UNIVERSIDADE TIRADENTES – UNIT

CURSO DE GRADUAÇÃO EM DIREITO

TRABALHO DE CONCLUSÃO DE CURSO – ARTIGO CIENTÍFICO

A IMPRECISÃO DO ART. 12 DA LGPD NO CENÁRIO DO *BIG DATA*

Hianna Maria Dantas Costa

Orientador: Prof. Me. Jéffson Menezes de Sousa

Aracaju

2020

HIANNA MARIA DANTAS COSTA

A IMPRECISÃO DO ART. 12 DA LGPD NO CENÁRIO DO *BIG DATA*

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito da Universidade Tiradentes – UNIT, como requisito parcial para obtenção do título de Bacharel em Direito.

Aprovado em_____/_____/_____.

Banca Examinadora

Professor Orientador – Me. Jéffson Menezes de Sousa

Universidade Tiradentes

Professor Examinador – Ma Fernanda Oliveira Santos

Universidade Tiradentes

Professor Examinador – Ma.Valquiria Nathali Cavalcante Falcão

Universidade Tiradentes

A IMPRECISÃO DO ART. 12 DA LGPD NO CENÁRIO DO *BIG DATA*

THE INACCURACY OF ART. 12 OF THE LGPD IN THE BIG DATA SCENARIO

Hianna Maria Dantas Costa[1]

RESUMO

O presente artigo objetiva desenvolver a temática da Lei Geral de Proteção de dados Pessoais em face da obscuridade do termo "esforços razoáveis" do art. 12, da dita lei, face ao processo de anomização quando objeto de tratamento pelo Big Data. Para tanto, foi realizada uma análise, por meio de uma estratégia metodológica de caráter fenomenológico-hermenêutico e transdisciplinar. Dentre as considerações finais, foi exposto que, muito embora haja a utopia que os dados tornam-se anônimos, estes são reindentificados quando há expostos ao tratamento junto com o banco de dados - *Big Data*.

Palavras-chave: Big Data. Lei Geral de Proteção de Dados. União Europeia.

ABSTRACT

This article aims to develop the theme of the General Law for the Protection of Personal Data in view of the obscurity of the term "reasonable efforts" of art. 12, of said law, in view of the process of anomeization when subject to treatment by big data. Therefore, an analysis was performed, through a methodological strategy of phenomenological-hermeneutic and transdisciplinary character. Among the final considerations, it was stated that, although there is the utopia that data becomes anonymous, it is reidentified when exposed to treatment along with the database - Big Data.

Keywords: Big Data. General Data Protection Law. European Union.

[1] Bacharelanda em Direito pela Universidade Tiradentes – UNIT, *campus* Estância. E-mail: hianna-maria@hotmail.com

1 INTRODUÇÃO

O avanço tecnológico e do capitalismo, fizeram com que a sociedade se organizasse por meio das redes, fato este que desencadeou discussões acerca da proteção de dados pessoais dos usuários, tendo em vista que, tais dados têm um valor econômico elevadíssimo tornando-se o "petróleo" do século XXI, o que gerou uma disputa voraz entre as empresas privadas, que diariamente investem em bancos de dados automatizados para se apropriar das novas tecnologias que permitem a análise de *big data*, o que em contrapartida, demanda pensar na proteção jurídica dos dados pessoais.

Atualmente, nota-se que as pessoas estão cada vez mais reféns de seus smartphones e seus aplicativos, os quais revelam o perfil detalhado do consumidor graças ao seu uso constante, seja por meio de compras, clicks, pesquisas ou até mesmo com informações inseridas voluntariamente. Contudo, o tratamento de dados pessoais, em particular por processos automatizados, é, uma atividade de risco. Pois, se utilizada por empresas privadas com finalidade diversa, poderá haver manipulação de informações e reversão do anonimato dos usuários.

Diante disso, no Brasil, em 14 de agosto de 2018, foi editada a Lei no 13.709, conhecida como a Lei Geral de Proteção de Dados Pessoais – LGPD, com o fito unificar as regras sobre o tratamento de dados pessoais de clientes de empresas públicas e privadas, proporcionando mais segurança aos dados de terceiros. Dessa forma, será realizada uma análise, por meio, de uma estratégia metodológica de caráter fenomenológico-hermenêutico e transdisciplinar, onde será abordada a imprecisão e obscuridade do termo "esforços razoáveis" presente no art. 12 da LGPD no cenário do *big data*.

