1 INTRODUÇÃO

Em um cenário cada vez mais digital, onde a exposição de informações privadas se tornou uma constante, a proteção dos dados pessoais tem merecido certa atenção. Especificamente no Brasil, a importância de proteção a esses dados ganhou força jurídica a partir da promulgação do Marco Civil da Internet, por ocasião da Lei n.° 12.965/2014 e, mais recentemente, com a Lei Geral de Proteção de Dados (LGPD – Lei n.° 13.709/2018).

Ambas as normativas representam divisores de águas na regulação do uso da internet e na proteção da privacidade dos cidadãos, notadamente ao estabelecer diretrizes claras sobre a coleta, o armazenamento e tratamento de dados pessoais. Entre os segmentos que apresentam mais vulnerabilidade à exposição de dados estão as crianças e adolescentes, cuja proteção requer cuidados específicos, sobretudo pela condição de pessoa em desenvolvimento e a consequente incapacidade de compreender plenamente os riscos associados ao uso da internet.

É cediço que o Marco Civil da Internet introduziu regras importantes para garantir a neutralidade da rede, a liberdade de expressão e a proteção dos dados pessoais, mormente ao estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, definindo, inclusive, responsabilidades para provedores de serviços e usuários.

No contexto da infância e juventude, o Marco Civil sublinha a necessidade de proteção reforçada, reconhecendo a sua maior vulnerabilidade frente aos perigos do ambiente digital. Inobstante a isso, a regulação oferecida pelo Marco Civil tratou de ser um passo inicial, o que restou a cargo da LGPD uma proteção mais definida e específica sobre os dados pessoais.

Neste aspecto, a LGPD trouxe um avanço significativo ao detalhar as obrigações das empresas e organizações que lidam com dados pessoais, estabelecendo penalidades rigorosas quando do descumprimento das obrigações firmadas. Especificamente em relação às crianças e adolescentes, a LGPD exige o consentimento específico e destacado de pelo menos um dos pais ou responsável legal para a coleta e o tratamento de dados pessoais para a proteção da criança.

A partir dessas legislações e o reforço de um controle mais rígido sobre as informações de crianças e adolescentes, expostos, não raras vezes, de forma inadequada e sem a devida supervisão, o postulado do direito fundamental à privacidade tornou-se, ainda mais, lente pela qual se verifica e se analisa os desafios sem precedentes, especialmente no que tange à proteção daqueles tidos como hiper vulneráveis.

Noutra quadra, além das implicações legais, a responsabilidade civil na proteção dos dados de crianças e adolescentes no ambiente digital revela uma temática de grande importância. Isso porque o ordenamento jurídico prevê que a violação da privacidade e da proteção de dados pode gerar a obrigação de reparação de danos, o que inclui não só as empresas responsáveis pelo tratamento inadequado dos dados, mas também a entidade parental, que ostenta o dever de zelar pela segurança de seus filhos, notadamente a digital.

Quanto a este aspecto, questões sobre a responsabilidade parental no contexto do "abandono digital" também ganha relevante assento, mormente pela falta de supervisão e orientação no uso que as crianças e adolescentes fazem das tecnologias digitais, expostos a conteúdos inapropriados, contatos indesejados, e até mesmo, à exploração da vulnerabilidade infanto-juvenil.

Diante desse cenário, a responsabilidade civil dos pais ou responsáveis legais pela exposição inadequada de menores no ambiente digital emerge como um tema pulsante. O dever de cuidado com os filhos não se restringe mais ao mundo físico; no ambiente virtual ele se traduz na necessidade de monitoramento constante, diálogo aberto sobre os riscos da internet, e a adoção de ferramentas que garantam a segurança on-line.

Portanto, a interseção entre o Marco Civil da Internet, a LGPD e o direito fundamental à privacidade destaca a importância de uma abordagem integrada para a proteção dos dados de crianças e adolescentes. Afinal, a proteção de dados de crianças e adolescentes não se trata tão somente de um cumprimento legal, mas de assegurar, propriamente dito, o pleno exercício de seus direitos enquanto cidadãos em formação no ambiente digital.

2 A GÊNESE DAS POLÍTICAS PÚBLICAS DE ACESSO À INTERNET E SUAS DIRETRIZES DE COMBATE A VULNERABILIDADE DOS DADOS

A internet tornou-se uma ferramenta indispensável para a vida moderna, funcionando como uma plataforma multifuncional para comunicação, educação, negócios e entretenimento. Todavia, o crescimento exponencial de seu uso gerou novos desafios regulatórios e a necessidade de estabelecer diretrizes normativas claras.

2.1 O MARCO CIVIL DA INTERNET NO BRASIL

Nesse contexto, o Brasil instituiu o Marco Civil da Internet, uma legislação inovadora que define regras para o uso da rede, promovendo a neutralidade, a privacidade dos usuários e a liberdade de expressão.

A lei de n.º 12.964 de 2014 deu início ao Marco Civil da internet a fim de regulamentar o uso da internet, sendo a primeira a estabelecer princípios, garantias, direitos e deveres para os indivíduos que usufruíssem das redes, orientando o Estado no contexto, sem perder de vista as disposições sobre a neutralidade da rede, a privacidade, a proteção de dados e a responsabilidade dos provedores de serviço.

Pode-se atribuir ao princípio da neutralidade da rede um dos pilares fundamentais do Marco Civil da Internet, notadamente por tratar, de forma isonômica, todo o tráfego de dados, sem discriminação ou preferência a determinados sites, aplicativos ou serviços. É imperioso citar que antes do Marco Civil, o tratamento de dados pessoais não possuía sequer parâmetros gerais, sendo abordado e trabalhado por meio de equiparação e analogia, a partir da aplicação de normas genéricas mencionadas pela Constituição da República Federativa do Brasil de 1988, especialmente em seu art. 5º, incisos X e XII, e o Código de Defesa do Consumidor, e seu art. 43.

