PROTEÇÃO DE DADOS PESSOAIS DA CRIANÇA E DO ADOLESCENTE

PROTECTION OF PERSONAL DATA OF CHILDREN AND ADOLESCENTS

Cassiane Melo Fernandes[1]

Renata Aparecida Follone[2]

RESUMO

O mundo contemporâneo é caracterizado pela grande quantidade de informações lançadas na rede mundial de computadores e as consequentes formas de utilização desses dados. Com isso, surgem entraves jurídicos importantes ligados aos direitos da personalidade, em especial a privacidade, no tocante ao mau uso, ou ao uso não autorizado, desses dados. O presente trabalho tem por finalidade discutir o contexto da exposição de dados pessoais de crianças quando os pais, familiares, amigos ou qualquer pessoa ligada aos menores, que inserem informações a respeito destes na internet, denominado *shareting* em contraposição à liberdade de expressão. Para tanto, a prática será analisada através dos mecanismos do Marco Civil da Internet (MCI), da Lei Geral de Proteção de Dados pessoais (LGPD) e da jurisprudência para endereçar tal colisão de normas. O artigo, também, analisa o papel dos provedores de aplicação, em especial redes sociais e ferramentas de busca, na criação de

[1]Doutoranda e Mestra em Direito pela UNAERP-Universidade de Ribeirão Preto, em Proteção e Fundamentos Constitucionais dos Direitos Coletivos, com área de concentração em Direitos Coletivos, Cidadania e Função Social do Direito. Especialista em Direito do Trabalho e Processo do Trabalho pela UGF-Universidade Gama Filho. Possui graduação em Direito pela UNIARA-Centro Universitário de Araraquara. Docente de Direito Processual Trabalho, Direito do Trabalho e Prática Trabalhista e Previdenciária na UEMG-Universidade de Minas Gerais/Campus de Frutal-MG (2011-2016). Docente de Direitos Reais no Centro Universitário - UNIFAFIBE. Conteudista no curso de Pós-Graduação à distância da Associação São Bento de Ensino mantenedora da UNIARA- Centro Universitário de Araraquara. Membro da Associação Mundial de Processo Constitucional. Presidente da Comissão "OAB vai à Escola" da 241ª Subsecção da Ordem dos Advogados do Brasil. Palestrante. Advogada com experiência na área de Direito, com ênfase em Direito de Família e Sucessões, Direito Processual Civil, Direito do Trabalho e Empresarial.E-mail **rfollone@uol.com.br**

[2]Mestre em Direitos Coletivos e Cidadania pela Universidade de Ribeirão Preto, advogada e especialista em Direito Empresarial pela Faculdade Barretos. Atualmente é Procuradora/Pesquisadora Institucional, atua junto ao Departamento Jurídico, Docente e Coordenadora do Núcleo de Métodos Adequados de Solução de Conflitos e do NAC - Núcleo Permanente de Acessibilidade e Inclusão da Faculdade Barretos. É membro da Associación Mundial de Justicia Constitucional. Tem experiência em Direito, com ênfase em Direito Empresarial, atuando principalmente com os meios adequados de solução de conflitos: Conciliação, Mediação e Arbitragem e Direito Digital. Leciona os componentes curriculares de direito ambiental, métodos adequados de tratamento de conflitos e direito digital.E-mail **cassiane.melo@hotmail.com**

mecanismos que assegurem o direito ao esquecimento das crianças e que previnam o compartilhamento exagerado de informações pelos pais; a esse respeito, foi realizada a comparação dos modelos brasileiro e europeu. Ao final, dentro do cenário normativo, conclui-se que a LGPD buscou impor limites no tratamento dos dados das crianças, medida esta que transmite o que há de mais avançado em termos de fortalecimento das crianças e adolescentes como sujeitos de direitos e protagonistas de seus direitos.
Palavras-chave: Proteção; dados pessoais; criança; adolescente.

ABSTRACT

The contemporary world is characterized by the large amount of information released on the world wide web and the consequent ways of using this data. As a result, important legal barriers related to personality rights, especially privacy, arise regarding the misuse, or unauthorized use, of these data. This paper aims to discuss the context of the exposure of children's personal data when parents, family members, friends or anyone connected to minors, who insert information about them on the internet, called shareting as opposed to freedom of expression. To this end, the practice will be analyzed through the mechanisms of the Marco Civil da Internet (MCI), the General Law for the Protection of Personal Data (LGPD) and the jurisprudence to address such a collision of standards. The article also analyzes the role of application providers, especially social networks and search engines, in creating mechanisms that ensure children's right to be forgotten and that prevent over-sharing of information by parents; in this regard, the Brazilian and European models were compared. In the end, within the normative scenario, it is concluded that the LGPD sought to impose limits on the treatment of children's data, a measure that conveys the most advanced in terms of strengthening children and adolescents as subjects of rights and protagonists of their rights.
Keywords: Protection; personal data; kid; teenager.

1 INTRODUÇÃO

O mundo contemporâneo é caracterizado pela grande quantidade de informações lançadas na redemundial de computadores e as consequentes formas de utilização desses dados. Com isso, surgem entraves jurídicos importantes ligados aos direitos da personalidade, em especial a privacidade, no tocante ao mau uso, ou ao uso não autorizado, desses dados. Diante desse cenário, é crescente a discussão sobre o tratamento

de dados, os deveres e a responsabilidade dos provedores de aplicação em relação à coleta, a guarda e o uso deinformações.