2 O BIG DATA E O PROCESSO DE ANONIMIZAÇÃO DE DADOS

2.1 *Big Data* (Megadados ou Grandes Dados)

O presente termo foi conceituado a partir dos anos 2000, todavia, até hoje não se tem uma definição rigorosa para o termo, considerando as suas características, Mayer-Schonberger e Cukier (2000) definem o *big data* como um conjunto de tendências tecnológicas que consiste em uma abordagem que aplica à matemática uma enorme quantidade de dados a fim de prever probabilidades, permitindo analisar muito mais dados,

sem devoção ao rigor da exatidão, buscando descobrir novos padrões e correlações nos dados que propiciam novas e valiosas ideias. Outros autores como Zikopoulos et al. (2012) dizem que *big data* se caracteriza por quatro aspectos: veracidade, variedade, velocidade e volume.

O aspecto veracidade condiz ao quão confiável e verdadeiro são os respectivos dados e informações. A variedade refere-se à variabilidade de formatos os dados são encontrados, já a velocidade descreve a rapidez que as informações são criadas e dispostas na internet. E o volume refere-se à quantidade de dados e informações que a indústria recebe ao longo de um determinado tempo.[1]

O *big data* é uma ferramenta que possibilita a análise e a interpretação de grandes volumes de dados, os quais são gerados diariamente através do uso da internet, de forma sistematizada, permitindo soluções especificas e acertadas. Possibilitando para as empresas, o esclarecimento preciso das preferencias e aversões dos indivíduos, para assim, disporem de uma maior segmentação de anúncios, produtos e serviços com base nesse conhecimento.

O crescimento exponencial de volume de dados gerado é gritante. Seguindo este contexto, Tótora (2006) afirma que no mundo capitalista pós Revolução Industrial, as pessoas são ferramentas essenciais para a máquina, e não somente usuários. São partes de um looping de informação.

Com isso, entende-se que a análise do *big data* revela uma forma de controle e vigilância dos usuários da internet, que diariamente, tem suas informações pessoais captadas pelo simples uso da rede, proporcionando para as empresas detentoras dos dados, a realização de uma análise meticulosa e aprofundada para encontrar estratégias corretas, a partir de padrões comportamentais que visem a objetivos específicos, tais como: Redução de custos, Economia de tempo, Desenvolvimento de produtos e Otimização de ofertas e criação promoções a partir de hábitos identificados do cliente.

Isto justifica a corrida para obter e desenvolver tecnologias capazes de capturar dados, visto que as máquinas não são somente evoluções da tecnologia, mas sim uma mutação (BRAGA; VLACH, 2004). As tecnologias detectam a posição de cada um, lícita ou ilicitamente, e operam uma modulação universal, através do controle contínuo e da comunicação instantânea abrindo espaço para violações à privacidade dos indivíduos

[1] ZIKOPOULOS, P; DE R OOS, D; PARASURAMAN, K; DEUTSCH, T; G ILES, J; CORRIGAN, D. Harness the power of Big Data- The IBM Big Data Platform. Emer yville: McGraw-Hill Osborne Media, 2012.

(DELEUZE, 1992).

2.2 Casos Conexos a Exploração de Dados Pessoais em Detrimento dos Cidadãos Brasileiros

O aproveitamento inadequado de dados pessoais gera resultados negativos para os cidadãos brasileiros, assim como para todos os outros usuários do mundo, não é novidade. Neste sentido, insigne a divulgação do ex-analista de inteligência Edward Joseph Snowden, a qual deu mais clareza a esta problemática, onde restou demonstrado a indistinção entre a exploração de informações pessoais de cidadãos alvo de investigação versus a exploração em massa de cidadãos comuns e até mesmo autoridades, como no caso do Brasil na espionagem da presidente Dilma. Junto a tal fato, próximo a edição da LGPD, casos parecidos foram expostos de abuso na obtenção de dados pessoais de brasileiros.