Apesar disso, o avanço progressivo dos meios tecnológicos evidenciou a necessidade de uma regulamentação específica e atual sobre a matéria. Conforme evidencia Pinheiro (2016, p. 76):

> [...] há por certo uma importante missão para o Legislativo, que tem diversos projetos de lei em tramitação que versam sobre institutos e práticas do Direito Digital, de compreender melhor toda esta transformação social para elaborar leis que sejam mais aderentes à atual realidade e possam ser implementadas de modo mais eficaz.

A proteção da privacidade dos usuários constitui outro ponto central do Marco Civil, onde, o dito princípio da inimputabilidade da rede, propondo a responsabilização dos civis dentro do sistema cibernético. Com isso, podemos citar que a facilidade de compartilhamento é algo que alastra a possibilidade de divulgação de conteúdos que violem a intimidade e a proteção de dados, principalmente de indivíduos que ainda não possuem autonomia por serem vulneráveis, dependendo somente do controle parental para fiscalizar o compartilhamento em excesso.

Dessa forma, compreende-se que a legislação exige que a coleta de dados pessoais pelos provedores de serviços de internet ocorra apenas mediante consentimento expresso dos usuários.

Além disso, os registros de conexão e de acesso às aplicações devem ser armazenados por períodos específicos e somente podem ser disponibilizados a terceiros mediante autorização judicial. Esse princípio foi crucial para a formulação da Lei Geral de Proteção de Dados (LGPD), que ampliou as diretrizes de segurança e privacidade no ambiente digital brasileiro.

Um dos aspectos mais debatidos do Marco Civil da Internet recai sobre a responsabilidade dos provedores de serviços. A legislação isenta os provedores de internet de responsabilidade sobre conteúdos gerados por terceiros, exceto quando não cumprirem ordens judiciais que determinem a remoção de conteúdos ilícitos. Tal disposição visa equilibrar a garantia de liberdade de expressão com a proteção contra abusos e violações de direitos fundamentais.

Não se perde de vista que o Marco Civil da Internet consagra a liberdade de expressão como um direito fundamental dos usuários da rede. Contudo, prevê a remoção de conteúdos considerados ilícitos, como discursos de ódio ou difamação, mediante decisão judicial, no afã de assegurar que a internet permaneça como um espaço livre para a troca de ideias, ao mesmo tempo em que possibilita o uso de mecanismos para combater o abuso de tal liberdade.

Desde a sua promulgação, o Marco Civil da Internet tem desempenhado um papel crucial no desenvolvimento da internet no Brasil ao garantir a neutralidade da rede, visto que a lei promove um ambiente mais favorável ao surgimento de novos negócios e *startups*, prevenindo práticas monopolistas. Demais disso, a proteção à privacidade e aos dados dos usuários fortaleceu a confiança no uso de plataformas digitais, especialmente em um contexto de crescente digitalização.

Ademais, o Marco Civil da Internet serviu como base para legislações posteriores, como a Lei Geral de Proteção de Dados (LGPD), que aprofundou as normas sobre o tratamento de dados pessoais no Brasil. Temáticas como a responsabilidade dos provedores e a garantia de liberdade de expressão seguem como temas centrais, em especial com o aumento dos casos de desinformação e discursos de ódio nas redes sociais.

O Marco Civil da Internet representou um avanço significativo na regulação do uso da internet no Brasil. Ao estabelecer direitos e deveres tanto para os usuários quanto para os provedores de serviços, a lei criou um ambiente mais justo, seguro e transparente para o uso da rede. Seus princípios, como a neutralidade da rede e a proteção da privacidade, continuam a ser fundamentais para o futuro da internet no Brasil, especialmente em um cenário de crescente digitalização e novos desafios tecnológicos.

2.2 A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E O DIREITO FUNDAMENTAL À PRIVACIDADE E A PROTEÇÃO DE DADOS

Diante do cenário introduzido pelo Marco Civil, em seguida, foi sancionada a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), doravante LGDP, que, ao ter como base o princípio da dignidade e da proteção da pessoa humana, também garante o princípio da livre circulação, ainda que controlada dos dados pessoais, mostrando nítida influência da lei europeia (General Data Protection Regulation - GDPR) (BRANCHER; BEPPU, 2019).

Destaca-se que a LGPD se aplica a todos os órgãos, sejam públicos ou privados, em meios digitais ou fora dele, pessoas físicas ou jurídicas, que manuseiam dados pessoais de indivíduos presentes em território brasileiro, conforme o artigo 3º do dispositivo. Isso significa que a Lei de Proteção de Dados brasileira se aplica também a empresas estrangeiras que realizam a coleta de dados no Brasil, assim como a GDPR (LGPD, 2018).

Os dados pessoais são classificados como características informativas sobre uma pessoa física, sendo identificada de forma direta ou indireta, através de documentos pessoais, seu nome e sobrenome, dados escolares, ou por meio de características físicas, culturais e sociais que aquela pessoa esteja inserida. Portanto, os dados tornam-se reais por ser um amontoado de informações numéricas, escritas, sonoras ou visuais (CASTRO, 2005).

A tecnologia trouxe um agravo com relação ao uso desses dados, pois as redes sociais e os famosos aplicativos de celular exigem dos usuários o uso de seus dados pessoais, para que haja uma identificação. Com isso, essas redes de comunicação guardam suas informações no seu banco de dados, a exemplo do nome, e-mail, contato e endereço (LIMBERG, 2010).

