade da Informação é o fato do valor econômico representado pelo conhecimento (cuja geração depende de informações) ser superior ao valor dos bens materiais confeccionados a partir dele.

> Tanto é assim que, atualmente, segundo Roberto Senise Lisboa, "os ativos do conhecimento, isto é, o capital intelectual, passaram a ser mais importantes para as empresas que os ativos financeiros e físicos"[11]. Nessa seara, Paula Forgioni apregoa que "a propriedade intelectual é o maior produto de exportação dos Estados Unidos"[12].

Logo, é importante explicar, ainda que de modo sumário, como se dá esse processamento de informações, com fulcro de vislumbrar pontos de possível conflito entre os procedimentos do Big Data e o sistema jurídico. Uma das formas de se compreender o ciclo do Big Data é vê-lo em fases específicas de formação, conforme explicado a seguir[13]:

1 – geração de dados: aqui o volume dos dados é enorme, sendo gerados por inúmeras e diversas fontes e, em geral, associados a grupos específicos como

[08] Referem-se, respectivamente a: megabytes (MB), gigabytes (GB), terabytes (TB), petabytes (PB), exabytes (EB), zettabytes (ZB) e yottabytes (YB).

[09] Essas unidades de tráfego de dados correspondem à forma binária com relação um ao outro, na seguinte ordem: MB, GB, TB, PB, EB, ZB e YB.

[10] KE, Ming; SHI, Yuxin. Big Data, big change: in the financial management. Open Journal of Accounting. Beijing/China: Beijing Wuzi University, v. 3, n. 4, 2014, p. 77–82.

[11] LISBOA, Roberto Senise. O consumidor na sociedade da informação. *In*: PAESANI, Liliana Minardi (Coord.). O direito na sociedade da informação. São Paulo: Atlas, 2007, p. 121.

[12] FORGIONI, Paula A. Fundamentos do antitruste. 8. ed. São Paulo: Revista dos Tribunais, 2015, p. 313.

[13] MEHMOOD, Abid *et. al*. Protection of Big Data privacy. IEEE Xplore Digital Library, v. 4, abril de 2016, p. 1823.

comércio, pesquisa, *internet* entre outros. Podem esses dados serem pessoais ou não[14];

2 – armazenamento de dados: nessa fase há o armazenamento e manutenção da enorme quantidade de dados gerada, mas ainda não há o exame específico a respeito do material colhido; aqui requer-se grande uma infraestrutura de *hardware* para manter todos dados a salvo para a próxima fase.

3 – processamento de dados: trata-se do que se pode considerar como extração de informações úteis a partir dos dados; algo como um refinamento dos dados para usos específicos.

Como se pode notar, apenas na primeira fase, a da geração de dados, é que o usuário comum está no controle, podendo alimentar o sistema de duas maneiras: ativa ou passiva[15].

Na maneira ativa, o indivíduo fornece dados de modo consciente a um terceiro. Na passiva, ao contrário, o fornecimento é inconsciente, como, por exemplo, ao navegar por *sites* de venda e "clicar" em certo produto para saber mais detalhes, mesmo que não venha a adquiri-lo. Tal ato gera um "dado de comportamento" que provavelmente será armazenado e, posteriormente, processado fora dos auspícios do indivíduo, que nem mesmo tem ciência de como isso ocorreu.

Evidentemente, existem muitos aspectos positivos na utilização do Big Data. Em termos comerciais, por exemplo, o conhecimento de certa tendência comportamental dos consumidores pode diminuir os custos das empresas ao possibilitar o direcionamento da produção para "esse ou aquele produto", minimizando a necessidade de estocagem, o que, ao menos em tese, pode baratear os preços finais, principalmente se estiver em cena um mercado que opere sob alta concorrência. Isso pode ocorrer inclusive em áreas como a saúde[16]

Todavia, nada impede (aliás, tudo recomenda) que se deite um olhar crítico sobre os limites do uso do Big Data, de modo a não agredir a privacidade das pessoas, direito elementar da personalidade e que compõe importante aspecto da dignidade da pessoa humana.

---

[14] Segundo a lei 13.709/2018, dado pessoal é a informação relacionada à pessoa natural identificada ou identificável (art. 5º, I) e dado pessoal sensível é aquele sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (art. 5º, II).

[15] MEHMOOD, Abid *et. al*., op. cit., p. 1823.