De acordo com Stone (2016), as declarações de Snowden revelaram a invasão da privacidade dos cidadãos pelos EUA, inclusive de pessoas que sequer eram investigadas por motivo algum, além da espionagem das agências estatais e de lideranças mundiais de outros países com o intuito de obter vantagem política e econômica. Como exemplo constam a aquisição de informações privilegiadas da empresa de Petróleo Brasileiro S.A., a Petrobras, e de líderes mundiais, tais como a Premier da Alemanha, Angela Merkel e a presidente do Brasil, Dilma Vana Rousseff. Tais declarações foram enviadas a jornalistas por meio de documentos secretos, sobre o período em que prestou serviços nas agências de inteligência norte-americanas, CIA - *Central Intelligence Agency* e NSA - *National Security Agency*, compreendido entre os anos de 2004 a 2013 e em virtude disso houve uma grande comoção mundial e o alerta sobre a insegurança no tráfego dos dados no ciberespaço.

Com os documentos cedidos por Snowden, percebeu-se a vulnerabilidade das informações que circulam pela rede mundial de computadores, principalmente, para operar na mutação do capitalismo. No programa Optic Nerve, verificou-se que milhões de internautas, em todo o mundo, sofreram interceptação e armazenamento de imagens de webcam do Yahoo pelo serviço de inteligência Britânico GCHQ - *Government Communications Headquarters* que faz parte do sistema de inteligência do Reino Unido (UK), com a ajuda da NSA, Agência de Segurança Nacional dos Estados Unidos. Em apenas seis meses, milhões de usuários no mundo inteiro, não suspeitos de irregularidades, sofreram vigilância em massa, interceptação e armazenamento de imagens da webcam do *Yahoo*, violando-se a privacidade dos usuários, incluindo uma grande quantidade de imagens sexualmente explícitas. (ACKERMAN; BALL,

2014; STONE, 2016).

Outro caso envolvendo a obtenção de dados pessoais de forma controversa foi conhecido quando se tornaram evidenciadas as práticas da empresa *Cambridge Analytica* no levantamento de inclinações políticas e da personalidade dos americanos, através de um teste psicográfico desenvolvido com base em dados pessoais extraídos da plataforma do *Facebook*. (CONFESSORE, 2018; GUIMÓN, 2018). Esse foi o maior vazamento de dados pessoais da história do Facebook, com cerca de 87 milhões de contas potencialmente impactadas e compartilhadas com a empresa Cambridge Analytica de maneira imprópria. Desse total, aproximadamente meio milhão de contas eram de brasileiros. Recentemente, foi divulgado pelo Diretor Técnico, chefe responsável por toda a parte tecnológica do Facebook, Chief Technology Officer, Mike Schroepfer, que 443.117 contas de brasileiros foram afetadas e compartilhadas indevidamente com a Cambridge Analytica (SCHROEPFER, 2018).

Mais prejuízo foi identificado noutro caso onde anota-se o vazamento de dados pessoais no Banco Inter S/A, cuja interferência de instituições públicas fez-se mister. Dessa vez, uma ação civil pública da CPDP do MPDFT pediu indenização de R$ 10.000.000,00 (dez milhões de reais) pelo fato de ocorrer efetivos danos morais coletivos por vazamento de dados pessoais de clientes desse banco e pessoas com as quais houve transações com esses clientes.

2.3 Processo de Anonimização de Dados

A rotina diária das pessoas e todos os seus dados, passaram a ser documentadas e armazenadas, considerando que, hoje, a maior parcela da população mundial utiliza a internet, de forma ilimitada no tempo e no espaço. Pode-se dizer que, a interação pessoal foi substituída pela virtual, através das redes sociais, tais como: *Google*, *Facebook*, *Instagram*, *Twitter*, etc. De repente, computadores nas escrivaninhas e nos quartos das crianças se tornaram quesito “obrigatório” em todas as famílias (SCHAAR, 2007).

Vale ressaltar que, foi o uso individual de mecanismos tecnológicos que possibilitaram o armazenamento e avaliação de dados pessoais relativos à vida intima, aumentando a possibilidade de pré-identificação mesmo após a anonimização, sem que houvesse a necessidade de um complexo prequestionamento apropriado para tal finalidade. Situações como estas começam a evidenciar a necessidade de criação de novas fronteiras, agora adequadas à realidade digital (DONEDA, 2006).