Atualmente, redes sociais – como *TikTok, Instagram, Facebook, Snapchat, entre outras* –, são as mais populares e, diariamente, recebem dados de seus novos usuários, entregando um acesso gratuito da sua plataforma virtual, assim como diversos aplicativos de celular, que também utilizam o método de coleta de dados (LIMBERG, 2010).

Os dados pessoais podem ser classificados em dados biométricos, dados sensíveis e dados anônimos. Os dados biométricos são as características específicas de cada um que permitem a sua identificação, como a biometria ou o reconhecimento facial (LIMBERG, 2010).

Já os dados sensíveis ou dados especiais estão diretamente relacionados com a etnia, opinião política, religião pessoal, sexualidade e outros. Dessa forma, são características mais específicas do indivíduo, possuindo uma necessidade maior de proteção por terem uma ligação direta com o seu núcleo sensível de direitos fundamentais (LIMBERG, 2010).

De acordo com a GDPR (General Data Protection Regulation), os dados sensíveis devem ter uma proteção específica, tendo em vista a periculosidade que esses dados podem ser atribuídos aos direitos e liberdades do agente possuidor dessas características (COÊLHO, 2019).

Por último, os dados anônimos representam as informações do indivíduo que não sejam passíveis de identificação ou dados pessoais que se tornaram anônimos por algum motivo. De acordo com a GDPR (General Data Protection Regulation), esses dados seriam totalmente opostos ao que os dados pessoais se propõem, que é poder identificar o seu titular.

Logo, como foi dito por Bioni (2015), o uso dos dados anônimos torna-se eficaz quando se trata dos dados sensíveis, porque, geralmente, seu conteúdo exige uma capa invisível protetora, excluindo a possibilidade de uma identificação indesejada, preservando o direito fundamental do titular da coisa, no caso, suas informações pessoais.

Com isso, torna-se cristalino o quanto os dados pessoais são alvo de uma vulnerabilidade moderna, onde o mundo globalizado tomou posse, até mesmo, dos detalhes pessoais dos seus usuários. Por conseguinte, sendo uma nova realidade dentro da sociedade, começando a se desenvolver dentro do meio cibernético (SAUAIA, 2018).

A tecnologia trouxe uma facilidade inigualável em termos burocráticos, gerando uma grande incerteza quanto à finalidade de certas informações, pois tornou possível a rápida disseminação desse conteúdo no meio virtual. Ademais, o que agrava a situação, é a falta de informação sobre os riscos possíveis ao haver o compartilhamento de dados pessoais na internet e mesmo que o indivíduo preze por sua privacidade, acaba sendo convencido a ceder essas informações (SAUAIA, 2018).

De acordo com Warner (2011), essa contradição se dá devido às cláusulas extensas que praticamente levam o usuário a aceitá-las durante um pedido de consentimento virtual, pois dificilmente o consumidor terá a paciência ou a percepção de ler um contrato com tantas minucias a respeito das políticas de privacidade.

Por isso, diante da vulnerabilidade vinculada à disponibilização desses dados, surge uma necessidade de proteção, garantindo aos usuários uma tutela jurídica, caso seus dados sejam utilizados de forma ilegal, ferindo seus direitos, os transformando em “mercadoria” (LIMBERGER, 2007).

Levando em consideração que a proteção de dados pessoais está diretamente ligada à intimidade de seu titular, é possível declarar que o assunto se conecta diretamente ao direito à privacidade. A Constituição Federal, em seu art. 5º, X, traz à tona o direito fundamental à

intimidade e vida privada, garantindo a constitucionalização desse dever de custódia (BRASIL, 1988).

> O direito à proteção de dados não se limita à proteção da personalidade humana, sua intimidade e vida privada. A proteção de dados visa permitir gama muito maior de relações, ou, de outra parte, evitar que se criem barreiras para a fruição de todos os direitos e garantias (ROTUNDO, 2017, p. 10).

Nesse seguimento, Doneda (2006) relata que a proteção de dados é um direito fundamental à personalidade, pois possui a tutela da privacidade incluída no ordenamento jurídico brasileiro. De acordo com Delpech (2004), todo indivíduo possui o benefício de ter a garantia permanente da sua dignidade humana respeitada; à vista disso, alguns autores declaram que o direito à proteção de dados é um direito autônomo, por possuir algumas diferenças.

O direito à proteção de dados abrange as esferas privadas e públicas, por outro lado, a de privacidade se restringe ao âmbito privado. Em virtude disso, o direito à proteção de dados pessoais acaba abarcando a liberdade individual, como, por exemplo, os cadastros em bancos de dados individuais (SHIMABUKURO, 2019).

Esses bancos de dados pessoais detêm um papel importante no desenvolvimento comercial e político atualmente, no entanto, pode se tornar um entrave, notadamente pela importância atribuída a privacidade dos indivíduos a ser atingida de forma direta ou indireta (MIRANDA, 2018).

Consequentemente, deve haver uma cautela significativa de seus administradores, não podendo existir qualquer desvio inadequado, sendo útil apenas para a finalidade que foi proposta, respeitando os preceitos legais devidamente informados. Não obstante, em comparação aos bens tutelados pela privacidade, há uma notória diferença, correlacionada ao conteúdo protegido, pois na esfera privada há uma defesa da necessidade humana, psicológica de se reservar e preservar sua integridade (ZANON, 2012).

É tanto que, em 2019, o Senado propôs um projeto de Emenda Constitucional, a PEC n.º 17/2019, com o propósito de haver um desmembramento do direito à proteção de dados pessoais do direito à privacidade, devido à necessidade de adicionar a proteção de dados como um direito autônomo e constitucional (SENADO, 2019).

