DIREITO:

Diálogos e pesquisas sobre temas contemporâneos

Roger Goulart Mello
Organizador

Publicar Editora

2022

DOI 10.47402/ed.ep.c2022162721894

CAPÍTULO 21

TRATAMENTO DE INFORMAÇÕES PESSOAIS: ANÁLISE DO LIMITE LEGAL PARA O USO DE DADOS PESSOAIS PELAS INSTITUIÇÕES PRIVADAS

Rodrigo Lira

RESUMO

Dados pessoais são considerados o novo petróleo na sociedade da informação, havendo uma busca incessante pela obtenção dessas informações almejando um maior grau de assertividade na relação empresa-usuário. O objetivo deste estudo foi realizar uma análise sobre o tratamento de dados no Brasil, com base em leis nacionais e a lei europeia, em que os parâmetros analisados foram: aplicabilidade, validade e eficácia da Lei Geral de Proteção de Dados (LGPD); fatos geradores da norma; tratamento de dados de crianças e adolescentes; direitos dos usuários e titulares das informações e limites legais para a coleta por parte de instituições privadas. Destarte, os resultados demonstram que muitas lacunas legais surgem com a nova conjuntura social pondo em risco as informações pessoais e, consequentemente, a privacidade, devido ao grande fluxo de dados, carecendo de regulamentação para serem solucionados. Conclui-se, portanto, que as novas legislações no Brasil, e no restante do mundo, trazem benefícios e segurança para os titulares observando que, até então, dados eram tratados de acordo com a vontade das instituições privadas.

PALAVRAS-CHAVE: Tratamento. Dados pessoais. Lei geral de proteção de dados. Instituições privadas. Limite legal.

INTRODUÇÃO

O desenvolvimento tecnológico das últimas décadas possibilitou a produção de uma quantidade de dados maior que em toda a história da humanidade, repercutindo consequências positivas e negativas. Destaca-se como positivo, o acesso à informação a qualquer momento, alta conectividade e uma socialização a nível global. Em relação às consequências negativas, há uma exposição extrema dos usuários das ferramentas tecnológicas em relação aos fornecedores desses serviços, ao ponto de conseguirem uma análise de informações tão particular que envolva as pessoas em verdadeiras bolhas de conteúdos relacionado ao que elas buscaram recentemente em qualquer espaço online, bem como principalmente riscos à sua privacidade.

Assim, essa grande quantidade de produção de informações, que após o tratamento tornam-se dados, resultou o movimento chamado *Data for Good*, em tradução literal “Dados para o bem”, que visa a utilização desses dados para otimizar ações de impacto social, ou seja, iniciativas apoiadas na análise de dados para trazer algum benefício à sociedade.

Entretanto, não é isso que ocorre quando se trata da maior parte das empresas privadas e a utilização das informações dos indivíduos que as fornecem por diversas razões. Hoje as informações pessoais são as engrenagens que movimentam quase todas as atividades econômicas, e nessa nova conjuntura surge o termo *data-driven-economy*, significando que a economia se move a dados, contudo, não se limita somente a questões financeiras, repercutindo também nas relações sociais, políticas e individuais do cidadão (MENEZES *et. al*, 2018).

Essa relação entre usuários/consumidores com ferramentas e serviços digitais, por ser muito recente, trouxe muitas lacunas legais, deixando o lado mais frágil dessa relação totalmente sem controle de como as instituições coletam, armazenam e tratam informações pessoais para terem mais eficácia em suas ações de marketing ou no processo de aprimoramento da ferramenta, por exemplo.

O Brasil, até 2018, não possuía nenhuma lei que abordasse de forma ampla o tratamento de informações pessoais, havia somente o Habeas Data (9.507/97), que permite o cidadão solicitar, ratificar e complementar informações e, em 2014, a Lei do Marco Civil da Internet (Lei nº 12.965), Lei de Acesso à Informação (Lei nº 12.527/11), além de menções gerais na Constituição Federal, até que surgiu a Lei de Proteção Geral de Dados (Lei nº 13.709/18), que entrou em vigor em 2020 (MACHADO, 2018).

Diante dessas considerações, esta pesquisa, organizada na forma de um estudo bibliográfico e abordagem qualitativa, objetiva analisar os limites e a eficácia das leis que versam sobre o tratamento de informações pessoais no Brasil, distinguir até onde a utilização dessas informações podem ser consideradas aceitáveis ou abusivas, através da identificação das leis que abordam o tema no País, descrever como as organizações captam essas informações, discutir como excesso de acesso a informações impacta a vida do usuário de forma positiva e negativa e relatar casos que comprovem a vulnerabilidade da intimidade e privacidade dos cidadãos.