O presente trabalho tem por finalidade discutir o contexto da exposição de dados pessoais de crianças quandoos pais, familiares, amigos ou qualquer pessoa ligada aos menores, que insereminformações a respeito destes na internet. Importante salientar que essa situação pode ocorrer nas situações mais rotineirasda criança, como a do pai orgulhoso dos êxitos de seu filho que posta em suas redes sociais fotografias e comentários sobre o menor.

O compartilhamento de informações feito pelos pais na internet é denominado *sharenting*.Procurar-se-á analisar a evolução das discussões referentes à colisão entre liberdade de expressão e a privacidade associando-asà esse contexto.

Sabe-se que é recorrente nos dias atuais a utilização das redes sociais para expressar aspectos da vida, das experiências da maternidade ou paternidade, sendo que tal hábito e constitui uma dasvertentes do direito de se expressar livremente. Todavia, ao exercerem essa liberdade, os pais expõem, semo consentimento dos filhos, dados a respeito destes, situação essa que, futuramente, pode não corresponder ao seu desejo. Com isso, a liberdade de expressão dos pais colide com interesses relativos à privacidade dos filhos.

Procurar-se-á discutir também o papel dos provedores de aplicações de internet, em especial das redes sociaise ferramentas de busca, no intuito de limitar a divulgação de informações de caráter pessoal de crianças. Por fim, será analisado o atual contexto regulatório brasileiro em relação ao tema e, paralelamente, com o direito comparado, objetivando investigar quais condutas poderiam ser adotadas pelos provedores de aplicação na indústria do*sharenting*.

2 O *SHARENTING* E OS DADOS PESSOAIS DOS MENORES

Sharenting é uma expressão da língua inglesa que decorre da união das palavras “share” (compartilhar) e “parenting” (cuidar, no sentido de exercer o poder familiar). Essa prática funda-se no hábito dos pais, ou responsáveis legais, postarem informações, fotos e dados dos menores que estão sob a sua tutela na internet. O compartilhamento dessas

informações, via de regra, decorre da nova forma de relacionamento via redes sociais e é realizado no âmbito do legítimo interesse dos pais de contar, livremente, as suas próprias histórias de vida, da qual os filhos são um elemento central. (STEINBERG, 2017, p. 877)

O entrave jurídico que decorre do*sharenting* diz respeito aos dados pessoais das crianças que são inseridos na internet ao longo dos anos e que lá permanecem, sendo que podem ser acessados muito tempo após a publicação, tanto pelo titular dos dados (a própria criança à época da divulgação) quanto por terceiros. De acordo Steinberg, essas informações podem causar impactos desde a infância até a vida adulta e podem expor as crianças a constrangimentos em razão de histórias, fotografias ou comentários divulgados na *web* que possam ser considerados embaraçosos. (2017, p. 877)

Na acepção jurídica do termo, dado pessoal é toda e qualquer informação relacionada a pessoa natural identificada ou identificável, consoante dispõe o art. 5º da Lei n. 13.853/2019 – Lei Geral de Proteção de Dados Pessoais - LGPD. Assim, ao exporem o nome dos próprios filhos na internet, por exemplo, os pais estarão divulgando os dados pessoais da criança. Podem também ser enquadradasnesse conceito informações que, quando analisadas em conjunto, permitam identificar o titular dos dados. Com efeito, imprescindível que tais informações estejam relacionadas à sujeitos identificados ou identificáveis para serem consideradas dados pessoais.

Importante ressaltar que, ainda que a intenção dos pais de exporem seusfilhos não seja explícita, ou, ainda, que os pais tentem exercer mecanismos para preservar os dados pessoais dos menores– omitindo o nome, por exemplo – a análise do comportamento dos adultos nas redes sociais pode permitirque terceiros façam inferências a respeito de informações que possam ser associadas a uma criança concretae específica, tais como localização, idade, aniversário e religião. (STEINBERG, 2017, p. 848)

O conceito de*sharenting* contempla também aquelas situações em que os pais fazem a gestão da vida digital de seusfilhos na *internet*, criando perfis em nome das crianças em redes sociais e postando continuamente informações sobre sua rotina. Nessa situação, os pais não estão tão somente administrando as suas próprias vidas digitais, mastambém criando redes paralelas em nome de seus filhos.

Consequentemente, a exposição de informações dos menores de maneira exacerbada pode representar ameaça à intimidade, vida privada e direito à imagem das crianças, interesses estes que são expressamente protegidos pelo art. 100, V, da Lei n. 8.069/1990, o Estatuto da Criança e do Adolescente (ECA).

O concepção de privacidade é contextual, temporal e varia muito de acordo com o modo de vida e nível de exposição que o próprio titular do direito está disposto a oferecer. Dessa forma, é perfeitamente possível – senão provável – que o critério sobre privacidade que os pais possuam seja diferente daquele que a criança vai desenvolver na vida adulta. Ou seja, a criança pode desaprovar a conduta dos seus pais e entender que teve sua vida privada exposta indevidamente durante a infância. (EBERLIN, 2017, p. 259)

Isso não quer dizer que o compartilhamento, pelos pais, de informações referentes aos seus filhos seja absolutamente vedado. Isso porque cabe à eles o poder-dever de cuidar dos filhos e decidir o que é mais conveniente para eles, inclusive no âmbito digital. Além do mais, há que ser considerada a liberdade de expressão dos pais de manifestar os seus próprios momentos ao lado dos filhos, ainda que isso acarrete a divulgaçãodos dados pessoais deles.