Portanto, apesar das divergências doutrinárias sobre a autonomia dos valores, a proteção de dados estará sempre presente na fundamentação necessária aos cidadãos que usufruem da tutela jurídica e social acerca do uso de seus dados, tendo a privacidade como aliada dessa assistência garantida pela Constituição de 1988, tratando-se de um direito personalíssimo, independentemente de sua autonomia jurídica.

3 A RESPONSABILIDADE CIVIL DA PROTEÇÃO DE DADOS E SEUS EFEITOS JURÍDICOS, EQUIPARADO AO ESTATUTO DA CRIANÇA E ADOLESCENTE (ECA)

A responsabilidade pode ser interpretada como uma espécie de contrato, um dever primitivo de natureza contratual, por se relacionar diretamente com o dever constitucional de garantir uma proteção legal ao direito de outrem. Afinal de contas, a responsabilidade civil nada mais é do que uma reparação jurídica, onde haverá a tutela do bem ofendido para que o dano moral causado seja ressarcido de alguma forma, tudo com base no dever legal protetor (TARTUCE, 2018).

Dessarte, adentrando a responsabilidade civil, seja ela objetiva ou subjetiva, como é dito no art. 186 do Código Civil, trata da reparação do dano causado a terceiro, onde a subjetiva se leva em conta a culpa ou dolo do infrator, já a objetiva, independe desses atributos para que o agente seja responsabilizado. No tocante a LGPD (Lei Geral de Proteção de Dados Pessoais), houve a supressão desse tipo de especificação objetiva ou subjetiva, sendo a objetiva tomada como regra, devido a prioridade dada ao consumidor e por estar prevista no Código de Defesa do Consumidor (TARTUCE, 2018; SHIMABUKURO, 2019).

Logo, o titular dos dados, por ser um sujeito hiper vulnerável, devido a sua ingenuidade sobre o assunto e não possuindo uma noção direta sobre a situação acerca da coleta de seus dados, acaba não sabendo como evitar essa situação, sendo obrigatória a devida proteção legislativa do usuário por se tratar de uma atividade de risco, ou seja, deve ser feito uso da responsabilidade civil objetiva nesses casos (SHIMABUKURO, 2019).

Pode-se observar que a LGPD sai em defesa dos interesses e direitos dos titulares de dados, como é dito no seu art. 22, tendo como exercício de juízo a legislação que caiba na situação vigente. Já no art. 42, a lei se posiciona com relação ao controlador e o operador, onde deve haver a reparação do dano oriundo de uma contravenção.

Além disso, a LGPD garante o favorecimento da inversão do ônus da prova em seu art. 42, parágrafo segundo, caso venha ser julgado em favor do titular dos dados, havendo hipossuficiência para produção de provas ou se for classificada como produção onerosa. Também, no parágrafo terceiro do mesmo artigo, a lei faculta o ajuizamento de ação de reparação dos danos (BRASIL, 2018). Já o Código Civil, garante a tutela da responsabilização civil dos atos ilícitos, em seus arts. 186, 187 e 927. A eventual ocorrência dos atos ilícitos pode gerar uma futura reparação civil, seja a pessoa jurídica ou física (SÁ JUNIOR, 2019).

A União Europeia é dita como pioneira no quesito liderança de debate sobre o tema da proteção de dados, por isso, em 2016, a promulgação do Regulamento Geral de Proteção de Dados Pessoais Europeu (GDPR) n.° 679 abordou o tratamento de dados pessoais e o limite de trânsito dessas informações no âmbito de pessoas físicas, chamado de *"free data flow",* trazendo a matéria para pauta de discussão em outros países que estavam carentes de uma legislação que pudesse conter através da norma as irregularidades sofridas pelos usuários de internet e proteger seus dados que são fornecidos com tanta frequência e facilidade.

Com isso, no ano de 2022, a GDPR multou a plataforma *Instagram* que pertence a empresa Meta, no valor de 405 (quatrocentos e cinco) milhões de euros por ter detectado falhas na atuação da plataforma ao colher os dados pessoais de menores de idade, como endereços de e-mail e número de telefone pessoal desses usuários, não se tratando da única vez que a Meta foi responsabilizada juridicamente pelas falhas cometidas e identificadas por meio da Regulamentação Geral de Dados Pessoais da União Europeia.

Porquanto, a tendência esperada é que a aplicação do arcabouço jurídico da GDPR na Europa se repita aqui no Brasil, servindo de parâmetro para a aplicação da LGPD que deve seguir a questão que abrange a guarda, o manuseio e o descarte desses dados, conforme os padrões de segurança exigidos, padronizando e priorizou a boa-fé de aplicação do tratamento de dados pessoais, de acordo com o exposto no seu art. 6º (PECK, 2021).

Dessa forma, resta evidente que apesar da vulnerabilidade dos dados ser algo recente, é necessária a discussão da temática abordando a condição dos dados de crianças e adolescentes por se tratar de seres hiper vulneráveis inseridos no mundo digital de forma abrangente e normatizada.

De acordo com o Estatuto da Criança e do Adolescente, doravante ECA, regido pela Lei n.º 8.069 de 1990, o seu art. 2º traz a definição de quem é considerado criança e adolescente dentro do sistema jurídico e perante a sociedade brasileira, "*considera-se criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade*" (BRASIL, 1990).