[16] SIMÃO FILHO; SCHWARTZ, op. cit., p. 13.

2 A PRIVACIDADE E ERA INFORMACIONAL

Conforme visto acima, o indivíduo pode, seja de maneira consciente ou inconsciente, fornecer dados que, de algum modo, serão utilizados por terceiros. Ocorre que os dados de alguém acabam por compor aspectos de seus direitos de personalidade. Lembrando Carlos Alberto Bittar, tais direitos:

> são prerrogativas de toda pessoa humana pela sua própria condição, referentes aos seus atributos essenciais em suas emanações e prolongamentos, são direitos absolutos, implicam num dever geral de abstenção para a sua defesa e salva-guarda, são indisponíveis, intransmissíveis, irrenunciáveis e de difícil estimação pecuniárias. Outrossim, são inatos (originários), absolutos, extrapatrimoniais, imprescritíveis, impenhoráveis, vitalícios, necessários e oponíveis *erga omnes*, segundo a melhor doutrina e o artigo 11 do Código Civil[17].

Os direitos de personalidade incluem, dessa forma, a imagem que o próprio homem tem de si e, de acordo com o citado autor, tais direitos prescindem da positivação, eis que seriam inatos ao homem[18], o que impedem de ser limitados voluntariamente, salvo previsão legal[19].

É fato que o advento da Sociedade da Informação, principalmente a partir das últimas duas décadas, acabou por mitigar, em certos aspectos, o que se concebe por vida privada. Como bem explica Stefano Rodotá:

> O desenvolvimento da informática colocou em crise o conceito de privacidade, e, a partir dos anos 80, passamos a ter um novo conceito de privacidade que corresponde ao direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações mesmo quando disponíveis em banco de dados[20].

[17] BITTAR, Carlos Alberto. Os Direitos da personalidade. 6. ed. Rio de Janeiro: Forense Universitária, 2003, p. 11.
[18] Ibidem, p. 7.
[19] DINIZ, Maria Helena; FIUZA, Ricardo. Novo Código Civil comentado. 5. ed. São Paulo: Saraiva, 2006. p. 48.
[20] RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 267.

O direito à privacidade permanece como sendo um dos pilares da dignidade da pessoa humana, verdadeiro princípio constitucional matriz[21] que deve pautar toda e qualquer relação jurídica, ainda que seja inevitável algum tipo de mutação com a chegada da Sociedade da Informação.

É possível notar que a ideia do Big Data, que já é uma realidade e não se cuida de uma mera ilação, pode ferir o conceito expresso por Rodotá sobre a proteção dos dados pessoais, posto que, nas fases posteriores à geração de dados, o indivíduo perde, muitas vezes por completo, o direito de dispor de seus dados, tenha o fornecimento ocorrido de maneira ativa ou passiva.

A teoria dos círculos concêntricos, desenvolvida por Heinrich Hubmann, pode auxiliar na compreensão dessa possível mutação sobre o que se compreende por privacidade. Assim, de acordo com Hubmann, o sentimento de privacidade pode ser entendido como círculos com graus diferentes de densidade, em que o círculo maior se refere à privacidade, o círculo intermediário ao segredo e o menor (nuclear) se refere à intimidade[22].

Segundo aponta Szaniawski, a teoria de Hubmann foi parcialmente modificada por Heinrich Henkel, que colocou na esfera interna o segredo, na esfera intermediária a intimidade e, na esfera mais externa, a privacidade *stricto sensu*[23]

Dessa forma, continua Szaniawski, o círculo mais externo seria o da privacidade, com relações mais rasas, que conteria as informações gerais que qualquer um poderia ter sobre o indivíduo no contexto do mundo atual; já o círculo intermediário, que seria o da intimidade, conteria dados mais íntimos, disponíveis apenas para aqueles que compartilhassem o círculo mais estreito, com informações referentes ao sigilo familiar e profissional, por exemplo.

Por fim, teríamos o círculo mais recôndito, denominado de segredo, onde se esconderiam as informações mais sensíveis não compartilhadas com ninguém, nem mesmo com pessoas próximas da família. Se compreendermos esse conceito de esferas concêntricas e aplicarmos não apenas ao cotidiano, mas também à captação

[21] PIOVESAN, Flávia. Direitos humanos e o direito constitucional internacional. 4. ed. São Paulo: Max Limonad, 2000, p. 54.