Em verdade, pressupõe-se que, na maioria das vezes, não há a intenção por parte do pai ou da mãe de expor seus filhos e respectivos dados; todavia, muitas vezes os responsáveis legais não têm conhecimento das consequências que o seu comportamento on-line pode causar aos menores ao longo do tempo. (STEINBERG, 2017, p. 847)

A ausência de compreensão das consequências em expor os dados decorre do baixo entendimento dos mecanismos da sociedade da informação, que tem como um dos pressupostos a constante coleta de dados. Assim, a falta de conhecimento e de aspectos práticos para limitar a coleta de dados dificulta sustentar, inclusive, que os pais seriam responsáveis pela excessiva exposição de informações de seus filhos.

Alguns exemplos da sociedade da informação mostram como a questão dos dados se torna complexa em função, por exemplo, da interação constante entre os diversos tipos de mídia. Acerca desse novel modelo de sociedade, destaca-se:

> A sociedade da informação é uma nova formação política, social e econômica firmada por relações em rede, centrada na coleta, seleção, triagem e distribuição de dados por meio das tecnologias da informação. Os processos e funções essenciais em sociedade permanecem em constante e rápida transformação. E, com o advento da internet e o seu crescente uso, tornou-se ainda mais viável o exercício das liberdades atinentes ao tratamento da informação e aos modos de expressão, possibilitando ainda a imortalização e o compartilhamento de notícias e dados diversos sem limites de tempo e espaço. (MOREIRA; MEDEIROS, 2016)

Ou seja, nesse modelo de sociedade,alguns comportamentos que outrora expunham crianças, mas que eram de certa forma controlados, hodiernamente não existe a mesma possibilidade de controle. Além disso, a sociedade da informação permite que terceiros disponibilizem na internet informações pessoais de crianças, tais quais as escolas que compartilham fotos em redes sociais de eventos, competições e festas envolvendo a participação de menores.

Nesse contexto de ambiente escolar, as fotografias tiradas por pais de alunos de seus filhos em eventos do colégio com outras crianças disponibilização ulterior dessas fotografias nas redes sociais já foi objeto de grande debate no Reino Unido. No ano de 2013, Bessant conduziu uma pesquisa junto a 206 autoridades locais responsáveis pela gestão educação na Inglaterra, Escócia e País de Gales. O resultado obtido apontou para o entendimento de que os pais podem fotografar seus filhos com outras crianças, desde que as fotografias se restrinjam a uma utilização pessoal. Todavia, o compartilhamento das fotos na internet é uma questão que ainda não foi respondida pela regulamentação do Reino Unido, o que causa bastante debate naqueles países. (2014, p. 271)

E não é somente os pais que podem expor as crianças e algum conteúdo que ofenda a privacidade delas, mas elas próprias. Nesse sentido, destaca-se o*cyberbullying*, prática esta que vem ganhando espaço na internet e que pode expor indevidamente informações pessoais de menores. De acordo com Viana, Maia e Albuquerque (2017), essa prática é um problema desaúde pública que justifica certas limitações à liberdade de expressão.

Steinberg (2017, p. 867) sugere que, uma das alternativas no campo das políticas públicas para o tema, seria a implementação de medidas para educar os pais acerca do uso de mídias sociais e que reconheçam a necessidade de proteção da privacidade das crianças.

Referida proposta permitiria não apenas aos pais, mas também a parentes, amigos, colégios e quaisquer outros terceiros que tenham relação com crianças, a aquisição de conhecimentos importantes sobre os riscos envolvidos pelo uso de redes sociais em se tratando de compartilhamento de informações referentes a menores. Esse tipo de conhecimento permitiria aos pais compartilharem suas histórias de vida nas redes sociais protegendo, ao mesmo tempo, a privacidade de seus filhos.

Nesse sentido, busca-se também no presente artigo debater a respeito de mecanismos de informação e educação digital, em especial sob a ótica das obrigações específicas dos provedores de aplicativos de internet que, de algum modo, lidam com dados pessoais de crianças, paralelamente à proteção conferida pela LGPD. Para tanto, primeiramente faz-se necessário demonstrar a atual dimensão dos direitos fundamentais à liberdade de expressão e à proteção de dados pessoais.

3 A LIBERDADE DE EXPRESSÃO E A PROTEÇÃO DE DADOS PESSOAIS

A liberdade de expressão, direito fundamental insculpido no art. 5º, IV da Constituição Federal (CF) estabelece o direito à livre manifestação do pensamento e o art. 220 da Lei Maior enfatiza a liberdade de informação, rechaçando de maneira expressa qualquer previsão que venha constituirentrave à liberdade de expressão ou qualquer censura de natureza política, ideológica ou artística.

Hodiernamente, a interpretação da jurisprudência no que diz respeito à liberdade de expressão é a de que dita garantia não tem caráter absoluto, que deve ser ponderado com o direito à dignidade, à honra e à imagem, além de outros direitos fundamentais e, além do mais, podem ser aplicadas à sua atual dimensão no mundo digital (EBERLIN, 2017, p. 262). A internet e as redes sociais viabilizaram a possibilidade da manifestação de pensamento de forma imediata e rápida, seja a respeito de si próprio ou de terceiros. Diante disso, paralelamente à proteção da privacidade, a garantia do direito à liberdade de expressão foi reconhecida no MCI como “condição para o pleno exercício do direito de acesso à internet” (art. 8º da Lei 12.965/2014). Na mesma linha, a LGPD, em seu

art. 2º, III, indicou a liberdade de expressão como fundamento da disciplina relativa à proteção de dados.