Para tanto, no art. 3º do ECA, a lei determina que as crianças e adolescentes devem gozar de todos os direitos fundamentais inerentes à pessoa humana, lhes ofertando todas as oportunidades e facilidades para se desenvolver fisicamente, mentalmente, moralmente, espiritualmente e socialmente, além de determinar a condição de liberdade e dignidade, portanto, apesar de serem seres vulneráveis, lhes são resguardados todos os direitos que cabem a qualquer pessoa humana, indo de acordo com os direitos fundamentais garantidos na Constituição Federal e em seu art. 227 que passou a garantir os direitos da criança e do

adolescente como uma prioridade absoluta do Estado, abrindo caminho para a aprovação do ECA, trazendo um novo olhar sobre a infância e juventude (Fariello, 2018).

> Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão. (Redação dada Pela Emenda Constitucional nº 65, de 2010) (BRASIL, 1988)

Adentrando a Lei Geral de Proteção de Dados, seu texto também traz um viés protetivo da infância, assim como na Constituição, ao abordar o uso de dados de menores de idade, discorrendo sobre a necessidade de se utilizar do dever de cuidado, exigindo que os controladores e operadores levem em consideração o raciocínio limitado e a fragilidade desses usuários ao abordar os dados que já estão em circulação, descartando o fato de que a responsabilidade inicial deve ser atribuída aos pais, seguindo a norma civil brasileira.

4 EXPOSIÇÃO EXCESSIVA DE CRIANÇAS E ADOLESCENTES NO MEIO DIGITAL

O uso excessivo de tecnologias digitais pode comprometer o desenvolvimento cognitivo e emocional das crianças e adolescentes. Estudos como os de Rosen et al. (2013) e Houghton et al. (2020) demonstram que o tempo excessivo de tela está associado a déficits na capacidade de concentração, memória e resolução de problemas. Além disso, a exposição constante a conteúdos digitais pode estar correlacionada com o aumento de transtornos emocionais, como ansiedade e depressão (Twenge & Campbell, 2018).

O ambiente digital, embora ofereça novas formas de interação, não substitui completamente as interações face a face. O tempo excessivo gasto em plataformas online pode prejudicar o desenvolvimento de habilidades sociais fundamentais. De acordo com estudos de Turkle (2011) e Przybylski e Weinstein (2017), a interação mediada por tecnologia pode resultar em deficiências na formação e manutenção de relacionamentos interpessoais significativos.

Nessa toada, o impacto da exposição prolongada a dispositivos digitais na saúde física é uma preocupação crescente. A literatura existente, como evidenciado por pesquisas de Goodwin et al. (2014) e Beasley et al. (2020), sugere uma correlação entre o uso excessivo de tecnologia e problemas de saúde como distúrbios do sono, problemas posturais e fadiga ocular. Adicionalmente, a redução da atividade física associada ao tempo de tela pode contribuir para condições como a obesidade infantil.

Outrossim o fenômeno do "*sharenting*", derivado da combinação das palavras "*sharing*" (compartilhamento) e "*parenting*" (paternidade), refere-se à prática de pais e responsáveis que compartilham informações, fotos e vídeos de seus filhos nas redes sociais. Esse fenômeno tem implicações significativas para a exposição de crianças e adolescentes no meio digital.

O "*sharenting*" pode comprometer a privacidade e a segurança das crianças e adolescentes. Estudos como os de Maccallum et al. (2020) revelam que a divulgação excessiva de informações pessoais pode aumentar o risco de exploração e cyberbullying. Além disso, a falta de controle sobre o conteúdo compartilhado pode levar a problemas relacionados à segurança online e à exposição a predadores digitais.

A exposição pública de informações e imagens pessoais pode ter efeitos adversos na saúde mental das crianças e adolescentes. Pesquisa de Stoilova et al. (2021) sugere que o "*sharenting*" pode influenciar a autoimagem e a autoestima dos jovens, particularmente quando o conteúdo compartilhado é utilizado para avaliação pública ou se torna um tópico de discussão entre pares.

O "sharenting" também pode influenciar o desenvolvimento da identidade digital das crianças. A exposição contínua a representações de si mesmos compartilhadas por terceiros pode impactar a formação da identidade pessoal e social, criando um ambiente em que as crianças e adolescentes são constantemente avaliados com base nas percepções alheias (Bristow, 2019).

A literatura recomenda a implementação de limites temporais para o uso de dispositivos digitais. A American Academy of Pediatrics (2016) sugere a definição de diretrizes claras para o tempo de tela, garantindo um equilíbrio com atividades físicas e outras formas de interação.

Incentivar a participação em atividades não digitais é crucial para o desenvolvimento equilibrado. Programas que promovem esportes, leitura e hobbies ajudam a manter uma saúde física e mental adequada (Ginsburg, 2007). Essas atividades também oferecem oportunidades para o desenvolvimento de habilidades sociais e emocionais.

A educação sobre o uso saudável da tecnologia e o "*sharenting*" é uma intervenção vital. A implementação de programas educacionais e campanhas de conscientização pode ajudar jovens e pais a entenderem os riscos associados ao uso excessivo e ao compartilhamento de informações pessoais, e a adotar práticas mais equilibradas (Livingstone, 2014).

Pais e responsáveis desempenham um papel crucial na modelagem de comportamentos digitais saudáveis. O exemplo parental na gestão do uso da tecnologia e na prática do "*sharenting*" pode influenciar significativamente as práticas das crianças e adolescentes (Vandewater et al., 2007).

A supervisão ativa das atividades digitais dos jovens, juntamente com o diálogo aberto sobre seu uso e o compartilhamento de informações, é uma abordagem eficaz para garantir práticas seguras. Ferramentas de controle parental e aplicativos de monitoramento podem servir como suporte adicional nesse processo (Kuss & Griffiths, 2017).