[22] Conforme Thomaz Jefferson Carvalho et al.: "A teoria dos círculos concêntricos de Heinrich Hubmann, justamente analisa sob três categorias a intimidade, inserindo como a esfera mais resguardada o segredo e em seguida reserva a categoria da intimidade ou da confidência e a última a vida privada, fora destas categorias teria a vida pública com fatos de conhecimento de toda a coletividade" (Porn revenge e o compartilhamento indevido: a violação dos círculos concêntricos de Heinrich Hubmann. IX EPCC – Encontro Internacional de Produção Científica UniCesumar, nov. 2015, n. 9, p. 4-8).

[23] SZANIAWSKI, Elimar. Direitos de personalidade e sua tutela. São Paulo: Revista dos Tribunais, 1993, p. 357-358.

e processamento de dados ocorrido num ambiente de Big Data, o tema permanece complexo.

Uma primeira questão é a possibilidade de aplicação das referidas esferas concêntricas ao conceito de privacidade na Sociedade da Informação. Outra questão, especificamente em se tratando de Big Data, gira em torno do fato de o indivíduo que gera dados sobre si de maneira inconsciente e que perde o controle sobre a disposição dos mesmos, independentemente do grau de densidade da privacidade (seja privacidade *stricto sensu*, intimidade ou de segredo).

Nesses casos, é bem sabido que tais dados serão tratados de maneira a auferir o máximo de rentabilidade comercial para os terceiros interessados, que terão acesso, por exemplo, aos hábitos ou as preferências desse indivíduo. Tanto isso é verdade que é bastante comum, e isso é uma situação notória, que após alguém navegar por um *site* qualquer em busca de certo produto passe, às vezes com intensidade, a receber mensagens eletrônicas alusivas a tal produto.

Não podemos deixar de considerar que a vida atual, ao menos para a grande maioria das pessoas, seria impensável sem a constante utilização das redes eletrônicas para as mais variadas finalidades, tais como transações bancárias, compras de produtos e serviços, conversas em geral, trocas de mensagens, procura de parcerias amorosas etc. O fato é que, de acordo com Zygmunt Bauman, trocamos o pesadelo panóptico de "nunca estar sozinho" pela esperança de "nunca mais vou ficar sozinho"[24].

Assim, no universo da Sociedade da Informação, não é estranho aventar que as esferas concêntricas da personalidade começam a se esgarçar ao ponto de quase se romperem; os limites ficam de difícil visualização e não é totalmente absurdo, numa primeira acepção, pensar em responsabilizar o próprio indivíduo por sacrificar sua privacidade em troca de um ingresso na vida informacional. Até quando a teoria das esferas concêntricas irá resistir satisfatoriamente é difícil afirmar.

Destarte, o próprio Bauman ensina que o sacrifício da privacidade pode ser o pagamento do preço por maravilhas oferecidas ou uma irresistível pressão social de sacrificar a autonomia pessoal no que tange ao manejo de sua própria privacidade, ao ponto de apenas alguns poucos indivíduos conseguirem resistir[25].

É difícil encontrar um ponto de equilíbrio. Nesse campo a doutrina está a dever pensamentos mais aprofundados e concernentes à realidade informacional de

[24] BAUMAN, Zygmunt. Vigilância líquida: diálogos com David Lyon. Rio de Janeiro: Zahar, 2013, p. 30.
[25] Ibidem, p. 28.

hoje. Não basta simplesmente, como acima aludido, culpar o indivíduo por abrir mão de sua privacidade em troca das comodidades oferecidas pelos meios eletrônicos. Não se pode esquecer que a utilização da *internet* ou de redes eletrônicas afins se tornou quase que obrigatória nos últimos anos.

Não se trata de uma questão de mero deleite, sendo certo que muitas relações jurídicas, inclusive aquelas estabelecidas com a própria administração pública, se travam por meio virtual (requerimentos, consultas a procedimentos, obtenção de informações, pedidos de certidões, agendamentos de consultas médicas etc.). Diversos tipos de contratação se fazem corriqueiramente por meio eletrônico.

Nessa conjuntura, é preciso ter em mente que a obtenção e o processamento dos dados, dentro do Big Data, ocorre independentemente da urgência ou relevância dos *sites* visitados pelas pessoas. Simplesmente não há outra alternativa, salvo para aqueles que decidirem viver reclusos na selva distante.