No que diz respeito aos dados pessoais, sua proteção está ligada à tutela da privacidade e as características de complementariedade e solidariedade dosprincípios constitucionais (§ 2º do art. 5º da CF). O art. 5º, X da CF prevê que são "invioláveis a intimidade,a vida privada, a honra e a imagem das pessoas". Por seu turno, o Código Civil (CC), preconiza que a vidaprivada da pessoa natural é inviolável (art. 21), constituindo a privacidade um direito de personalidade.

Nesse sentido, a evolução histórica da legislação sobre proteção de dados demonstra o liame desse direito com a tutelada privacidade. Mendes explica essa evolução em 4 gerações de leis (MENDES, 2014, p. 37).

Na década de 70, os indivíduos se preocupavam com os bancos de dados das Administrações Públicas e do poder queesses dados conferiam ao Estado sobre a vida privada dos cidadãos. Nesse momento, as leis estabeleciam procedimentos para novos bancos de dados, tal qual a exigência de autorização pública prévia para criação deum sistema de armazenamento.

Posteriormente, em uma segunda fase, a preocupação se concentrava nas normas de proteção de dados pessoais e privacidade, ultrapassada a preocupação com o procedimento em si. A terceira geração, a partir da década de 80, consagrou a ideia de autodeterminação informativa, vale dizer, as pessoas passam a participar do processamento de dados "como um envolvimento contínuo em todo o processo, desde a coleta, o armazenamento e a transmissão e não apenas como opção entre 'tudo ou nada'" (MENDES, 2014, p. 42).

A quarta geração de proteção de dados consagrou a proteção dos denominados "dados sensíveis", além de instituir normas setoriais a respeito do assunto. Nesse sentido, tem-se por dados sensíveis aqueles que se relacionam a questões particulares das pessoas, tais como gênero, orientação sexual, origem social e étnica, convicções políticas, orientação religiosa, questões filosóficas, dados de saúde, informações genéticas, dentre outras. No Brasil, esse conceito foi positivado pela Lei do Cadastro Positivo (Lei n. 12.414/2011, art. 3º, § 3º, II).

Posteriormente, a LGPD dispõe no art. 5º, inciso II, que: D

> Dado pessoal sensível: dado pessoal 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;

Essa construção legislativa se desenvolveu juntamente à sociedade dos dados, segundo a qual, de acordo com Schreiber (2011, p. 129), traz à privacidade um significado que vai além da tradicional proteção da vida íntima, representando um direito de controle sobre os dados pessoais, isto é, o direito de a pessoa escolher se quer ou não ter as suas informações divulgadas e compartilhadas.

Em se tratando do *sharenting*, essa nova geração do direito à privacidade é bastante complexa. De acordo comSteinberg, as crianças possuem interesse em proteger as informações a seu respeito que foram postadas por seus pais, evitando sua disseminação sem controle, assim como podem não concordar com a decisão dos pais de compartilhar informações pessoais; no entanto, as crianças não possuem uma opção de *opt-out* e nenhum tipo de controle em relação às decisões de seus pais que deixem rastros digitais. Essa falta de controle por parte dos titulares dos dados (no caso, as crianças) nega o exercício do direito à autodeterminação informativa (2017, p. 843).

Daí porque afirmar que a proteção à privacidade ganha contornos bastante complexos. De acordo com Mendes, o reconhecimento da proteção de dados pessoais como direito fundamental é uma "necessidade para tonar efetivos os fundamentos e princípios do Estado Democrático de Direito, na sociedade contemporânea da informação, conforme determina a Constituição Federal" (2014, p. 172).

No caso específico da internet, o MCI estabeleceu, expressamente, a proteção da privacidade e dos dados pessoais como princípio do uso da internet no Brasil (art. 3º, II e III da Lei 12/965/2014), o que foi ratificado pela LGPD (art. 2º), corroborando, portanto, o entendimento acima.

Em uma abordagem internacional, o caráter fundamental do direito à proteção de dados foi expressamente reconhecido na legislação comunitária europeia, por meio do

Regulamento 2016/679[3], que considera a proteção de dados como um direito fundamental (arts. 1º e 2) e que deve ser equilibrado com outros direitos fundamentais em conformidade com o princípio da proporcionalidade.

Assim, no caso do *sharenting*há dois interesses opostos em colisão. De um lado, os direitos fundamentais à privacidade e à proteção de dados pessoais das crianças e, do outro, o direito à liberdade de expressão de terceiros no ambiente digital. Nesse sentido, o conflito entre as normas que regulam tais diretos deve ser endereçado por meio de técnicas de ponderação.

Alexy explica que as normas são classificadas como regras ou princípios. As regras devem ser analisadas como normas que impõem condutas (ou proibição de condutas) e que devem ser aplicadas a um determinado caso concreto na exata maneira como formuladas; nem mais, nem menos (2012, p. 91). Por seu turno, o conflito entre regras ocorre na dimensão da validade das normas, vale dizer, uma regra será válida e a outra não. Já os princípios, são "normas que ordenam que algo seja realizado na maior medida possível dentro das possibilidades jurídicas e fáticas existentes" (2012, p. 90).

Ou seja, os princípios são mandamentos de otimização, normas de maior generalidade, se e quando analisadas isoladamente, podem levar a resultados diferentes em uma mesma situação concreta. Os princípios em colisão devem ser sopesados com base na máxima da proporcionalidade, isto é, deverá haver a relativização dos princípios em face das possibilidades jurídicas em cada caso concreto (2012, p.117).