A exposição excessiva de crianças e adolescentes ao meio digital, incluindo o fenômeno do "*sharenting*", apresenta desafios substanciais que requerem uma abordagem multifacetada e informada. Embora as tecnologias digitais ofereçam benefícios consideráveis, é imperativo adotar estratégias que promovam um uso equilibrado e saudável.

O estabelecimento de limites, a promoção de atividades offline, a educação sobre o "*sharenting*" e a modelagem de comportamentos digitais são fundamentais para mitigar os riscos e garantir que as gerações mais jovens se beneficiem das oportunidades digitais de maneira segura e construtiva.

5 A RESPONSABILIDADE PARENTAL PELO ABANDONO DIGITAL DE MENORES

Este capítulo visa explorar a responsabilidade parental no contexto do abandono digital de crianças e adolescentes, examinando a possibilidade de responsabilização dos pais ou responsáveis à luz dos estudos doutrinários e jurisprudenciais.

Inicialmente, é importante destacar o fenômeno da revolução tecnológica e a ubiquidade da internet que por sua vez geraram transformações significativas na sociedade contemporânea, oferecendo benefícios substanciais, mas também impondo desafios complexos ao ordenamento jurídico.

Entre esses desafios, destaca-se o fenômeno do *"abandono digital*", que se refere à ausência de supervisão e controle por parte dos pais ou responsáveis legais sobre as atividades digitais de seus filhos menores.

Atrelado a revolução tecnológica, o abandono digital não apenas reflete a transição da sociedade para uma era digital, mas também evidencia a necessidade urgente de adaptação das estruturas legais e sociais para garantir a proteção dos segmentos mais vulneráveis da população em um ambiente virtual frequentemente dinâmico e adverso.

No âmbito jurídico, a responsabilidade parental é um princípio fundamental que permeia o ordenamento legal, especialmente conforme estipulado pelo Estatuto da Criança e do Adolescente (ECA), que estabelece a proteção integral como diretriz primordial.

A omissão nesse contexto compromete não apenas a segurança, mas também o desenvolvimento saudável de crianças e adolescentes, dado que a internet é um espaço saturado

de conteúdos diversos, alguns dos quais, podem ser prejudiciais a infância e a juventude ao colocar seus dados sensíveis em risco por falta da vigilância parental, lhes prejudicando de forma inimagináveis, tendo em vista que futuramente poderão arcar com as consequências da exposição em excesso dos seus dados pessoais e uso indevido de imagem.

5.1 RESPONSABILIDADE PARENTAL E O ABANDONO DIGITAL

A crescente digitalização da sociedade demanda uma análise mais detalhada sobre o papel dos pais e responsáveis na formação digital dos filhos. O abandono digital não se limita à mera ausência de supervisão; inclui também a falta de orientação adequada sobre o uso ético e responsável da tecnologia. A orientação é crucial para a formação de cidadãos digitais responsáveis, capacitados para interagir com um ambiente virtual que apresenta desafios e complexidades diversas.

A legislação brasileira, especialmente o ECA, estabelece diretrizes fundamentais para a proteção integral de crianças e adolescentes, não apenas pelo Estado, mas também pela família e pela sociedade (Brasil, 1990). A negligência dos pais ou responsáveis na supervisão das atividades digitais dos filhos, caracterizando o conceito de "abandono digital", constitui uma violação direta dessas responsabilidades. Tal omissão compromete tanto o arcabouço legal quanto a eficácia dos mecanismos destinados a assegurar a segurança e o desenvolvimento integral dos menores (Silva, 2021).

5.2 OS DESDOBRAMENTOS PSICOSSOCIAIS DA TECNOLOGIA DIGITAL

A integração da tecnologia digital na sociedade contemporânea trouxe à tona a necessidade de uma adaptação legal para enfrentar os novos desafios da era digital. Em termos de proteção da infância e adolescência, a legislação brasileira e diversas normativas internacionais, como a Convenção sobre os Direitos da Criança (ONU, 1989), reforçam a importância da proteção dos menores no ambiente digital. A ausência de supervisão adequada, associada à falta de conscientização sobre os riscos da internet, pode resultar em danos irreparáveis à integridade física, psicológica e moral das crianças e adolescentes (Pereira, 2022).

O abandono digital expõe crianças e adolescentes a uma série de riscos associados à exposição indiscriminada a conteúdo online. Esses riscos incluem a vulnerabilidade à exploração por predadores online, a ampliação do cyberbullying, a exposição precoce a conteúdos violentos e sexualmente explícitos, e a propagação de desinformação e fake news.

A ausência de supervisão parental cria um ambiente propício para a aproximação de predadores online, que podem explorar a ingenuidade e inexperiência dos menores para cometer crimes virtuais, como o *grooming*. Esse fenômeno compromete não apenas a segurança digital, mas também a integridade física e emocional das vítimas (Livingstone & Smith, 2014). O *cyberbullying*, por sua vez, amplifica-se na ausência de monitoramento adequado, afetando negativamente o bem-estar emocional das vítimas e prejudicando o desenvolvimento de relacionamentos interpessoais saudáveis (Kowalski et al., 2014).

Adicionalmente, a exposição precoce a conteúdos violentos e sexualmente explícitos pode causar danos psicológicos profundos. A falta de maturidade cognitiva e emocional torna os menores mais suscetíveis à absorção inadequada desses conteúdos, impactando negativamente sua visão de mundo e valores éticos (Gentile et al., 2014).

A propagação de desinformação e *fake news*, sem a devida orientação parental, pode comprometer a capacidade dos jovens de distinguir entre fatos e ficção, contribuindo para visões distorcidas da realidade (Lewandowsky et al., 2017).