Uma pesquisa publicada na *Harvard Business Review* Brasil em fevereiro de 2016 aponta que as pessoas, apesar de terem pleno conhecimento de que suas informações pessoais são coletadas pelas empresas com que mantêm relação, surpreendem-se com a falta de informação quanto aos tipos específicos de dados que fornecem; a pesquisa aponta que, das pessoas entrevistadas, 27% percebem que compartilham a sua lista de amigos em redes sociais, 25% que compartilham a sua localização, 23% suas buscas na web, 18% seus históricos de comunicação como "*chat logs*", 17% seus endereços de IP e 14% percebem que compartilham seu histórico de navegação na web. (MOREY et al., 2016).[2]

Mas como ocorre a anomização desses dados? Primeiramente, faz-se necessário definir dados anônimos e anonimizados. Aquele é caracterizado pela impossibilidade de identificação de um indivíduo, os quais não são objeto de proteção pelas leis. Já os dados anonimizados, por sua vez, dizem respeito a dados que, por meio de técnicas de anonimização, tiveram seu potencial de identificação mitigado. Então, vê-se que eles são submetidos a técnicas especificas de supressão, generalização e pseudoanonimização[3].

Há múltiplas razões para anonimização de dados, dentre elas, a redução de riscos de serem transmitidos dados entre empresas privadas ou do vazamento desses dados, posto que, com a formação de perfis, por meio de banco de dados automatizados, somos mapeados e copiados para dentro do sistema. Deixamos de ser usuários do produto para sermos o produto.

Um ponto crucial para a razão da anonimização dos dados é relativo à impossibilidade de reidentificação do usuário e titular dos dados, para que tão logo não seja utilizado como produto. Tal processo, visa eliminar o elo entre o elemento identificador e o sujeito titular, com o fito de vedar a reidentificação. Entretanto, o pensamento de que técnicas de anonimização podem garantir de maneira integral a reidentificação não passa de um mito (NARAYANA; SHMATIKOV, 2010).

De acordo com Bioni (2019), hoje, não existe uma técnica que possibilite de maneira integral impedir a pré-identificação do usuário. Ao invés disto, exige-se das operações de anonimização que o resultado final gere dados que não lograriam ser reassociados ao seu titular através do emprego das tecnologias disponíveis à época do tratamento. Nesse interim, a ideia de impossibilidade integral da irreversibilidade do processo de anonimização dá espaço a mitigação dos riscos de irreversibilidade.

[2] (MOREY, Timothy; FORBATH, Theodore; SCHOOP, Alisson, Dados dos consumidores: modelos de transparência e confiança. Harvard Business Review Brasil, São Paulo, fevereiro 2016, p. 47)
[3] BIONI, Bruno Ricardo. Op. Cit. 2016. p. 25

A LGPD dispõe em seu artigo 5º, III, que o dado anonimizado corresponde ao "dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento". No caput do artigo 12, encontramos:

> Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.
> § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.
> § 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

Ao analisar o art. 12, da LGPD, percebe-se que os dados anonimizados não estão resguardados pela referida lei, salvo quando possível sua reversão e a identificação de técnicas razoáveis e disponíveis ao tempo do seu tratamento, que ensejem a desconsideração do anonimato como dado pessoal, levando em conta a razoabilidade.

Não obstante, cabe indagar o que são "esforços razoáveis" e se o trabalho foi realizado por "meios próprios". Está problemática não se encontra solucionada no ordenamento brasileiro, a qual não traçou limites da anonimização. Entretanto, busca-se inspiração na experiência europeia, que emitiu um parecer 05/2014 sobre técnicas de anonimização, segunda o qual não são considerados anônimos os dados que permitam a individualização do usuário.

Espera-se que a recém-criada Autoridade Nacional de Proteção de Dados, no exercício de sua competência de editar normas sobre privacidade e proteção de dados, manifeste-se prontamente, considerando a sensibilidade da questão.

Além disso, o parágrafo 2º do art 12, LGPD, nos traz uma segunda hipótese de proteção, senão vejamos, os dados anonimizados poderão ser considerados pessoais, caso sejam utilizados para a prática de definição de perfil comportamental de determinada pessoa natural, conquanto seja identificada. Isto evidencia uma abordagem consequencial sobre os dados anonimizados, é dizer, em vez de ater-se à consideração da razoabilidade da reversão do processo de anonimização, a lei leva em conta os possíveis impactos a serem gerados ao livre desenvolvimento da personalidade individual decorrentes do processamento de dados.