Sobre o assunto, Canaris reconhece que "pertence à essênciados princípios gerais de Direito que eles entrem, com frequência, em conflito entre si, sempre que, tomadosem cada um, apontem soluções opostas" (2002, p. 205). Nesse ínterim, para se trabalhar com as aparentes contradições de princípios e valores, deve-se lançar mão de ferramentas tais como a interpretação sistemática,vale dizer, interpretar uma norma ou uma

[3] Regulamento (UE) do Parlamento Europeu e do Conselho nº 2016/679, 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. Disponível em: <http://eurlex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:32016R0679&from=en>. Acesso em: 28 ago. 2019.

situação entendendo o sentido de cada princípio para o sistema ebuscando uma solução que faça valer esse sentido dentro do caso concreto (CANARIS, 2002, p. 205).

Diante desse contexto atual, entende-se que a atuação direta e maior regulação dos aplicativos de internet pode contribuir para que se alcance a melhor solução, por serem intermediários na divulgação de dados.Para tanto, imprescindível compreender quais os critérios e extensão da responsabilidade desses aplicativos, quer existentes, ou demandar por eles, se inexistentes.

Nesse sentido, o contexto atual brasileiro aponta para um caminho de pouca responsabilidade dos provedores de aplicativos no que diz respeito ao conteúdo gerado por terceiros, independentemente da natureza das atividades que realizam[4]. Assim, o MCI estabeleceu a regra no sentido de que os provedores de aplicação somente serão responsabilizados se deixarem de cumprir ordem judicial especifica, “no âmbito e nos limites técnicos de seu serviço” (art. 19). Em se tratando de conteúdo gerado por terceiros conter imagens, vídeos ou outros materiais “contendo cenas de nudez ou de atos sexuais de caráter privado”, o provedor deve adotar medidas imediatas, independentemente de ordem judicial, mas ainda sim “no âmbito de e nos limites técnicos de seu serviço” (art. 21). Em se tratando de *sharenting*, isso significa que os *websites* só estariam obrigados a adotar medidas independentemente de ordem judicial em casos extremos como os de pedofilia.

Sobre o assunto, o modelo europeu indica um caminho da existência de deveres, com maior rigor e de maior amplitude na responsabilização dos provedores de aplicativos, inclusive ferramentas de busca, fundamentados no direito ao esquecimento, em relação ao conteúdo gerado por terceiros como será demonstrado a seguir.

3.1 O MODELO EUROPEU E AS ALTERNATIVAS PARA O MODELO BRASILEIRO

[4] O AgInt no REsp n. 1.593.873-SP44 é um caso emblemático a respeito do entendimento do SuperiorTribunal de Justiça (STJ) sobre a (ausência de) responsabilidade de provedores de aplicação pelo conteúdogerado por terceiros. No caso específico, foi analisada a responsabilidade das ferramentas de busca e que, nos termos do acórdão, a ferramenta de busca éparte ilegítima para esse tipo de pedido, sendo que o ofendido deveria buscar medidas tendentes à supressãodo conteúdo ofensivo diretamente perante aquele que disponibiliza esse conteúdo na rede e não perante osite de pesquisas. Naquele momento, um dos aspectos bastante acentuados nessa decisão é o fato de o Brasil não possuir umalegislação geral para proteção de dados pessoais até então.

O “velho mundo” regula a proteção de dados e a respectiva inserção destes por terceiros na rede mundial de computadores com maior rigor. Aqui, eleger-se-á o caso “Lindqvist” (UNIAO EUROPEIA, 2014) como marco da implementação desse modelo. Nesse precedente, a Sra. Lindqvist, além de exercer suas atividades profissionais, era catequista numa Paróquia na Suécia. Em 1998, no âmbito de um curso de informática que havia frequentado, resolveu desenvolver uma página de internet, com seu computador e em sua residência, para que os paroquianos pudessem obter informações eventualmente necessárias para prepararem a crisma.

Nessa página criada pela a Sra. Lindqvist, esta inseriu informações pessoais a seu respeito de mais 18 colegas da Paróquia, incluindo nomes, hobbies, funções ocupadas na atividade paroquial, estado civil e número de telefone. Por sua vez, a Sra. Lindqvist não avisou os colegas da existência do site e, além disso, solicitou ao administrador da página de internet da igreja que fizesse um link para o site criado por ela. Assim que soube que alguns dos colegas não estavam satisfeitos com a página, a Sra. Lindqvist a retirou do ar. Por essa razão, a paroquiana foi processada por tratar dados de caráter pessoal sem obter a autorização dos seus titulares e sem avisar a autoridade de controle sueca. (EBERLIN, 2017, p. 268)

Em prosseguimento, o Tribunal de Justiça da União Europeia entendeu que a disponibilização de informações de caráter pessoal da internet, deixando-as acessíveis a todos, mesmo na peculiar situação da Sra. Lindqvist, que era um site particular, sem finalidades econômicas, constitui tratamento de dados[5].

Referida decisão foi um dos marcos para a construção de um conceito amplo sobre o que é tratamento de dados pessoais e tem o efeito prático de impor as obrigações da legislação de proteção de dados às mais singelas atividades que tragam qualquer tipo de divulgação de informações de caráter pessoal.

Ainda no âmbito no Direito Europeu, é emblemático o caso conhecido como “Google Spain” (UNIAO EUROPEIA, 2014). Nesse caso, o autor da ação, Sr. Mario Costeja

[5] A Sra. Lindqvist, também, foi acusada de ter transferido dados pessoais para outros países sem autorização dos seus titulares, na medida em que os disponibilizou na rede mundial de computadores, de modo que pudessem ser acessados por residentes em outros países. Sobre esse aspecto, o Tribunal entendeu que a acusação não procedia, pois o site e os dados pessoais estavam hospedados dentro do próprio Estado ou de um Estado Membro.