Num contexto tão dinâmico quanto esse, a regulação do tema por meio de normas legais é possivelmente a solução mais legítima e, sobretudo, democrática. Ainda que imperfeitas, num regime democrático, as leis refletem o resultado do consenso havido entre os diversos interesses e anseios sociais existentes em determinado momento. O recurso à regulação legal tem sido o caminho escolhido por vários povos, conforme abordado a seguir.

3 A PRIVACIDADE DIGITAL NA UNIÃO EUROPEIA

É certo que cabe a cada país lidar com a questão da privacidade, segundo suas respectivas Constituições e legislação, advindo-se, evidentemente, diferenças nos respectivos regimes protetivos. Pode-se usar como exemplo os Estados Unidos da América e a União Europeia, dois dos principais polos de utilização de redes eletrônicas como a *internet*, para identificar a maneira como se lida com o problema de privacidade digital. Conforme ensinam Simão Filho e Schwartz[26]:

> Enquanto nos EUA se opera princípios de livre comércio e *opting out*, na proteção dos dados, na União Europeia se reforça a metodologia do consentimento expresso e a posição jurídica da pessoa afetada, prestigiando-se os direitos fundamentais e criando instrumentos de apoio na proteção como a figura

[26] SIMÃO FILHO; SCHWARTZ. op. cit., p. 21.

> do *Data Protection Officer* como uma entidade protetora de dados a exemplo da *Agencia Española de Protección de Datos* (AEPD)".

Isso significa que nos Estados Unidos, de um modo geral, a autonomia da vontade acaba prevalecendo sob o conceito do *opt out*[27], enquanto a União Europeia tende a ter um viés mais protetivo. Embora não seja objeto do presente artigo aprofundar a legislação comparada, nesse ponto será utilizada a experiência europeia para ilustrar o foco na proteção do direito da privacidade do indivíduo.

Como existe uma preocupação da União Europeia com os denominados dados sensíveis e o seu uso pelas grandes corporações, em 1995 foi adotada a denominada *Directive* 95/46/EC,[28] cujo objetivo era a proteção de dados pessoais, contendo, dentre outras medidas, que o uso de dados pessoais apenas poderia ocorrer apenas se o usuário permitisse e, ainda assim, apenas se necessário ao objetivo perseguido.

Esse quadro foi parcialmente modificado em 25 de maio de 2018, quando entrou em vigor o *General Data Protection Regulation* (GPDR)[29], adotado pelo Parlamento Europeu em 27 de abril de 2016 e que revogou a *Directive* 95/46/EC, elevando ainda mais a proteção à privacidade em se tratando de dados obtidos por meio eletrônico. Nesse contexto, passaram a ser objeto de proteção legal[30]:

> quaisquer informações relativas a um indivíduo, quer se trate de sua vida privada, profissional ou de sua vida pública. Pode ser qualquer coisa como um nome, uma foto, um endereço de e-mail, dados bancários, seus posts em redes sociais, suas

[27] Opt out significa que o tratamento de determinados dados, que não estão incluídos na intervenção estatal do Regulamento Geral de Proteção de Dados Europeu, pode submeter-se tanto à oposição daquele que se sentir ofendido quanto ao esquecimento (vide EUROPEAN PARLIAMENT. Directive 95/46/EC: Lex access to European law an of Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data).

[28] EUROPEAN PARLIAMENT. Directive 95/46/EC: lex access to European law an of Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[29] COUNCIL OF THE EUROPEAN UNION. Proposal 9565/15 for a regulation of the general data protection regulation.

[30] BRUSSELS. The European Commission: proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses. O texto original é o seguinte: "any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, your posts on social networking websites, your medical information, or your computer's IP address. The EU Charter of Fundamental Rights says that everyone has the right to personal data protection in all aspects of life: at home, at work, whilst shopping, when receiving medical treatment, at a police station or on the Internet".

> informações médicas, ou seu endereço de IP no computador. A Carta dos Direitos Fundamentais da União Europeia diz que todos têm direito à proteção dos dados pessoais em todos os seus aspectos da vida: em casa, no trabalho, enquanto faz compras, quando está recebendo tratamento médico, em uma delegacia de polícia ou na própria *Internet* .