Diante do que foi abordado, Rodotà (2008) sustenta que a formação de perfis baseados em dados pessoais sensíveis pode gerar discriminação por dois motivos: 1°) Seja porque

dados pessoais, aparentemente não “sensíveis”, podem se tornar sensíveis se contribuem para a elaboração de um perfil; 2°) seja porque a própria esfera individual pode ser prejudicada quando se pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas.

Para que a plenitude à esfera pública seja mantida, são determinadas rigorosas condições de circulação destas informações. Elas recebem um fortíssimo estatuto “privado”, que é manifestada, sobretudo, pela intervenção de sua coleta por parte de alguns sujeitos (por exemplo, empregadores) e pela exclusão de legitimidade de certas formas de coleta e circulação (RODOTÀ, 2008).

2.4 Fiscalização e Padrões Técnicos de Segurança

Em julho de 2019, foi aprovada a Lei 13.385/19, atribuindo a criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão federal com o objetivo de regulamentar e fiscalizar o cumprimento da nova lei. A finalidade é desenvolver um elo entre o governo e a sociedade. Nada impede, porém, que órgãos como Ministério Público, Procon e Secom também atuem em questões jurídicas ou aplicação de multas.

Deve-se destacar que, o presidente Jair Bolsonaro, vetou 09 (nove) dispositivos da lei, dentre eles a proibição dos órgãos públicos compartilharem dados pessoais de cidadãos que utilizarem a Lei de Acesso à Informação. Mas, permaneceu a regulamentar que as empresas serão auditadas e caso constatado irregularidades serão multadas.

Os principais princípios abordados nesta temática na LGPD, são direcionados aos temas de segurança, prevenção e da responsabilização e prestação de contas. Segurança e sigilo representam dois elementos incontornáveis para que, de fato, seja possível falar em proteção de dados pessoais (SOUZA, 2019).

Neste sentido, o art. 52 prevê sanções administrativas para o descumprimento da LGPD, são elas: Advertência, com indicação de prazo para adoção de medidas corretivas; Multa simples, de até 2% do faturamento líquido da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, limitada, no total, a R$ 50.000.000,00 por infração; Multa diária; Publicação da infração após devidamente apurada e confirmada a sua ocorrência; Bloqueio dos dados pessoais envolvidos na infração até a sua regularização;

Eliminação dos dados pessoais envolvidos na infração.

3 A (DES)PROTEÇÃO DE DADOS ANONIMIZADOS E OS PADRÕES ADOTADOS PELO GDPR NA UNIÃO EUROPEIA

3.1 Aspectos Históricos da GDPR na União Européia

O debate acerca da necessidade de normas, perante os contornos dos novos fenômenos tecnológicos e a intervenção de terceiros e do Estado na vida pessoal dos usuários de tecnologia é destaque das discussões da Comunidade Europeia e da União Europeia, desde meados de 1981, com a aprovação da Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108/CE), que buscou a proteção de indivíduos relativa ao processamento automático de tratamento de dados. Assim como, aspirava estabelecer métodos mais severos e específicos as "garantias relativas à coleta e tratamento de dados pessoais".

Posteriormente, em 1995, com a finalidade de aprimorar à Convenção 108/CE, foi implementada a Diretiva 95/46/CE, a qual estabeleceu diretrizes à proteção de dados pessoais entre os Estados-membros e a criação de um arcabouço de autoridades centrais responsáveis pela fiscalização, legislação e arbitragem em questões envolvendo a proteção de dados pessoais, denominadas autoridades centrais de proteção de dados. Sendo seguida pela Diretiva 2002/58/CE (única ainda em vigor) e a Diretiva 2006/24/CE, concernentes, em síntese, à proteção de dados no contexto das comunicações eletrônicas.

Assim, diante de todo o contexto outrora apresentado, nota-se que o desenvolvimento legislativo europeu foi formado a partir de uma estrutura jurídica fundamental do direito à privacidade e à proteção de dados pessoais. Em que pese "o 'direito à privacidade' (right to privacy) tenha se desenvolvido originalmente na jurisprudência e doutrina norte-americanas"[4], a Europa tem lugar destacado "como a fonte dos principais e mais completos conjuntos de leis sobre proteção de dados pessoais, que emergiram nessas décadas".[5] Pautada nos riscos e oportunidades à realização de direitos e liberdades fundamentais a União Europeia traçou sistematicamente o tratamento e proteção dos dados pessoais.