González, sustentava que, quando pesquisado o seu nome, a ferramenta de buscas da Google apresentava duas páginas do jornal La Vanguardia do ano de 1998 com informações sobre a venda de imóveis decorrente de um arresto em função de dívidas que este possuía. Sustentava também que o processo de arresto já havia sido resolvido há vários anos e que não havia pertinência na referência ao mesmo no site de busca, motivo pelo qual requereu que seus dados pessoais deixassem de aparecer nos resultados de pesquisa associados aos fatos acima narrados. De outro lado, a Google alegou não ter controle sobre o conteúdo postado por terceiros e que o Autor deveria adotar as providências que entendesse pertinentes diretamente junto ao site que publicou as informações.

Mais uma vez, o Tribunal de Justiça da União Europeia entendeu que a atividade realizada pela Google se enquadra no conceito de tratamento de dados pessoais, estando sujeita às obrigações respectivas, dentre as quais se encontram a de assegurar a correção e exatidão dos dados. Além do mais, o Tribunal enfrentou a necessidade de contrabalancear os interesses do autor e os da coletividade, em especial daqueles que, por qualquer motivo, queiram ter acesso à informação. A conclusão do Tribunal apontoupelo reconhecimento do direito ao esquecimento no caso concreto por não haver razões especiais que justificassem um interesse preponderante da coletividade na informação referente às dívidas já quitadas pelo autor da ação.

Nesse aspecto, importante salientar que o reconhecimento do direito ao esquecimento pelo Tribunal de Justiça da União Europeia e da obrigação de o provedor de aplicações adotar medidas para efetivar esse direito é um indicativo importante para a proteção dos interesses das crianças no *sharenting*. Assim, de acordo com Steinberg, o reconhecimento do direito ao esquecimento pode ser uma alternativa para encontrar o justo equilíbrio entre a proteção da privacidade da criança e a liberdade de expressão dos pais. De acordo com a autora, quando os pais compartilham informações sobre o seus filhos na internet, eles tem o objetivo de expressar questões ligadas, em especial, ao crescimento dos filhos e ao seu momento de vida como pai ou mãe. Esse objetivo perde o propósito com o crescimento da criança, de modo que a imposição da obrigação de apagar os dados pessoais de crianças de sites de busca com o passar do tempo assegura, ao mesmo tempo, o

direito dos pais de se manifestarem em relação ao crescimento de seus filhos e os interesses das crianças em relação aos seus dados pessoais (STEINBERG, 2017, p. 876).

Apesar de não estar positivado expressamente no ordenamento jurídico pátrio, o direito ao esquecimento é reconhecido pela doutrina brasileira. Nesse sentido,Chehab o conceitua como "a faculdade que o titular de um dado ou fato pessoal tem para vê-lo apagado, suprimido ou bloqueado, pelo decurso do tempo e por afrontar seus direitos fundamentais" (2015).

Acioli e Erhardt Júnior (2017) entendem que algumas expressões do direito ao esquecimento estão presentes no MCI (como o direito à exclusão dos dados pessoais - art. 7º - e o direito à remoção de conteúdo gerado por terceiros que divulgue, sem autorização, materiais contendo cenas de nudez ou de atos sexuais de caráter privado - art. 21). Nesse sentido, o art. 60 da LGPD regulamentou nas disposições finais e transitórias o direito de exclusão estampado no art. 7º do MCI.

Dessa forma, tem-se que o direito ao esquecimento é reconhecido pela doutrina e jurisprudência e que o mundo digital possui aspectos específicos que colocam as crianças em situação de vulnerabilidade acentuada. Nessa senda, o sistema jurídico pátrio possui normas estabelecendo obrigações de cuidado em relação às crianças (art. 227 da CF e art. 100, V do ECA), obrigações de prestar informações claras e precisas sobre os serviços contratados e seus riscos, com base na boa-fé (art. 31 do CDC e art. 113 do CC) e obrigações de reparar danos (arts. 6º, VI e 7º, § único do CDC e 927 do CC).

Da análise de todo esse aparato normativo, pode-se eleger duas espécies de obrigações decorrentes: a primeira seria uma obrigação de caráter preventivo, vale dizer, de melhorar a qualidade das informações sobre os serviços oferecidos, em especial dos riscos associados ao compartilhamento de dados, sendo que cuidado deve ser redobrado quando o provedor detectar a possibilidade de compartilhamento de informações de crianças.

Em segundo, a obrigação que pode ser adotada no atual contexto da legislação brasileira é de caráter corretivo, ou seja, como as crianças não possuem qualquer controle sobre os dados que seus pais – ou terceiros correlatos – postam a seu respeito, o exercício de direitos depende da instituição de mecanismos capazes de apagar esses dados a seu respeito que foram postados por terceiros ao longo da infância.

A União Europeia, por meio da General Data ProtectionRegulation (GDPR), em vigor desde maio de 2018, explicitamente reconhece que crianças e adolescentes precisam de maior proteção. Segundo a regulação, essa proteção específica deve ser aplicada à utilização de dados pessoais de crianças e adolescentes para efeitos de comercialização, de criação de perfis e na coleta de dados pessoais em serviços disponibilizados diretamente a eles. Para serviços da sociedade da informação, há a obrigação de consentimento parental ou de responsável legal para coleta tratamento de dados de pessoas com até 16 anos de idade, ainda que os Estados-membros possam definir a idade de maioridade para consentimento, desde que não inferior a 13 anos.