O GPDR[31] criou obrigações referentes ao uso de dados pelos respectivos controladores[32]. O direito ao esquecimento é uma dessas obrigações, salvo exceções impostas no art. 65 que inclui a necessidade de retenção dos dados para defesa legal, por exemplo. Outro aspecto importante é que o GPDR exige uma anuência clara do usuário para o uso de dados particulares.

O art. 24 do GDPR foca especificamente no Big Data e o art. 60[33] exige que o indivíduo seja informado do processamento de informações a seu respeito e o propósito para tal e, mais importante, o indivíduo deverá ser cientificado da existência de *profiling* (análise do perfil) e das consequências do seu uso. Deverá mesmo ser informado da lógica do *profiling*, ou seja, não apenas as razões do *profiling*, mas também de como é feita essa análise de perfil. A redação dos textos dos referidos arts. 24 e 60 evidenciam essas exigências, valendo a respectiva transcrição:

> Art. 24. O tratamento dos dados pessoais de seus titulares que estejam sob controle de alguém, subcontratante ou que não esteja estabelecido na União, também deve sujeitar-se ao presente regulamento quando estiver relacionado com o monitoramento do comportamento dessas pessoas, já que seu papel ocorre dentro do território nacional. Para determinar se uma atividade de processamento de dados pode ser considerada válida a monitorar o comportamento dos titulares de dados, deve determinar-se se as pessoas, singularmente consideradas, são rastreadas na Internet, incluindo o uso subsequente de técnicas de processamento de dados que consistem em traçar uma pessoa, particularmente para tomar decisões relativas a ela ou analisar e prever suas preferências, comportamentos e atitudes" (tradução livre).
> Art. 60. Os princípios de processamento justo e transparente

[31] EUR-LEX ACCESS TO EUROPEAN LAW. Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016.

[32] No Brasil, a teor do art. 5º, VI, da Lei 13.709/2018, o controlador é pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

[33] EUR-LEX ACCESS TO EUROPEAN LAW, cit.

> exigem que o titular dos dados seja informado da existência da operação e de seus objetivos. O responsável pelo tratamento deve fornecer ao titular dos dados quaisquer informações adicionais necessárias para garantir um tratamento justo e transparente, tendo em vista as circunstâncias específicas e o contexto em que os dados pessoais são processados. Além disso, o titular dos dados deve ser informado da existência de perfis e das consequências de tal definição. Quando os dados pessoais são recolhidos do titular dos dados, o seu titular também deve ser informado para saber se está ou não obrigado a fornecer os dados pessoais e quais as consequências, caso não os forneça. Essas informações podem ser fornecidas em combinação com ícones padronizados, a fim de oferecer, de um modo facilmente visível, inteligível e legível, uma visão geral significativa do processamento pretendido e, onde os ícones forem apresentados eletronicamente, eles deverão também ser legíveis, por máquinas" (tradução livre) [34].

Constata-se, pois, que a União Europeia busca limitar o uso indiscriminado de Big Data, impondo obrigações relevantes ao controlador. É possível antever, dessa maneira, que se busca ultimar um equilíbrio entre os interesses comerciais das grandes corporações (legítimos, aliás) com a questão da privacidade dos usuários que, como visto, ao menos na grande maioria das hipóteses, não podem simplesmente decidir por não se servirem das redes eletrônicas nos seus mais diversos afazeres. O mesmo vem ocorrendo em países como o Brasil.

[34] UNIÃO EUROPEIA. 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. No original: "Art. 24. The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes" [...] "Art. 60. The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable".

4 A PRIVACIDADE DIGITAL NO BRASIL

O art. 3° do Marco Civil da Internet (lei nº 12.965, de 23 de abril de 2014) traz como um de seus princípios a proteção da privacidade (inciso II) e, em seguida, a proteção dos dados pessoais (inciso III), na forma da lei, sendo esta a Lei Geral de Proteção de Dados Pessoais (lei nº 13.709, de 14 de agosto de 2018).

Apesar dos debates sobre regulamentação da *internet* não serem recentes[35], o Marco Civil da Internet no Brasil, notadamente o art. 7º, inciso VIII, alínea 'c', preceitua que as empresas não podem utilizar os dados das pessoas, salvo disposição expressa em contratos de prestação de serviços ou termos de uso.

Entretanto, se essa proteção se referir apenas aos dados estruturados fornecidos pelo usuário (é o que parece), a conclusão é que o Marco Civil da Internet não previu a fluidez própria da operacionalização do Big Data, cuja alimentação (fornecimento de dados) pode ocorrer de maneira automática, sem mesmo que o usuário tenha consciência a respeito. Por conseguinte, da forma como foi editada, essa lei restou um tanto quanto insuficiente no que tange à proteção em face do Big Data.