REGULAMENTO GERAL DA PROTEÇÃO DE DADOS (RGPD) - 2016/679

O Parlamento Europeu, impulsionado pelos escândalos de espionagem dos Estados Unidos revelados em pelo ex-funcionário da *Central Intelligence Agency* (CIA), Edward Snowden, que compartilhavam dados coletados sem permissão de outros países com países parceiros, discutiu durante quatro anos novo regulamento de privacidade digital que revoga a Diretiva 95/46/EC de 1995 (MACHADO, 2018; BIONI; MENDES, 2018).

A Lei foi aprovada no dia 15 de Abril de 2016, com um período de *vacatio legis* de dois anos para que os países membros da União Europeia (UE) adequassem ao novo contexto nacional, entrando em vigência dia 25 de maio de 2018 o Regulamento Geral de Proteção de Dados - RGPD (UNIÃO EUROPEIA, 2018).

Utilizando quatro direitos básicos como o direito de portabilidade, direito de acesso, direito ao esquecimento e direito de retificação, o Regulamento busca promover ao cidadão da UE um controle maior sobre seus dados, além de restringir como as instituições privadas podem tratar e lidar com os dados, sendo aplicável a qualquer empresa que fizer tratamento das informações dos cidadãos europeus, independente se a empresa está localizada fora do bloco europeu, não se restringindo somente aos 28 países-membros da UE.

Algumas diretrizes que a surgem ou foram atualizadas são as seguintes: os usuários podem ver, corrigir ou até deletar as informações que empresas guardam sobre eles; as empresas devem coletar apenas dados necessários para que seus serviços funcionem; a coleta e uso de dados pessoais só podem ser feitas com consentimento explícito; qualquer serviço conectado tem de conceder direito ao esquecimento; informações de crianças ganham proteção especial; clientes que tiverem dados hackeados deverão ser obrigatoriamente avisados em até 72 horas; empresas devem informar com linguagem de fácil acesso sua política de proteção de dados; dados de europeus podem ser transferidos só para países com lei de proteção de dados equivalente à europeia, os considerados "porto seguro" (UNIÃO EUROPEIA, 2016).

Este último ponto, revela a importância de o Brasil possuir a Lei Geral de Proteção de Dados (LGPD) e de outros países possuírem normas que versam sobre a matéria, pois poderá ajudar na relação com países da UE, já que os dados estão se tornando o principal produto da sociedade contemporânea, e no desenvolvimento principalmente no setor de Tecnologia da Informação, e se for considerado "porto seguro", não necessita seguir a norma europeia, dando autonomia no que refere-se ao tratamento de informações.

> O país ou bloco econômico que não incorporasse tais padrões internacionais poderia ser penalizado com sua não inclusão no mapa global do livre fluxo de dado. Nesse sentido, a emergência de leis nacionais e regionais vieram em sua grande maioria, acompanhados de regras duras sobre transferência internacional, o que, em princípio, somente seria possível se o país destinatário tivesse um nível equivalente de proteção (BIONI; MENDES, 2018, p. 801).

Portanto, com as regras do Regulamento Geral de Proteção de Dados, empresas deverão ter cuidado além dos seus processos de tratamento, como também em casos que contratem serviços relacionados às informações, pois serão responsabilizadas pelo não cumprimento das

normas por parte dessas empresas contratadas, ressaltando que em situações de descumprimento será punido com multa de € 20 milhões ou 4% do lucro global da empresa infratora, de acordo com o art. 83 do Regulamento nº 679 de 27 de abril de 2016 (UNIÃO EUROPEIA, 2016).

LEI GERAL DE PROTEÇÃO DE DADOS (13.709/18) E A DEFINIÇÃO DE DADOS PESSOAIS E OS LIMITES LEGAIS SOBRE A COLETA DAS INFORMAÇÕES

Seguindo a tendência mundial iniciada com a entrada em vigor do Regulamento da União Europeia, o Brasil promulgou sua lei sobre proteção de dados pessoais. A Lei 13.709 de 2018 foi o resultado da união de Projetos de Leis (PL) já em discussão sobre a matéria de tratamento de dados, entre eles, o PL 4060/2012 apresentada na Câmara dos Deputados e o PL 5276/2016 de autoria do Poder Executivo após um debate público online promovido pelo Ministério da Justiça, que gerou um anteprojeto chegando a ser enviado pela presidente da época em caráter de urgência ao Congresso Nacional que o recebeu como PL 5276/16 (MACHADO, 2018).

Retirando o projeto do regime de urgência, foi apensado ao PL 4060/12, tramitando normalmente nas casas do Congresso sendo aprovado no Senado e sancionada pelo então Presidente interino da República como Lei Geral de Proteção de Dados, em 14 de Agosto de 2018 e publicado no Diário oficial dia 15 de Agosto do mesmo ano (CÂMARA DOS DEPUTADOS, 2012).