Ainda, o regramento europeu define que qualquer informação e comunicação sobre os procedimentos da coleta e tratamento de dados deve estar redigida em uma linguagem clara e simples, que crianças e adolescentes compreendam facilmente. Nos Estados Unidos, desde 1998, o Children's Online PrivacyProtectionAct (COPPA), atualizado em 2013, especifica regras para a garantia da privacidade de crianças na Internet, incluindo a notificação parental para o tratamento de dados e a aprovação da coleta em caso de compartilhamento dos dados com terceiros

Nesse sentido, a LGPD buscou tutelar essa categoria de indivíduos no contexto da sociedade da informação.

4 O TRATAMENTO DA LGPD EM RELAÇÃO ÀS CRIANÇAS E ADOLESCENTES

A Lei Geral de Proteção Dados Pessoais (LGPD) sancionada recentemente cria direitos dos cidadãos e regras para empresas e poder público no que diz respeito ao tratamento de dados pessoais no Brasil. Com o intuito de proteger de forma especial os hipervulneráveis, a norma jurídica contempla, em seu artigo 14, especificidades para o tratamento de dados pessoais de crianças e adolescentes para protegê-los de qualquer forma de exploração ou violação de seus direitos.

A criança está em condição peculiar de desenvolvimento social e biopsíquico. Por isso, crianças e adolescentes podem estar menos cientes dos riscos e consequências do tratamento de dados, bem como dos direitos correlatos. Esta afirmação é ainda mais

relevante diante da característica da atividade de tratamento de dados, invisível aos olhos, abstrata e, ainda assim, com alto grau de complexidade, dificultando sua observação e entendimento, especialmente para crianças.

Nesse sentido, imprescindível que uma lei geral de proteção de dados traga parâmetros mínimos para a regulação desta questão, de acordo com o dever constitucional de prioridade absoluta das crianças nas políticas e normas legais e assegurando-lhes o respeito ao seu melhor interesse.

A LGPD estabelece, no artigo 14, o melhor interesse de crianças e adolescentes como base legal exclusiva para a autorização do tratamento de dados dessas pessoas, colocando-as a salvo de toda forma de exploração ou violação de direitos.

No caso de dados pessoais de crianças, pessoas de até 12 anos de acordo com o ECA, é exigido consentimento para a coleta de dados. Pelo menos um dos pais ou o responsável legal precisa dar o consentimento para a operação e, diferentemente do consentimento em outros casos, esta manifestação deve ser específica para cada caso, solicitada em destaque, além de livre, informada e inequívoca, tal qual os demais previstos na lei.

A coleta e uso dos dados pessoais de crianças podem ocorrer sem consentimento parental apenas em duas situações: a primeira é justamente para contatar os pais ou o responsável legal, desde que os dados sejam utilizados uma única vez e sem armazenamento. Na segunda hipótese de dispensa de consentimento parental, quando o objetivo for a proteção desses indivíduos que estão em peculiar estágio de desenvolvimento. Em nenhum dos casos os dados pessoais em questão poderão ser repassados a terceiros.

Nesse sentido, o controlador dos dados deve realizar todos os esforços razoáveis para verificar que o consentimento foi dado pelo responsável pela criança, considerando as tecnologias disponíveis. Órgão competente deve regulamentar as práticas adequadas e em quais hipóteses se supõe que o melhor esforço foi empregado. A criança poderá até utilizar um aplicativo de jogo no celular antes do responsável legal autorizar a coleta, porém seus dados pessoais não poderão ser coletados.

O parágrafo 4º do artigo 14 da LGDP prevê que os controladores de dados não devem condicionar a participação de crianças ao fornecimento de dados pessoais em jogos,

aplicações de internet ou outras atividades semelhantes. Ou seja, se não há consentimento parental para o tratamento, as crianças mesmo assim devem continuar tendo acesso. Ainda, os responsáveis por estes sistemas e soluções devem observar a regra da minimização da coleta ao estritamente necessário à atividade.

Além das obrigações de transparência previstas em outros artigos da LGPD, o artigo 14 obriga os controladores de dados pessoais a manterem pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos dos titulares tais como: confirmação da existência do tratamento; acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei; portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa do titular; eliminação dos dados pessoais tratados com o consentimento do titular; informação sobre a possibilidade de não fornecer consentimento e as consequências e revogação do consentimento.

As crianças e adolescentes estão um processo contínuo e inconcluso do desenvolvimento de suas capacidades, inclusive da compreensão de conceitos abstratos, técnicos ou jurídicos. Pensando nisso, os legisladores brasileiros inovaram ao prever, no parágrafo 6° do artigo 14 da LGPD, que as informações sobre o tratamento de dados de crianças e adolescentes deverão ser fornecidas de maneira simples, clara e acessível – com uso de recursos audiovisuais, quando adequado, a crianças – para que eles possam ter contato com este universo progressivamente e, à medida de seu amadurecimento, tomar conhecimento das práticas de tratamento de dados e assumir sua autodeterminação informacional.

O Brasil, com a aprovação do LGPD, se enquadra na lista de países que entendem as crianças como sujeitos em desenvolvimento e que essa condição inerente exige proteção adicional a estes sujeitos, de forma que o tratamento de seus dados só podem ser tratados com consentimento de ao menos um dos pais ou responsável legal.

5 CONSIDERAÇÕES FINAIS

Em um primeiro momento, mister salientar que os*harenting* é um fenômeno atual e intimamente ligado à sociedade da informação, sendo que, quando realizado dentro de certos limites, é atividade legítima do exercício da liberdade de expressão por parte dos pais que querem compartilhar informações a respeito de seus filhos.