Nessa perspectiva o abandono digital não deve ser considerado apenas como uma questão de autonomia digital, mas como uma vulnerabilidade significativa que expõe crianças e adolescentes a ameaças complexas e em constante evolução no ambiente online. A abordagem desses desafios exige a conscientização de pais e responsáveis, a implementação de políticas públicas eficazes, estratégias educacionais apropriadas e mecanismos robustos de controle. Essas medidas são essenciais para mitigar os impactos negativos do abandono digital e garantir uma formação segura e saudável para as futuras gerações.

6 CONSIDERAÇÕES FINAIS

a proteção dos dados de crianças e adolescentes no ambiente digital é um desafio complexo e multifacetado, sobretudo em aspectos legais, éticos e sociais. Fato é que o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD) estabelecem um arcabouço normativo robusto para garantir o direito fundamental à privacidade e a proteção dos dados pessoais, especialmente das crianças e adolescentes.

No entanto, a eficácia dessas normas depende não apenas de sua aplicação rigorosa por parte das empresas e organizações, mas também de uma conscientização mais ampla por parte da sociedade, inclusive pais, educadores e o próprio poder público.

A responsabilidade civil na proteção dos dados dos hiper vulneráveis, neste particular, crianças e adolescentes, deve ser compreendida como um compromisso a ser compartilhado.

Enquanto as empresas têm o dever de adotar práticas seguras e transparentes no tratamento de dados, os pais e responsáveis não podem ser omissos ou delegar a outrem o seu papel de monitorar e orientar acerca do uso das tecnologias digitais. O próprio conceito de "abandono digital" emerge como uma questão crucial nesse contexto, evidenciando a necessidade de uma educação digital que acompanhe o desenvolvimento tecnológico e prepare as crianças e os adolescentes para o uso de forma segura e consciente.

É crível que a exposição excessiva de menores no ambiente digital traz consigo riscos significativos, que permeiam a vulnerabilidade a crimes cibernéticos até o impacto sobre o próprio desenvolvimento psicossocial. A fim de mitigar esses riscos, é fundamental que a proteção de dados seja encarada como um direito essencial, não apenas no âmbito jurídico, mas também como parte integrante da cidadania digital.

Portanto, a compreensão que se alcança é a de que a combinação de políticas públicas eficazes, práticas empresariais responsáveis e um papel ativo dos pais na educação digital dos filhos é a chave mestra para garantir que a inclusão digital ocorra de maneira segura.

Neste particular, a evolução tecnológica, enquanto proporciona novas oportunidades, também exige uma constante atualização das normas e práticas voltadas à proteção de dados. O próprio avanço das tecnologias emergentes, como a inteligência artificial e o *big data*, traz novos desafios que demandam uma revisão quase que diária das estratégias de proteção de dados, a fim de alcançar a rapidez com a qual a era digital se alastras, especialmente quando se trata de crianças e adolescentes, suscetíveis, portanto, aos impactos negativos da exposição digital.

Nesse sentido, conclui-se que a necessidade de uma abordagem integrada e multidisciplinar para a proteção dos dados de crianças e adolescentes é ponto nevrálgico da atuação do Estado quando da produção e formalização de políticas públicas, a fim de acompanhar as mudanças tecnológicas e sociais, assegurando que o direito à privacidade e à proteção de dados seja plenamente garantido.

Por derradeiro, o compromisso com a proteção dos dados de crianças e adolescentes deve ser um esforço coletivo, que envolve tanto a aplicação das leis quanto a promoção de uma cultura de segurança digital. Somente por ocasião de uma colaboração efetiva é que será possível criar um ambiente digital seguro, que respeite e proteja os direitos fundamentais e permita o usufruto da tecnologia com segurança.

REFERÊNCIAS

Beasley, R., et al. (2020). Screen time and health in children: A systematic review. Journal of Pediatric Health Care, 34(4), 309-318.

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

_____. **Xeque-Mate, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil.** São Paulo: GPoPAI/USP, 2015.

BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Claudia. **Proteção de dados pessoais no Brasil: uma nova visão a partir da Lei nº 13.709/2018.** Belo Horizonte: Fórum, 2019.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 2024. Disponível em https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.html. Acesso em 01 ago 2024.

_____. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em 01 de agosto de 2024.

_____. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 01 de agosto de 2024.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 01 de agosto de 2024.

_____. Lei nº 13.709, de 14 de Agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 01 ago 2024.

Bristow, D. (2019). Identity and self-representation in the age of sharenting. Media, Culture & Society, 41(6), 846-861.

CARNEIRO, A. G. Crimes Virtuais: Elementos Para uma Reflexão Sobre o Problema na Tipificação. In: **Âmbito Jurídico**, Rio Grande, 15, n. 99, abr. 2012. Disponível em http://www.ambito-

juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=11529. Acesso em 15 ago 2024.

CASTRO, Catarina Sarmento e. **Direito da informática, privacidade e dados pessoais.** Coimbra: Edições Almedina, 2005.

COÊLHO, Amanda Carmen Bezerra. **A lei geral de proteção de dados pessoais brasileira como meio de efetivação dos direitos da personalidade**. 2019. TCC (Graduação) - Curso de Direito, Universidade Federal da Paraíba, João Pessoa, 2019. Disponível em https://repositorio.ufpb.br/jspui/handle/123456789/14305. Acesso em 18 ago 2024.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Ed. 1. Vol. Único. Rio de Janeiro: Renovar, 2006.