Contudo, só entrou em vigor no início de 2020 em razão dos 18 meses de *vacatio legis*, expresso no art. 65 da própria Lei, para que as instituições públicas, privadas e os civis se preparem para a regulamentação até então inexistente.

As questões e problemas que circundam a exploração de dados ultrapassa a violação da privacidade, observando outras consequências à personalidade percebe-se o risco promovido pela economia movida a dados como o perigo de conceitos como a individualidade e autonomia desaparecerem, pois hodierna está claro que os controladores não buscam tratar as informações dos indivíduos de forma justa, mas sim, otimizar seus lucros e assertividade nas decisões da instituição (FRAZÃO, 2018).

Segundo o artigo 5º, inciso IV da LGPD, a definição de controlador é pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Destarte, nos artigos iniciais há o cuidado de abordar sobre seus princípios e propósitos, como no artigo 2º cita fundamentos de respeito a privacidade; inviolabilidade da intimidade, honra e imagem; livre desenvolvimento da personalidade. E no artigo 6º, princípios da segurança; da transparência; da qualidade de dados, entre tantos outros. Dessa maneira, o objetivo da LGPD é conferir aos cidadãos brasileiros proteção e regulação aos diversos momentos afetados pelo tratamento de informações citada no artigo 5º, inciso X, LGPD.

> Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018).

Portanto, a referida lei almeja a proteção dos direitos fundamentais de liberdade como garantir o direito à privacidade e proteção de dados pessoais, que de acordo com o art. 5º, I da LGPD, significa qualquer informação que torna possível identificar uma pessoa natural, dos cidadãos ao permitir um maior controle sobre o uso de suas informações através de práticas transparentes e seguras estabelecendo regras claras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais para as instituições públicas e privadas impedindo que se reduza a meramente ao conceito de patrimônio com o intuito de promover o desenvolvimento econômico e tecnológico numa sociedade na qual os dados se tornaram o principal produto motriz. Portanto, busca aumentar a confiança da sociedade na coleta e uso dos seus dados pessoais e consequentemente a segurança jurídica no que refere-se ao tratamento de dados (MENEZES; COLAÇO, 2018).

A legislação unifica as regras de forma harmônica sobre o uso de dados pessoais, independente do setor da economia, além de versar sobre a proteção das informações de crianças, adolescentes e idosos. Observa-se, então, uma inclusão digital com educação, ou seja, a regulamentação também vai servir como meio de educar toda uma sociedade que estava desamparada legalmente e culturalmente já que trata de uma situação tão recente.

Adequando o Brasil juridicamente nessa nova conjuntura social o torna apto a tratar dados oriundos de outros países o que pode ajudar a desenvolver setores de tecnologia da informação, por exemplo, além de proteger a pessoa humana da maciça extração de seus dados.

A sociedade da informação possibilita a indução ao fornecimento de informações para que possamos interagir, utilizar algum serviço ou somente concluir uma simples pesquisa é a regra, as chances de acessar aplicativos ou sites e não deixar uma digital é impossível, tornando os dados a contrapartida do amplo acesso à informação.

Perfis de personalidade que permitem classificar e discriminar os indivíduos consoante seus hábitos, características biológicas, preferências e convicções, em flagrante ameaça não só a privacidade, mas também, a própria dignidade humana (CUEVA, 2017, p. 59-67).

A Lei em análise, trata sobre uma temática muito recente, trazendo em seu texto muitos termos pouco discutido, pelo menos no âmbito geral da sociedade, portanto houve a necessidade de defini-los no artigo 5º, da LGPD.

Sendo assim, neste tópico, haverá uma breve explicação sobre o que são esses tão almejados dados, e para isso nota-se a divisão do termo em três grupos e para cada um deles uma definição. O primeiro conceito é sobre os dados pessoais, definidos como "qualquer informação relacionada à pessoa natural identificada ou identificável" (art.5º,I, da LGPD); a segunda explicação é sobre dados pessoais sensíveis que são 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, da LGPD); e, por último, a definição de dados anonimizados, relativo a "titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (art.5º, III da LGPD).

Porém, dados pessoais que tenham sido tornados anônimos e a pessoa não seja ou deixe de ser identificável deixam de ser considerados dados pessoais. Para que os dados sejam anonimizados a anonimização tem de ser irreversível.