[4] BYGRAVE, Lee A. Data protection pursuant to the right to privacy in human rights treaties. International Journal of Law and Information Technology, v. 6, n. 3, p. 247-284, 1998

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

Não obstante, apesar de toda regulamentação, o desenvolvimento tecnológico e o crescimento exponencial do uso da internet, incitaram a continuidade e a necessidade de inovação das normas no âmbito europeu. Foi a partir da desvantagem regulatória que materializou-se então o Regulamento 2016/679 do Parlamento Europeu e do Conselho, o Regulamento Geral de Proteção de Dados (GDPR), entrando em vigor em 2018, conceituando dados sensíveis, influenciando inclusive, diretamente a LGPD, que conceituou de forma semelhante, senão idêntica, em sentido e grafia, a referida lei, vejamos: Dados pessoais: "qualquer informação relativa a uma pessoa singular identificada ou identificável" (EC, 95) versus "informação relacionada a pessoa natural identificada ou identificável (BRASIL, 2018).

Além disso em seu artigo 9 (1) e (2), o GDPR estabelece um regime bastante estrito, proibindo, via de regra, o processamento de dado pessoal:

> [...] qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de 39 colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição [...]

Desse modo, nota-se que, apesar da especificidade do método europeu, e de o continente ser destaque de maneira positiva quanto às leis sobre proteção de dados pessoais, com a difusão tecnológica e a expansão do uso da internet, foi preciso atualizar as normas de segurança, com isso surgiu o Regulamento Geral de Proteção de Dados (GDPR).

3.2 Padrões Adotados pela GPDR

A nova regulamentação da UE, foi produzida com variação de níveis. Em um primeiro ponto, abarcado dos artigos 1º ao 11, foram asseguradas as garantias fundamentais amplas e conceitos utilizados em todo o corpo da norma. Tal estrutura concede uma modulação e maior durabilidade à obra, visto que, mesmo com mudanças no campo tecnológico, as normas serão amoldadas a aplicações futuras.

Já no artigo 4º da GDPR, encontra-se definido mais de vinte e cinco termos, dentre eles a definição de dado pessoal, o qual para uma acepção expansionista, não é imprescindível que a capacidade de identificação de um indivíduo seja plena e inequívoca. Assim, também é considerada dado pessoal a unidade informacional que pode de maneira indireta chegar a identificar uma pessoa, seja pela localização de usuário, IDs de dispositivos móveis e até endereço IP. Essa é uma estratégia normativa que parte da premissa de que "dados anônimos são sempre passíveis de reversão".

A coleta de dados sensíveis - aqueles que revelam origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos, dados relativos à saúde ou dados relativos à orientação sexual - é expressamente proibida, nos termos do artigo 9º. A regulação prevê algumas exceções, autorizando a coleta de dados sensíveis para fins de medicina preventiva e ocupacional, para avaliar a capacidade de trabalho do funcionário, diagnóstico médico, prestação de cuidados médicos ou sociais e tratamento ou gestão de sistemas e serviços de saúde, assistência social com base no direito do Estado-Membro ou por força de contrato com um profissional de saúde. Não obstante, o usuário que permitir a coleta de seus dados tem o direito de, a qualquer tempo, proibi-la.

De mais a mais, também é especificado no regulamento o princípio de responsabilidade civil das empresas detentoras de todos os dados que coletam e armazenam. Possuindo como obrigação a reparação de qualquer dano causado aos titulares das informações coletadas e armazenadas em virtude de violação ou vazamento.

Outro elemento inovador é a aplicação de multas administrativas que podem chegar a €20.000.000,00 ou, em se tratando de uma empresa, até 4 % do seu volume de negócios anual em nível mundial correspondente ao exercício financeiro anterior. Neste caso, diversas são as situações previstas no GDPR, como por exemplo, violação de princípios como “privacy by design” 59, não cumprimento das obrigações relacionadas ao processamento ou a não designação de um Responsável pela Proteção de Dados. As multas para esses casos buscam remediar a efetiva ou potencial violação dos direitos estabelecidos nos artigos 8º, 11, 25, 39, 42 e 43 do Regulamento.