Prosseguindo, no que tange à já referida lei 13.709 (LGPD), logo no art. 1º é preceituado que a norma dispõe sobre o tratamento dos dados das pessoas[36], tanto no meio físico quanto nos meios digitais, sejam pessoas físicas ou jurídicas, com o objetivo de proteger os direitos fundamentais da liberdade e da privacidade. Entretanto, o *modus operandi* dos ambientes digitais, notadamente considerando o advento do Big Data, torna bastante complexo esse tipo de proteção. Aqui, segundo Manuel Castells[37]:

> O entusiasmo com a liberdade trazida pela Internet foi tamanho que esquecemos a persistência de práticas autoritárias de vigilância no ambiente que continua sendo o mais importante de nossas vidas: o local de trabalho. À medida que os trabalhadores se tornam cada vez mais dependentes da

[35] LIMA, Caio César Carvalho. Garantia da privacidade e dados pessoais à luz do Marco Civil da Internet. *In:* LEITE, George Salomão; LEMOS, Ronaldo (coord.). Marco civil da internet. São Paulo: Atlas, 2014, p. 148-164.

[36] Conforme estabelece o art. 5º, X, da LGPD, tratamento é "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

[37] CASTELLS, Manuel. A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade. Trad. de Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar, 2003, p. 143.

> interconexão por computador em sua atividade, a maioria das companhias decidiu que têm o direito de monitorar os usos de suas redes por seus empregados.

Não se pode negar, contudo, que a Lei Geral de Proteção de Dados vem ao encontro da tendência internacional de se proteger direitos como a privacidade dentro dos ambientes virtuais, sendo certo que a norma em foco atribui direitos subjetivos aos titulares dos dados pessoais, bem como impõe limitações e obrigações àqueles responsáveis pelos tratamentos de dados[38].

Nessa toada, por exemplo, o art. 7º, I, determina que o tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular, sendo restritas as hipóteses em que esse consentimento é dispensado, encontrando-se tais dispensas relacionadas ao atendimento de interesses maiores (incisos II a X do art. 7º). Apenas como exemplos, dispensa-se o consentimento: para o cumprimento de obrigação legal ou regulatória pelo controlador (inciso II), para a proteção da vida ou da incolumidade física do titular ou de terceiro (inciso VII), para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias (inciso VIII), para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (inciso X).

Ademais, o consentimento necessita referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais são tidas por nulas (§4º do art. 8º), sendo possível a revogação a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado (§4º do art. 8º). O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados (art. 9º, *caput*), sendo que o controlador deve adotar medidas para garantir a transparência do indigitado tratamento (§2º do art. 10).

Por sua vez, o art. 18 da LGPD estatui que o titular dos dados pessoais tem direito de obter do controlador informações a respeito dos respectivos dados tratados, mediante requisição, destacando-se que, segundo o art. 20 da norma em foco, é possível solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que venham a atingir interesses do titular, incluídas as decisões relativas à definição de perfil pessoal, profissional, de consumo e de crédito ou mesmo outros aspectos de sua personalidade.

[38] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 49.

Nos termos do art. 55-A da LGPD (incluído posteriormente ao texto original), foi criada a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República, cuja missão é atuar como órgão administrativo regulador da proteção dos dados. Dentre as várias competências da ANPD que, em resumo, funciona como uma espécie de agência regulatória, está a possibilidade de aplicar sanções administrativas em caso de infrações cometidas às normas da LGPD. Nesses termos, o art. 52 prevê as seguintes penalidades:

> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.

A LGPD também traz disposições a respeito da responsabilidade e dever de indenização em caso de danos provocados por controladores ou operadores de dados pessoais, sendo certo que, nos termos do §2º do art. 42, analogamente ao que ocorre no direito do consumidor, poderá haver inversão do ônus da prova a favor do titular dos dados quando "houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa".

Evidentemente, somente após a integral entrada em vigor da LGPD[39] é que se poderão tornar mais aprofundados os estudos a seu respeito, dado que, apenas a partir de então, é que a dinâmica social passará a engendrar situações concretas quiçá não previstas ou integralmente reguladas pela legislação e, por conseguinte, se poderá testar os diversos instrumentos protetivos insculpidos na norma.