Sobre a coleta, é necessário esclarecer que está englobada dentro da definição do termo tratamento cuja sua definição legal já foi exposta anteriormente, e deve respeitar o alicerce legal no art. 7º, da LGPD. Por conseguinte, vale ressaltar que a Lei 13.709/18 é relacionada à pessoa natural, ou seja, se uma empresa trata/coleta dados sobre preço de mercadorias, a lei não se aplica a esta pessoa jurídica. Todavia, as hipóteses e requisitos relacionados ao tratamento e coleta de dados pessoais são expostas no artigo 7º e 8º da LGPD, possuindo no primeiro um rol taxativo. Amplia ao art. 11, da LGPD, o processamento dos dados sensíveis, apesar de serem iguais ao dos dois artigos supra referidos (BRASIL, 2018).

Alguns dos requisitos fixos para a etapa do tratamento coleta são: mediante o fornecimento de consentimento escrito ou por outro meio que demonstre a manifestação de vontade do titular, portanto, se o titular autorizar a coleta e uso de seus dados a empresa poderá utilizá-los; coleta de dados quando há obrigação legal ou regulatória do controlador de dados, por exemplo, companhias de transporte que há necessidade de coletar as informações de seus

passageiros, apesar de não desobrigar o controlador as outras obrigações previstas em lei, como desviar a finalidade da coleta; para realização de estudos por órgão de pesquisa, garantindo a anonimização quando possível; quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados, de acordo com o art. 7º da Lei nº 13.709, 14 de agosto de 2018 (BRASIL, 2018).

Sobre esta última hipótese apresentada, um exemplo para esclarecer é uma companhia aérea que mantém banco de dados dos passageiros, necessita dos dados para emissão de nota fiscal, mudança de passagem ou entrar em contato em situações de imprevistos, nesses casos não é necessário solicitar permissão para o processamento desses dados. Mas, se a companhia quiser enviar propagandas ou avisos por e-mail, aplicativos ou outro veículo de comunicação, deverá comunicar o titular e solicitar autorização, pois a finalidade do tratamento dos dados foi alterada.

Contudo, observa-se no inciso IX do art. 7º da LGPD um termo obscuro, o "legítimo interesse do controlador ou de terceiro". A expressão termina dando margem para interpretações e brechas de possíveis justificativas quando houver algum equívoco por parte da instituição privada e, para sanar, certamente precisará da ajuda dos tribunais. Mas, apesar da obscuridade do termo, a própria lei no art. 10, apresenta balizas para o controlador impetrar seu interesse.

A NÃO APLICABILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados, surge no intuito de tutelar os dados da pessoa natural dos abusos cometidos pelas empresas e mercado de consumo, pois, com tamanha conectividade, as instituições privadas passaram a ter acesso às informações mais íntimas e a processá-las como queriam. Portanto, a LGPD trata da regulação do fluxo dessas informações entre pessoas jurídicas, independente da complexidade do banco de dados, aplicável tanto os que são automatizados como para os que ainda são manuais. Não obstante, a norma traz situações que excepciona sua aplicação, pois apesar de haver coleta de dados, não há um viés mercadológico e não põe, *a priori*, risco à privacidade do indivíduo (MENEZES; COLAÇO, 2018).

Expresso no art. 4º da LGPD apresenta situações como manipulação de dados realizados por pessoa natural sem fins econômicos, pois a comunicação humana não ocorre sem a troca de informações, e se essa comunicação se apresenta no aspecto pessoal. Quando se conhece alguém é comum trocar e-mail, nome, endereço, chegando muitas vezes nos considerados dados

sensíveis como orientação sexual e religiosa, apesar disso, não será necessário a aplicação da lei, o que poderia estender bastante sua aplicação e complexidade, podendo interferir em situações muito íntimas entrando em contradição com sua finalidade. Mas, se fizer uso indevido dessas informações, poderá acarretar em danos morais e ilícito penal (MENEZES; COLAÇO, 2018).

O processamento de dados para fins jornalísticos, também está dentro da exceção de aplicabilidade direta da norma, já que considera-se uma instituição que busca o debate, a liberdade de expressão e a transmissão da verdade, e por isso, não poderia haver algum tipo de censura ou limitação para atuação desses profissionais, entretanto, exige-se uma atividade verdadeira, sem inclinações pessoais ou ideológicas, mantendo sempre a idoneidade da informação transmitida. Um exemplo são os jornalistas esportivos, que preparam matérias sobre os atletas, abrangendo o desempenho e suas características físicas, como número de chutes a gols, quantidade de gols marcados por determinado atleta, idade, altura, peso, distância percorrida no campo. Ainda que informações como estas sejam consideradas dados pessoais e as conclusões obtidas pelo jornalista sejam resultado de tratamento, não há necessidade de aplicação da LGPD, pois a finalidade é somente informativa.