No entanto, ao sopesar os riscos decorrentes da exposição exagerada de informações sobre as crianças na internet, assim como os interesses também legítimos das crianças em relação à privacidade,imprescindível que sejam adotadasmedidas que balizem esse comportamento.

Assim, a complementariedade e a solidariedade na interpretação das garantias constitucionais do indivíduo, como a proteção de dados pessoais, a privacidade, o direito ao esquecimento e a garantia à liberdade deexpressão é medida que se impõe na intenção de garantir o exercício de tais direitos de maneira universal.

Além das possibilidades analisadas ao longo do texto, sustenta-se que políticas públicas teriam sobremaneira importância no que diz respeito à educação em relação ao uso das ferramentas digitais. Tais políticas podem ser executadas pelo próprio Estado e pelas empresas que exploram as atividades econômicas ligadas ao *sharenting*, tais quais as redes sociais e as ferramentas de busca.

Em especial aos aplicativos e ferramentas de busca da internet, partindo-se da premissa que elas criam o ambiente paraque o *sharenting* ocorra e que, também, criam expectativas de segurança em relação aos dados pessoais, mister que a caminhem para a prevenção e correção de eventual exposição de informações de crianças, ainda que realizada por seus pais ou responsáveis legais, que ultrapasse os limites de violação de seus direitos.

No Brasil, a construção do caminho para proteção dos interesses das crianças com a preservação dosdemais interesses envolvidos pode decorrer tanto de uma evolução legislativa,como da evolução no entendimento jurisprudencial, objetivando a efetivação de medidas concretas pelos provedores, especialmente no que tange às obrigações de informação e à implementação de mecanismos técnicos para viabilizar o direito ao esquecimento.

Nessa senda, a LGPD buscou impor limites no tratamento dos dados das crianças, medida esta que transmite o que há de mais avançado em termos de

educação/comunicação e fortalecimento das crianças e adolescentes como sujeitos de direitos e protagonistas de seus direitos.

REFERÊNCIAS

ACIOLI, Bruno de Lima; EHRHARDT JÚNIOR, Marcos Augusto de Albuquerque. Uma agenda para o direito ao esquecimento no Brasil. **Revista Brasileira de Políticas Públicas**, v. 7, n. 3, 2017.

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. São Paulo: Malheiros, 2012.

BESSANT, Claire. Data protection, safeguarding and the protection of children's privacy: exploring local authority guidance on parental photography at school events. **Information & Communications Technology Law**, v. 23, n. 3, p. 256-272, 2 set. 2014. Informa UK Limited. http://dx.doi.org/10.1080/13600834.2014.973178. p. 271.

BRASIL. Superior Tribunal de Justiça. **AgInt no Recurso Especial n. 1.593.873-SP**. Agravante: Google Brasil Internet Ltda. Relatora: Ministra Nancy Andrighi. Brasília, DF, 10 de novembro de 2016. DJe. Brasília, 17 set. 2019.

CANARIS, Claus-Wilhelm. **Pensamento Sistemático e Conceito de Sistema na Ciência do Direito**. 3. ed. Lisboa: Fundação Calouste Gulbenkian, 2002.

CHEHAB, Gustavo Carvalho. O direito ao esquecimento na sociedade da informação. In: CLÈVE, Clèmerson Merlin. **Doutrinas Essenciais de Direito Constitucional**. São Paulo: Revista dos Tribunais, 2015. p. 563-596.

COLOMBO, Cristiano; FACCHINI NETO, Eugênio. Ciberespaço e conteúdo ofensivo gerado por terceiros: a proteção dos direitos de personalidade e a responsabilização civil dos provedores de aplicação, à luz da jurisprudência do Superior Tribunal de Justiça. **Revista Brasileira de Políticas Públicas**, v. 7, n. 3, 2017.

EBERLIN, Fernando Büscher von Teschenhausen. Sharenting, liberdade de expressão e privacidade de crianças no ambiente digital: o papel dos provedores de aplicação no cenário jurídico brasileiro. **Rev. Bras. Polít. Públicas**, Brasília, v. 7, nº 3, 2017 p. 255-273.

LIMA, Cíntia Rosa Pereira de. Direito ao Esquecimento e Internet: o fundamento legal no Direito Comunitário europeu, no Direito italiano e no Direito brasileiro. **Revista dos Tribunais,** v. 946, p.77-109, ago. 2014.

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

MOREIRA, Rodrigo Pereira; MEDEIROS, Jaquelaine Souza. Direito ao Esquecimento: Entre a Sociedade da Informação e a Civilização do Espetáculo. **Revista de Direito Privado**, v. 70, p. 71-98, 2016

SCHREIBER, Anderson. **Direitos da Personalidade**. São Paulo: Atlas, 2011.

STEINBERG, Stacey B. Sharenting: Children's privacy in the age of social media. **Emory Law Journal, Atlanta**, v. 66, p. 839-884, 2017. Disponível em: <http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1796&context=facultypub>. Acesso em: 21 ago. 2019.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. **Acórdão nº C-131/12**. Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González. Luxemburgo, 2014. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT>. Acesso em: 09 set. 2019.

VIANA, Janile Lima; MAIA, Cinthia MANESES; ALBUQUERQUE, Paulo Germano Barrozo de. O cyberbullying e os limites da liberdade de expressão. **Revista Brasileira de Políticas Públicas**, v. 7, n. 3, 2017.

Submetido em 30.09.2019

Aceito em 07.10.2019