De qualquer forma, diante do aqui esposado, notadamente em face de ter sido conferido ao titular maior transparência e possibilidade de controle sobre seus dados pessoais, bem como considerando a criação de uma autoridade nacional e um sistema sancionatório específico, fica bastante clara a intenção da lei 13.709/2018 de conferir proteção suficientemente eficaz à privacidade das pessoas nos ambientes virtuais. Em resumo, em linha assemelhada à legislação europeia, a LGPD também busca limitar o uso indiscriminado do Big Data.

[39] Partes da LGPD somente entrarão em vigor 24 (vinte e quatro) meses após sua publicação (art. 65, II).

5 CONSIDERAÇÕES FINAIS

O cenário social descortinado após o advento da Sociedade da Informação, com a utilização em massa de redes eletrônicas como a *internet*, passou a requerer de legisladores e operadores do direito atenção especial no tratamento a direitos da personalidade como a privacidade, visto que a utilização de tais mecanismos permite que terceiros colham enorme variedade de dados pessoais dos respectivos usuários, muitas vezes de maneira camuflada ou não declarada, principalmente com finalidade econômica, mas não só.

Esse fenômeno ficou conhecido como Big Data, dada a disponibilidade e o uso exponencial dessa pletora de informações estruturadas e não estruturadas disponíveis nas redes. Tanto é que tem se tornado cada vez mais comum o recebimento de anúncios eletrônicos acerca de um produto anteriormente pesquisado pelo usuário em algum *site*, muitas vezes poucos minutos antes. Portanto, a colheita prévia de dados para posteriores ofertas comerciais é uma realidade que não pode ser negada.

Como na atualidade, para a maioria das pessoas, é praticamente impossível levar a vida sem a utilização das redes eletrônicas, o fornecimento de dados pessoais, seja de modo consciente ou inconsciente, desafia a efetiva proteção do que se concebe por privacidade, elemento que compõe a dignidade da pessoa humana.

Diante disso, os países vêm positivando leis e normas regulamentares que procuram equilibrar os legítimos interesses econômicos das grandes corporações com os não menos legítimos anseios pela preservação da privacidade das pessoas. Nessa toada, o *General Data Protection Regulation* da União Europeia, dentre outras medidas, proíbe a extração de dados privados de maneira automática para compor um perfil de consumo sem anuência do usuário que, em adição, deve ser informado de maneira clara sobre quais dados está fornecendo e para quais finalidades.

No que se refere ao direito brasileiro, o Marco Civil da Internet (lei 12.965/2014) mostrou-se insuficiente para conferir uma adequada proteção à privacidade frente ao fenômeno do Big Data, o que, em certa medida, procurou ser corrigido pela Lei Geral de Proteção de Dados (lei 13.709/2018) que majorou o nível de proteção ao determinar medidas como maior transparência por parte das empresas operadoras e controladoras, além da possibilidade de controle pelo titular sobre os dados pessoais fornecidos.

A norma em foco igualmente criou a Autoridade Nacional de Proteção de Dados e um sistema sancionatório administrativo e judicial específico, com possibilidade de inversão do ônus da prova em benefício do usuário. Todavia, considerando que a LGPD somente entrará integralmente em vigor no início de 2020, ainda é cedo para aferir os resultados em termos de limitação do uso indiscriminado do Big Data no Brasil.

REFERÊNCIAS

BAUMAN, Zygmunt. **Vigilância líquida**: diálogos com David Lyon. Rio de Janeiro: Zahar, 2013.

BITTAR, Carlos Alberto. **Os Direitos da personalidade**. 6. ed., Rio de Janeiro: Forense Universitária, 2003.

BRASIL. **Constituição da República Federativa do Brasil**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 28 set. 2018.

BRASIL. **Lei nº 12.527**, de 18 de novembro de 2011. Lei de Acesso à Informação. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 30 nov. 2018.

BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 30 nov. 2018.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Dispõe sobre a Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 30 nov. 2018.

BRUSSELS. **The European Commission**: proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses. Disponível em: http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en. Acesso em: 20 nov. 2018.