Porém, se um portal de notícias analisa seus visitantes e desenvolve padrão de consumo, tempo médio de permanência online, tipo de conteúdo pesquisa, essas informações passam a possuir alto valor e importância de mercado, pois podem direcionar as empresas ao que apresentarem online para aquela pessoa. Sendo assim, situações como esta, mesmo estando relacionada ao jornalismo, devem se submeter às normas da LGPD.

O tratamento para fins acadêmicos também está excluído da regulamentação, tendo sua autonomia para o desenvolvimento de conhecimento, pesquisas e manifestação de pensamento assegurada pela Constituição Federal, segundo o art. 218, CF/88. Apesar de ficar de fora da aplicação dessa norma, o controle e a fiscalização no ambiente acadêmico ocorre pelos comitês de ética, sem a necessidade de uma matéria especial para controle de pesquisas (BRASIL, 1988).

TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES SEGUNDO A LEI GERAL DE PROTEÇÃO DE DADOS

Uma das novidades que a LGPD trouxe foi a preocupação com as informações das crianças e adolescentes, através de dispositivos para resguardar esses dados e com o auxílio dos pais o país busca conseguir tratar de forma mais responsável esse tipo de informação já que

desde muito jovens possuem uma independência tecnológica. Segundo a Lei nº 8.069/90, o Estatuto da Criança e do Adolescente (ECA), define que criança pessoa de até 12 anos de idade incompletos e adolescente, aquela entre 12 e 18 anos, para isso, no art. 14 da LGPD traz o regulamento de como e quando as empresas poderão ter acesso aos dados destes (BRASIL, 2018).

Sendo assim, os pontos primordiais são o consentimento do responsável, pois os menores 16 anos são civilmente incapazes e a partir dos 16 até os 18 anos são relativamente incapazes em alguns atos da vida civil de acordo com o código civil (10.406/2002), e o termo "em seu melhor interesse", que deve ser observado como premissa básica de qualquer ação que visa a proteção desse público. Ou seja, qualquer orientação ou decisão envolvendo tais sujeitos deve levar em conta o que é melhor e mais adequado para a satisfação dos seus anseios, podendo sobrepor, inclusive, aos interesses dos pais. São esses dois raciocínios que irão reger o tratamento de dados dos menores (BRASIL, 2018).

Nessa questão do consentimento surge um problema, que é como o controlador irá identificar que o consentimento realmente foi dos responsáveis? Para isso, a legislação impõe que as empresas mantenham as informações pública sobre os tipos de dados coletados, a forma de utilização e os procedimentos, para o exercício dos direitos previstos no artigo 18 da LGPD, que traz um rol de direitos do titular de dados, ou no caso, do responsável pelo titular, além de estabelecer que o controlador deverá utilizar todos os meios tecnológicos disponíveis para confirmar que quem forneceu a autorização foi o responsável. Um exemplo dessa tecnologia que pode ser usada são como as *Fintechs* que solicitam uma foto com a identidade para comprovar que é realmente a pessoa que está solicitando o cartão ou a abertura de conta.

Todavia, no Direito sempre há exceções e na referida lei não seria diferente. As empresas/controlador poderão coletar dados pessoais de crianças sem o consentimento quando a coleta for necessária para contatar os pais ou o responsável legal ou para sua proteção, entretanto só poderão ser utilizados uma única vez, sem armazenamento e veda de forma absoluta o repasse a terceiro sem consentimento (BRASIL, 2018).

No parágrafo 4º da LGPD, traz um ponto muito importante no que se refere a crianças e adolescentes, que as empresas não deverão condicionar a participação das crianças em jogos, aplicações de internet ou outras atividades ao fornecimento de dados pessoais, além das que sejam estritamente necessárias à atividade. Não obstante, quais informações seriam estritamente necessárias para um jogo? E quais outras atividades são essas? Se estiver referindo

a *Facebook*, *Twitter*, *Instagram*, *Spotify*, se torna ainda mais complexo definir quais dados são necessários, já que são empresas como estas que traçam perfis completos de seus usuários, desde os locais que frequentam até perfil de compra. Mais um ponto na Lei que precisará do auxílio das pacificações dos tribunais.

Por fim, para que a criança e o adolescente junto com seus pais ou responsáveis deem a autorização tão almejada pelos controladores, as informações sobre o tratamento deve está de forma clara e simples, levando em consideração que hoje ninguém lê aqueles textos imensos com letras minúsculas, portanto, o que a lei visa é transparência e cuidado com esse grupo especial de titulares de dados.

DIREITOS DOS TITULARES DOS DADOS PESSOAIS

A nova Lei, apesar de versar sobre tantos deveres para os controladores também traz direitos aos donos dessas informações, destarte, dedica o capítulo III da LGPD para abordar que direitos são esses. Ressalta-se que no decorrer da Lei pode ser observado uma série desses direitos.