A imposição dessas sanções exigirá, por parte dos tribunais, avaliação caso a caso das circunstâncias da infração, sendo considerados fatores como a gravidade e a duração da infração, os atos intencionais ou negligentes, medidas de mitigação de danos que tenham sido implementadas, medidas técnicas e organizacionais e, por fim, o modo como a autoridade supervisora tomou conhecimento dos eventos alegadamente infrativos.

O sistema protetivo da GDPR funda-se, de um lado, na principiologia típica da seara da proteção de dados, frisando a promoção das garantias e prerrogativas individuais implicadas na matéria, e, de outro, em determinações específicas, concretas, regras que visam à cobertura das situações fáticas já verificadas, aptas a manter-se a par do desenvolvimento tecnológico.

3.3 Casos Exemplares de Desanonimização de Dados Sensíveis

Em 2014, na China, o governo chinês anunciou a implementação do sistema de crédito social até 2020. Por meio dele, o governo mapeará as ações públicas, financeiras e virtuais dos cidadãos, classificando em condutas aprovadas ou reprovadas, perante os olhos do Estado, atribuindo pontuação positiva ou negativa para cada pessoa, que servirá para determinar se tal pessoa poderá ou não ter acesso a serviços públicos. Conforme o governo chinês, a política visa priorizar "atos de honestidade" e credibilidade, publicando aqueles que forem considerados reprováveis.

Já em 2016, uma prestadora de serviços de coleta e doação de sangue na Austrália, a *Red Cross Blood Service*, sofreu um duro golpe em seu sistema de segurança de dados, quando informações referentes a 550.000 doadores de sangue vieram a público devido à transferência de um arquivo contendo informações desses doadores a um ambiente computacional não seguro, acessível por pessoas sem a devida autorização para manejar aqueles dados. Os dados se referiam a coletas de sangue realizadas entre os anos de 2010 e 2016. Dentre as informações contidas na base de dados, uma era especialmente sigilosa, qual seja, a que especificava que determinado doador seria "pessoa com comportamento sexual de risco".

Essa categorização era determinada por meio de questionário do tipo "verdadeiro-falso" disponibilizado ao doador no momento da coleta de sangue, em que se perguntava se o mesmo havia participado de atividades sexuais de risco nos últimos 12 meses. Tanto as perguntas realizadas no questionário, como as respostas, compunham a base de dados e estabeleciam a conexão com o doador, individualizado por seu nome e pelas demais informações pessoais. A *Red Cross* pediu desculpas formais aos doadores e disponibilizou todo um aparato de atendimento às pessoas que tiveram seus dados violados.

4 CONSIDERAÇÕES FINAIS

Diante de todo o exposto, podemos inferir que com o avanço tecnológico e do capitalismo, a sociedade iniciou uma organização por meio de redes, fato este que gerou um aumento exponencial de registro de dados, configurando assim o *big data*, o qual permite a análise e a interpretação de grandes volumes de dados, o que consequentemente fez com que os usuários da internet fossem identificados, tornando-se uma forma de controle e vigilância

dos usuários da internet, proporcionando para as empresas detentoras dos dados, a possibilidade de encontrar as estratégias corretas, a partir de padrões comportamentais, que visem a objetivos específicos.

Não à toa, a busca incessante das entidades, sejam públicas ou privadas, de aprimoramento de programas, com a finalidade de categorização e reconhecimento de padrões — *data mining* — em enormes conjuntos de dados — *big data*. Em contrapartida, esta evolução trouxe consigo a preocupação quanto a quais informações estão sendo diariamente disponibilizadas online, direta ou indiretamente, ao utilizar os serviços online, ao mover-se na sociedade da informação.

A lógica necessária ao abordar o tema da LGPD no cenário do *big data*, portanto, é a de que, em que pese sua denominação – "proteção de dados pessoais" – indique um âmbito reduzido e unilateral de estudo, seu objeto resulta numa disciplina abrangente da realidade informacional (DONEDA, 2006). Para além da defesa da privacidade, o que se protege e regula, a partir de suas proposições, é o direito de acesso e o poder de controle a informações pessoais, muitas vezes que tangenciam o caráter individualista de privacidade.

Também, verificou-se que, embora importantes, os mecanismos de controle estatais são incapazes de delimitar e esclarecer a obscuridade do termo "esforços razoáveis" do art. 12 da LGPD comprometendo a proteção de dados quando objeto de tratamento pelo *big data*, face a caracterização como "anônimos".