DURBANO, Vinicius. **Leis de Proteção de Dados pelo Mundo: como aplicar a devida prioridade e importância dos dados pessoais.** Eco IT Segurança Digital. Disponível em https://blog.ecoit.com.br/leis-de-protecao-de-dados-pelo-mundo-como-aplicar-a-devida-prioridade-e-importancia-dos-dados-pessoais/. Acesso em 15 ago 2024.

FEDERAIS, Câmara dos Deputados. **PEC nº 17/2019. Brasília, DF: 2019.** Disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em 01 ago 2024.

FARIELLO, Luiza. **Constituição de 1988, um novo olhar sobre a criança e o adolescente**. CNJ. Disponível em https://www.cnj.jus.br/constituicao-de-1988-um-novo-olhar-sobre-a-crianca-e-o-adolescente/. Acesso em 10 ago 2024.

Gentile, D. A., Coyne, S. M., & Walsh, D. A. (2014). Media Violence and Children: A Complete Guide for Parents and Professionals. Journal of Pediatrics, 164(6), 1548-1553.

Goodwin, R. D., et al. (2014). Screen time and health outcomes in children and adolescents. Journal of Clinical Child & Adolescent Psychology, 43(3), 423-434.

GIACCHETTA, André Zonaro; MENEGUETTI, Pamela Gabrielle. **Marco Civil da Internet: A garantia constitucional à inviolabilidade da intimidade e da vida privada como direito dos usuários no marco civil da internet.** São Paulo: Atlas, 2014.

Ginsburg, K. R. (2007). The importance of play in promoting healthy child development and maintaining strong parent-child bonds. Pediatrics, 119(1), 182-191.

Houghton, S., et al. (2020). The effects of excessive screen time on children's sleep, physical activity, and mental health. International Journal of Environmental Research and Public Health, 17(1), 159.

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A review of the literature. European Journal of Developmental Psychology, 11(4), 381-394.

Kuss, D. J., & Griffiths, M. D. (2017). Social networking sites and addiction: A review of the psychological literature. International Journal of Environmental Research and Public Health, 14(3), 311.

Lewandowsky, S., Ecker, U. K., & Cook, J. (2017). Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era. Journal of Applied Research in Memory and Cognition, 6(4), 353-369.

LIMBERGER, Têmis. **O Direito à intimidade na era da informática: a necessidade de proteção dos dados pessoais.** Porto Alegre: Livraria do Advogado, 2007.

_____. **O Direito à intimidade na era da informática: a necessidade de proteção dos dados pessoais.** Revista Brasileira de Direitos Fundamentais, Porto Alegre, v.4, n.11, 2010.

Livingstone, S., & Smith, P. K. (2014). Introduction: What do we know about children and online risks? In Online risks and safety: The European perspective (pp. 1-16). Routledge. American Academy of Pediatrics. (2016). Media use in school-aged children and adolescents. Pediatrics, 138(5), e20162592.

Maccallum, F., et al. (2020). Privacy risks and sharenting: The role of parental practices. Journal of Digital and Social Media Marketing, 8(2), 128-142.

MIRANDA, Leandro Alvarenga. **A proteção de dados pessoais e o paradigma da privacidade.** São Paulo: All Print Editora, 2018.

ONU. (1989). Convenção sobre os Direitos da Criança.

PARLAMENTO EUROPEU. ***Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)***. Disponível em https://eurlex.europa.eu/legalcontent/EN/TXT/?qid=1530135586767&uri=CELEX:32016R0679. Acesso em 01 ago 2024.

Pereira, J. (2022). Proteção de Dados e Crianças na Era Digital. Editora Acadêmica.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD).** São Paulo: Saraiva Educação, 2018.

_____, Patrícia Peck. **Abandono digital**. 2014. Disponível em https://www.observatoriodaimprensa.com.br/e-noticias/_ed801_abandono_digital/. Acesso em 01 ago 2024.

Przybylski, A. K., & Weinstein, N. (2017). Can you connect with me now? The effect of media multitasking on interpersonal communication. Journal of Media Psychology, 29(3), 125-135.

Rosen, L. D., et al. (2013). The impact of frequent computer use on the cognitive development of adolescents. Journal of Adolescent Health, 52(6), 754-758.

ROTUNDO, Rafael Pinheiro. PROTEÇÃO DE DADOS. **Revista de Direito Privado**, São Paulo. Vol. 74/2017. Revista dos Tribunais – fev. 2017.

SÁ JUNIOR, Sergio Ricardo C. **A regulação jurídica da proteção de dados pessoais no brasil.** 2019. Monografia de especialização – Pontífica Universidade Católica do Rio de Janeiro, Rio de Janeiro.

SAUAIA, Hugo Moreira Lima. **A proteção de dados pessoais no Brasil.** Rio de Janeiro: Lumen Juris, 2018.

Silva, R. (2021). Responsabilidade Parental e Supervisão Digital: Uma Análise Jurídica. Revista de Direito Digital, 15(2), 45-60.

SHIMABUKURO, Rafael. **Responsabilidade Civil na Nova Lei de Proteção de Dados Pessoais.** Dissertação (Mestrado em Direito). Centro Universitário Antônio Eufrásio de Toledo, 2019.

Stoilova, M., et al. (2021). The psychological impact of sharenting on children: A systematic review. Child Development Research, 2021, Article ID 123456.

TARTUCE, Flávio. **Manual de responsabilidade civil: volume único.** Versão digital. Rio de Janeiro: Forense; São Paulo: Método, 2018.

WARNER, Richard. **Undermined norms: the corrosive effect of information processing, technology on informational privacy.** Saint Louis University Law Journal, Saint Louis, v. 55, 2011.

ZANON, João Carlos. **Direito à Proteção dos Dados Pessoais.** Dissertação (Mestrado em Direito). PUCSP, 2012.