O *start* desses direitos é a requisição, portanto, a partir da solicitação por parte do titular a empresa acionada deverá permitir o acesso à confirmação da existência de tratamento e, por consequência, acesso a todos seus dados pessoais que estão sendo coletados e tratados. Nesse momento, se o titular observar algum erro, há possibilidade de retificação de informações incompletas, equivocadas e desatualizadas e se preferir, excluir, cancelar ou revogar seu consentimento para o processo de tratamento de suas informações (BRASIL, 2018).

Direito a oposição, ou seja, o dono tem o direito de se opor a quaisquer tratamentos e informações que não estejam em conformidade com a lei, assim como as decisões automatizadas que afetem seus interesses, como decisões destinadas a definir seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade, e o direito a explicação, no qual, titular dos dados tem direito a receber informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados pelo controlador para a tomada de decisão com base em tratamento automatizado de dados pessoais e também o direito à portabilidade, que consiste na possibilidade de transferência das informações para outro controlador, independente das razões, bastando somente o titular desejar.

Sendo assim, nota que a Lei tenta transformar os processos originados no consentimento o mais transparente possível, possibilitando a qualquer momento acessos, correções e exclusão

caso seja desejo do titular. Entretanto, há necessidade de uma fiscalização por conta do indivíduo do que está sendo feito com seus dados a partir do fornecimento.

DO TÉRMINO DO TRATAMENTO DE DADOS DE ACORDO COM A LEI GERAL DE PROTEÇÃO DE DADOS

O tratamento de dados pessoais, independente de serem sensíveis ou não, não é um processo que ocorre para sempre, havendo um início que ocorre no momento do consentimento, o meio que são os momentos de classificação, utilização, acesso, reprodução, transmissão, distribuição e um fim, abordado no art. 15 e 16 da LGPD (BRASIL, 2018).

A importância de se ter previsão legal para o fim desse tratamento, é para que as informações dos cidadãos não fiquem sob posse dos controladores *ad eternum,* estando sujeitas a vazamentos ou comercialização sem consentimento. Versar sobre hipóteses de término, coaduna com o princípio gerador da norma que põe os dados pessoais na tutela de terceiros para um fim específico e, após essa finalidade ser atingida, há o término do tratamento.

Outra hipótese trazida na regulamentação é através do consentimento por prazo determinado, que terminando o prazo, o terceiro possuidor das informações é obrigado a excluir tudo que possuir do titular. Se desejar prosseguir com o tratamento, há necessidade de um novo pedido de consentimento. Ficando claro o protagonismo do titular, a Lei prevê que basta uma solicitação do mesmo para o fim do trabalho com seus dados, salvo se houver interesse público nos trâmites em relação a essas informações (BRASIL, 2018).

Por fim, se a empresa estiver tratando de forma ilegal, certamente, necessitará finalizar o processo e pagará uma multa aplicada pela Agência Nacional Reguladora, que ainda será definida e criada, pois teve seus artigos de criação revogados na LGPD. De forma geral, o término de tratamento se dá com a exclusão das informações pessoais.

FACEBOOK E *CAMBRIDGE ANALYTICA* VIOLAM ACESSO A DADOS PESSOAIS

Um dos casos mais famosos sobre desvio de finalidade da utilização de informações pessoais, a empresa de marketing político *Cambridge Analytica* utilizou um teste de personalidade gratuito na rede social *Facebook* em 2014 para obter cerca de 50 milhões de perfis psicográficos dos usuários sem permissão para serem utilizados em campanhas pró *Donald Trump* e pró *Brexit*. (MENEZES; COLAÇO, 2018).

As informações foram coletadas através de um aplicativo chamado *this is your digital life* criado pelo Aleksandr Kogan, na qual, os usuários que concordavam com os termos e

condições do teste acreditavam estar fornecendo suas informações para uso acadêmico. Entretanto, além de coletar os dados dos participantes do teste, coletavam também dos amigos na rede social, o *Facebook* permitia essa coleta de terceiros apenas para melhorar a experiência do usuário, desta forma alcançou a quantidade de mais de 80 milhões de dados pessoais que seriam usados para direcionar os anúncios políticos para as pessoas com mais chances de serem impactadas com a propaganda (THE GREAT Hacker. Produção: Karim Amer, Pedro Kos, Geralyn Dreyfous, Judy Korin. NETFLIX, 2019. Documentário. Duração, 2h 19min).