Conforme visto, os dados anonimizados não recebem status de proteção jurídica, uma vez que, teoricamente, os mesmos não podem ser identificados salvo quando possível sua reversão e a identificação de técnicas razoáveis e disponíveis ao tempo do seu tratamento, que ensejem a desconsideração do anonimato como dado pessoal, levando em conta a razoabilidade.

Com a LGPD, surge o problema de etiquetação de permissões e proibições, para a utilização de determinadas informações/dados, gerando riscos objetivos de criar novas lacunas. Entretanto, para sanar a obscuridade contida no termo "esforços razoáveis", buscou-se inspiração na experiência europeia, que emitiu um parecer 05/2014 sobre técnicas de anonimização, segunda o qual não são considerados anônimos os dados que permitam a individualização do usuário.

Assim, espera-se que a ANPD - Autoridade Nacional de Proteção de Dados, no

exercício de sua competência de editar normas sobre privacidade e proteção de dados, manifeste-se prontamente, considerando a sensibilidade da questão, para que seja sanada a omissão da norma em delimitar o necessário.

Outrossim, caberá as empresas integrar em toda sua cadeia de produção e administração princípios éticos, adaptação de suas tecnologias e a seguridade de seus dados, além de treinamento de seus colaboradores e estabeleçam uma relação de transparência em seu trabalho. Além do esforço que será necessário ser empreendido pela doutrina e jurisprudência, para, agora, favorecer e intensificar a interpretação dos dispositivos contidos na LGPD, para que as normas não se tornem antigas tão logo deixem de ser futuras.

REFERÊNCIAS

BIONI, B. R. MONTEIRO, A. L.; GOMES, M. C. O. **GDPR matchup: Brazil's General Data Protection Law**. 2018. Disponível em: < https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/>. Acesso em: 16 out. 2020.

BIONI, B. R. **Proteção de Dados Pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BIONI, Bruno Ricardo, **Xeque-mate**: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. [S.I.: s.n.], 2016. Disponível em: https://www.researchgate.net/publication/328266374_Xeque-Mate_o_tripe_de_protecao_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil. Acesso em: 09 nov. 2020.

BRASIL. **LEI 13.709/18 ARTIGO 44º, V - Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.html>. Acesso em: 20 set. 2020.

BRASIL. **LEI 13.709/18 ARTIGO 5º, II - Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.html>. Acesso em: 20 set. 2020.

BRASIL. **LEI 13.709/18 ARTIGO 5º, III - Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.html. Acesso em: 20 set. 2020.

BYGRAVE, Lee A. Data protection pursuant to the right to privacy in human rights treaties. **International Journal of Law and Information Technology**, v. 6, n. 3, 1998.

CONSELHO EUROPEU. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. Estrasburgo, 1981. Disponível em: < https://rm.coe.int/1680078b37>. Acesso em: 02 set. 2020.

DONEDA, D. **A proteção dos dados pessoais como um direito fundamental**. EJJL-Espaço Jurídico: Journal of Law, v. 12, n. 2, Rio de Janeiro, 2011.

GRUPO DE TRABALHO PARA A PROTEÇÃO DAS PESSOAS NO QUE DIZ RESPEITO AO TRATAMENTO DE DADOS PESSOAIS. **Parecer 05/2014 sobre técnicas de anonimização,** 10 de abril de 2014. Disponível em: https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831045040634.pdf. Acesso em 15 nov. 2020.

GUIDI, G. B. C. **Modelos Regulatórios para Proteção de Dados Pessoais**. in: BRANCO, Sérgio; TEFFÉ, Chiara de Teffé (Org.). **Privacidade em perspectivas**. 1. ed. Rio de Janeiro: Lumen Juris, 2018.

MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. **Big data: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana.** Tradução Paulo Polzonoff Junior. Rio de Janeiro: Elsevier, 2013.

MOREY, T. FORBATH, T. SCHOOP, **A. Dados dos consumidores: modelos de transparência e confiança.** Harvard Business Review Brasil, São Paulo, fevereiro 2016.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust De-anonymization of Large Sparse Datasets. In: **Proceedings of the 2008 IEEE Symposium on Security and Privacy**, 2008, Washington: IEEE Computer Society. 2008.

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