CARVALHO, Thomas Jefferson; CARAVELO, Luiz Felipe Rocha; CASADO, Aline Pescaroli; SILVA, Felipe Rangel da; FERREIRA, Allan Bruno Gomes. Porn revenge e o compartilhamento indevido: a violação dos círculos concêntricos de Heinrich Hubmann. *In*: EPCC – ENCONTRO INTERNACIONAL DE PRODUÇÃO CIENTÍFICA

UNICESUMAR, 9., nov. 2015, n. 9, p. 4-8. **Anais eletrônico** [...]. Maringá, PR: UniCesumar, Disponível em: http://www.cesumar.br/prppge/pesquisa/epcc2015/anais/thomaz_jefferson_carvalho_2.pdf. Acesso em: 10 fev. 2019.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Trad. de Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar, 2003.

COUNCIL OF THE EUROPEAN UNION. **Proposal 9565/15 for a regulation of the general data protection regulation**. Disponível em: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf. Acesso em: 20 nov. 2018.

DANIELS, Eve. Business must look at data's big picture to take advantage of analytics. **IBM Systems Magazine**, julho de 2015. http://ibmsystemsmag.com/power/businessstrategy/bi-and-analytics/data-big-picture. Acesso em: 27 nov. 2018.

DINIZ, Maria Helena. **Código Civil Anotado**. 13. ed. São Paulo: Saraiva, 2008.

DINIZ, Maria Helena; FIUZA, Ricardo. **Novo Código Civil comentado**. 5. ed. São Paulo: Saraiva, 2006.

EUROPEAN PARLIAMENT. **Directive 95/46/EC***:* Lex access to European Law of Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Disponível em: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046. Acesso em: 20 nov. 2018.

EUR-LEX ACCESS TO EUROPEAN LAW. **Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016**. Disponível em: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em: 20 nov. 2018.

FORGIONI, Paula A. **Fundamentos do antitruste***.* 8. ed. São Paulo: Revista dos Tribunais, 2015.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA). Big Data – impacts and benefíts. 2013. Disponível em: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Big-Data-Impacts-and-Benefits.aspx. Acesso em: 20 nov. 2018.

KE, Ming; SHI, Yuxin. Big Data, big change: in the financial management. **Open**

Journal of Accounting. Beijing/China: Beijing Wuzi University, v. 3, n. 4, 2014, p. 77–82. Disponível em: http://file.scirp.org/Html/1-2670045_49748.htm. Acesso em: 27 nov. 2018.

LÉVY, Pierre. **Cyberculture**. Trad. Robert Bononno. Minneapolis: University of Minnesota Press, 2001.

LIMA, Caio César Carvalho. Garantia da privacidade e dados pessoais à luz do Marco Civil da Internet. *In*: LEITE, George Salomão; LEMOS, Ronaldo (coord.). **Marco civil da internet**. São Paulo: Atlas, 2014, p. 148-164.

LISBOA, Roberto Senise. O consumidor na sociedade da informação. *In*: PAESANI, Liliana Minardi (coord.). **O direito na sociedade da informação**. São Paulo: Atlas, 2007, p. 113-142.

MEHMOOD, Abid; NATGUNANATHAN, Iynkaran; XIANG, Yong; HUA, Guang; GUO, Song. Protection of Big Data privacy. **IEEE Xplore Digital Library**, v. 4, abril de 2016, p. 1823. Disponível em: https://ieeexplore.ieee.org/document/7460114. Acesso em: 27 set. 2018.

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

PIOVESAN, Flávia. **Direitos humanos e o direito constitucional internacional**. 4. ed. São Paulo: Max Limonad, 2000.

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

SIMÃO FILHO, Adalberto; SCHWARTZ, Germano André Doederlein. "Big Data" big problema! paradoxo entre o direito à privacidade e o crescimento sustentável. *In*: RIBEIRO, Diógenes Vicente Hassan; SCHWARTZ, Germano André Doederlein (org.). **Teorias sociais e contemporâneas do direito**. Florianópolis: CONPEDI, 2016, p. 10. Disponível em: https://www.conpedi.org.br/publicacoes/c50o2gn1/tz6xhk8k/cBPURL3ZR7xFVuQD.pdf. Acesso em: 27 set. 2018.

SZANIAWSKI, Elimar. **Direitos de personalidade e sua tutela**. São Paulo: Revista dos Tribunais, 1993.

UNIÃO EUROPEIA. **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. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=pt. Acesso em: 20 nov. 2018.

Recebido em: 22/02/2019

Aceito em: 10/12/2019