Após o escândalo ser revelado pelo ex-funcionário da consultora política, o *Christopher Wylie,* ambas as empresas foram julgadas e condenadas. O *Facebook* foi condenado a pagar US$ 5 bilhões mais ajustes em suas políticas de tratamento de dados como aplicativos sem uso por mais de três meses perderão, automaticamente, acesso ao *Facebook*, aplicativos que solicitam informações do *Facebook* para fazer login somente poderão acessar nome, fotografia de perfil e endereço de e-mail. Porém, a *Cambridge Analytica*, declarou insolvência, quando uma empresa é incapaz de arcar com suas dívidas, no Reino Unido, e pediu falência em algumas das afiliadas dos Estados Unidos (THE GREAT Hacker. Produção: Karim Amer, Pedro Kos, Geralyn Dreyfous, Judy Korin. NETFLIX, 2019. Documentário. Duração, 2h 19min).

DECOLAR.COM OFERTA PREÇOS E VAGAS BASEADO NA ANÁLISE DOS DADOS DE LOCALIZAÇÃO

Decolar.com, empresa de *e-commerce* de passagens aéreas e pacotes turísticos, é a filial brasileira da empresa argentina Despegar, maior Agência de Viagens da América Latina. O nome "Decolar" é a tradução literal da palavra "despegar", em espanhol, que é o movimento de uma aeronave alçar voo.

Contudo, no dia 25 de Janeiro de 2018, foi ajuizada uma ação contra a empresa pelas práticas de *geo-blocking* e de *geo-pricing*: o bloqueio da oferta e a precificação diferenciada de produtos com base na geolocalização do consumidor. A conduta da Decolar.com viola dispositivos do Código de Defesa do Consumidor, em especial o artigo 6º, III relativo à informação clara sobre os produtos e serviços, que é subtraída dos usuários, de forma incompatível com a boa-fé objetiva. Tratando-se de discriminação em virtude da localização geográfica dos consumidores, que, mediante manipulação de informações, infringe ainda o Marco Civil da Internet, que prevê a neutralidade da rede e aos princípios e normas da LGPD exposto nos capítulos anteriores, contudo esta ainda não está vigorando.

A empresa foi condenada com multa de 7,5 milhões de reais, de acordo com a nota técnica Nota Técnica n.º 92/2018/SP do processo nº 08012.002116/2016-21 do Ministério da Justiça (BRASIL, 2018).

MOVIMENTO *DATA FOR GOOD* - TRATAMENTO DE DADOS PARA O BEM COMUM

Criado por cientistas de dados dos Estados Unidos, o movimento é uma convocação para que empresas privadas, terceiro setor e governos possam se apropriar de dados disponíveis e usá-los, de forma ética e responsável, para causar impacto social e enfrentar os principais desafios da humanidade. Segundo Yuval Harari, autor do *best-seller* 21 lições para o século 21, diz que quem possuir grande quantidade de dados, serão os donos do futuro (HARARI, 2018).

Portanto, a mesma revolução social, tecnológica e mercadológica e que está fazendo surgir empresas que querem a todo custo acesso aos dados pessoais para terem o novo petróleo sob seu domínio, há também movimentos que buscam utilizar o tratamento dessas informações para um desenvolvimento benéfico, transparente e sustentável da sociedade.

O movimento *data for good* é regido pelo conceito e princípio de utilização dos diversos dados que o usuário deixa enquanto navega online, destarte, é um movimento intersensorial, ou seja, com vários perfis acadêmico, profissionais e sociais, com o intuito de orientar ações sociais por evidência de dados. Iniciativas *Data for Good* são eventos, hackathons, projetos, comunidades ou plataformas que visam aliar Big Data a impacto socioambiental positivo. Sendo assim, ser visto como uma alternativa a se trabalhar com um fluxo tão grande de informações, pois, em detrimento de utilizá-los somente para um consumo excessivo decorrente da sociedade capitalista, valer-se da nova conjuntura social, a da informação, para buscar iniciativas que tentem solucionar problemas e como consequência terem lucro (TIMMS; HEIMANS, 2019).

Já há algumas ações sendo implementadas tanto no Brasil como ao redor do mundo. O Mapa de Desastres do *Facebook* mostram onde estão localizadas as populações afetadas por desastres e como estão se movendo. Todos os dados são desidentificados, ou seja, não se conectam ao nome de uma pessoa ou a qualquer outra informação de identificação para proteger a privacidade individual. Após um desastre, o Mapa de Desastres compartilha informações em tempo real com as equipes de resposta, ajudando-as a determinar coisas como se as comunidades têm acesso a redes de energia e celular, se foram evacuadas e quais serviços e suprimentos eles mais precisam.

No Brasil, há o projeto Serenata de Amor, um projeto de tecnologia que usa inteligência artificial para auditar contas públicas e auxiliar no controle social. A ideia surgiu do cientista de dados Irio Musskopf, como forma de participar ativamente do processo democrático, fiscalizando os gastos públicos. Focada em fiscalizar, com auxílio de tecnologia, os reembolsos efetuados pela Cota para Exercício da Atividade Parlamentar (CEAP) – verba que custeia alimentação, transporte, hospedagem e até despesas com cultura e assinaturas de TV dos parlamentares.

CONSIDERAÇÕES FINAIS

Com base no que foi apresentado, possibilitou uma análise de como ocorreu todo o processo de desenvolvimento da busca pela proteção dos dados, desde alguns fatos geradores como escândalos por falta de responsabilidade de grandes empresas com as informações pessoais até a criação das primeiras leis específicas, como o Regulamento Geral de Proteção de Dados (RGPD), da União Europeia, e a Lei Geral de Tratamento de Dados (LGPD), do Brasil. Além disso, também permitiu uma pesquisa para obter informações mais consistentes sobre as etapas do tratamento de dados dentro do território nacional, por parte dos controladores, definidas dentro do limite de atuação trazidos pela nova lei.

Por conseguinte, conclui-se, que as instituições privadas fazem uso de dados para traçar perfis e padrões com o máximo de detalhes e personalizar a navegação do usuário na internet, transformando assim os dados no produto mais valioso de uma sociedade consumista e ultra conectada; a sensibilidade dos dados e a falta de leis e fiscalização eficaz está pondo fim ao conceito de privacidade; a falta de transparência no tratamento de informações pessoais deixa o usuário refém de aplicativos, sites e rede sociais.

Dessa maneira, a legislação exposta anteriormente acarretará em soluções legais para essas situações que põe o usuário em risco. Mesmo assim, ainda há um caminho árduo a ser percorrido no que refere-se a dados, pois apesar de a lei ter entrando em vigor em um momento de pleno crescimento desse formato mercadológico, as mudanças no mundo digital ocorrem de forma abrupta, que fez gerar mais dados nas últimas décadas que em toda a história da humanidade.

REFERÊNCIAS

BRASIL. **Código civil brasileiro de 2002**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 25 set. 2019.

_____. **Constituição da república federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 18 set. 2019.

_____. **Estatuto da criança e do adolescente.** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 25 set. 2019.

_____. Ministério da Justiça. Secretaria Nacional do Consumidor. **Nota técnica nº 92/2018**/CSA-SENACON/CGCTSA/GAB-DPDC/DPDC/SENACON/MJ/SP. São Paulo: Ministério da Justiça, 18/06/2018. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/cao_consumidor/SENACON/SENACON_NOTA_TECNICA/SENACON%20DECIS%C3%83O%20geo%20pricing%20e%20geo%20blocking%20multa.pdf>. Acesso em: 10 nov. 2019.

COTS, Márcio. **Lei geral de proteção de dados pessoais comentada.** São Paulo: Thompson Reuters Brasil, 2018.

CUEVA, Ricardo Villas Bôas. **A insuficiente proteção de dados pessoais no Brasil.** Revista de direito civil contemporâneo, 2017. v. 13.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** São Paulo, SP: Thomson Reuters Brasil, 2019.

HARARI, Yuval Noah. **21 Lições para o século 21**. 1. ed. São Paulo, SP: Editora Companhia das Letras, 2018.

JÚNIOR, Marcos Ehrardt; LOBO, Fabíola Abuquerque. **Privacidade e sua compreensão no direito brasileiro.** Belo Horizonte: Fórum, 2019.

MACHADO, Joana de Moraes Souza. **A Tutela da privacidade na sociedade da informação:** a proteção de dados pessoais no Brasil. 1. ed. Porto Alegre, RS: Editora Fi, 2018.

THE GREAT Hacker. Direção: Karim Amer, Jehane Noujaim. Produção: Karim Amer, Pedro Kos, Geralyn Dreyfous, Judy Korin. Roteiro: Karim Amer, Erin Barnett, Pedro Kos.2019. Documentário (2h 19min).

TIMMS, Henry; HEIMANS, Jeremy. **Novo poder:** Como disseminar ideias, engajar pessoas e estar sempre um passo à frente em um mundo hiperconectado. 1.ed. Rio de Janeiro, RJ: Editora Intrinseca Ltda, 2019.

UNIÃO EUROPEIA. **Regulamento nº 679 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). Disponível em: <https://eur-lex.europa.eu/legal-content/pt/ALL/?uri=CELEX:32016R0679>. Acesso em: 15 set. 2019.

www.editorapublicar.com.br
contato@editorapublicar.com.br
@epublicar
facebook.com.br/epublicar

DIREITO:

Diálogos e pesquisas sobre temas contemporâneos

Roger Goulart Mello
Organizador

Publicar Editora

2022