

Parte 06

Publicidade digital e a proteção de dados de crianças e adolescentes

1. Crianças *on-line*: orientações da OCDE sobre publicidade digital e consumo

A Organização para Cooperação e Desenvolvimento (OCDE) é organização internacional que tem por objetivo constituir políticas públicas para melhoria da qualidade de vida dos cidadãos, trabalha o estabelecimento de padrões internacionais baseados em evidências científicas e busca de soluções para os desafios sociais, econômicos e ambientais¹.

O foco do trabalho da OCDE é a melhoria do desempenho econômico, a criação de empregos, além do incentivo à educação e o combate à evasão fiscal internacional. São oferecidos fóruns de discussão e centro de conhecimento exclusivos para dados e análises, troca de experiências, compartilhamento de melhores práticas e consultoria sobre políticas públicas e estabelecimento de padrões internacionais.

Há inúmeros estudos e orientações da OCDE em relação ao desenvolvimento da criança, em especial no que diz respeito às políticas públicas educacionais e de saúde. Na mesma linha, há estudos que indicam a necessidade de proteção da infância no ambiente digital que e tocam a publicidade nesse meio.

Em maio de 2011, o órgão publicou as primeiras diretrizes a respeito dos cuidados e das ferramentas relacionadas aos riscos do uso da internet por crianças e adolescentes, denominadas “The Protection of Children Online: risks faced by children online and policies to protect them”. Ainda na mesma linha, em maio de 2020, o órgão emitiu novas diretrizes com o título “Protecting children online an overview of recent developments in legal frameworks and policies OCDE digital economy papers” (documentos anexos).

Os dois relatórios fazem um mapeamento dos riscos a que crianças e adolescentes estão expostos pelo uso das novas plataformas digitais. *Grosso modo*, o órgão divide os riscos em três categorias: i) riscos de tecnologia na internet; ii) riscos relacionados ao consumo; e iii) privacidade da informação e riscos de segurança.

¹ Disponível em: <http://www.oecd.org/about/>. Acesso em: 31/10/2021.

Figure 7. Typology of risks

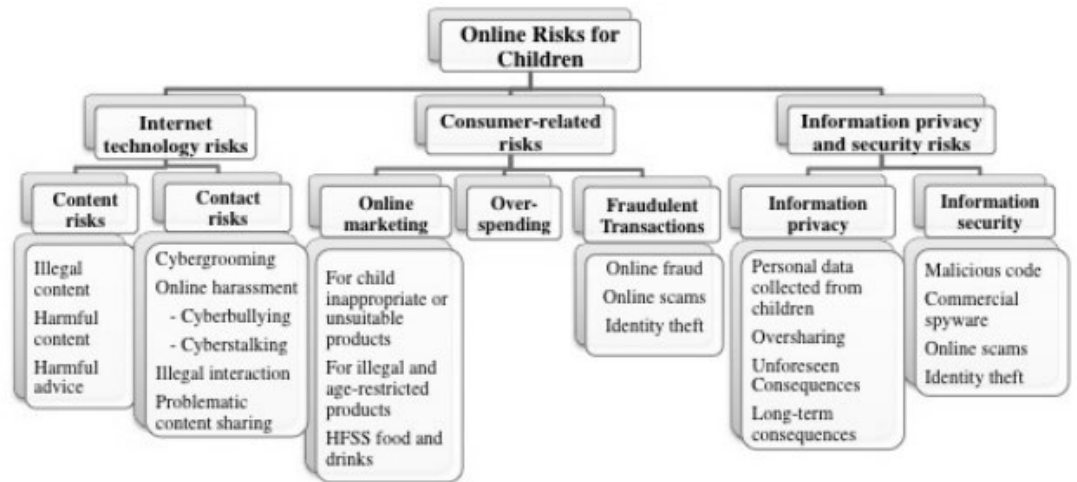


Figura 1 – Typology of risks

Fonte: <http://www.oecd.org/about/>.

Importante notar que os documentos estão baseados em dados coletados no Reino Unido, na Austrália, no Japão e na União Europeia, considerando a idade, o local onde as crianças acessam a rede mundial de computadores (se de casa, da escola, de estabelecimento comercial), entre outras informações.

Apesar de apresentar dados quantitativos e qualitativos que dão base para a pesquisa, o órgão esclarece que a disponibilidade de dados quantitativos varia de acordo com o risco, uma vez que poucos são os dados sobre as interações ilegais, sobre o marketing *on-line* destinado a crianças, especialmente sobre as transações fraudulentas, bem como sobre a segurança da informação e os riscos de privacidade.

Para desenhar a figura acima, foram utilizados especialmente os dados da pesquisa “Revisão de Pesquisas Existentes de Segurança Cibernética Australiana e Internacional” e do estudo “EU Kids Online”, que fornecem informações detalhadas sobre o tema.

Sendo o foco deste trabalho a publicidade infantil, seguiremos para a análise do item que trata das crianças vistas como consumidores na internet. Nessa seara, a OCDE aponta que as crianças estão em risco quando: i) recebem mensagens *on-line* com conteúdo inapropriado, dirigido ao público adulto (como publicidades relacionadas a

bebidas alcoólicas ou que ofereçam serviço de namoro *on-line*); ii) estão expostas a conteúdo publicitário sem a correta identificação da mensagem publicitária; e iii) são expostas a conteúdo que explore sua inexperiência, criando risco econômico para si e sua família (como nas situações de fraude).

1.1. Riscos relacionados ao consumo

1.1.1. Publicidade de produtos e serviços adultos

A publicidade *on-line* relacionada a produtos e serviços restritos a adultos, como álcool, cigarro e medicamentos é constante preocupação diante do risco que representa às crianças. Isso porque, especialmente para adolescentes, pode ocorrer promoção e venda de produtos não apropriados para tal idade.

Embora haja restrições de idade para a compra desses produtos *on-line*, elas não necessariamente são respeitadas pelos compradores. O estudo traz como exemplo uma pesquisa feita nos Estados Unidos da América em 2006, indicando que mais de 70% dos adolescentes tentaram comprar cigarros *on-line* com sucesso; outra pesquisa de 2002 descobriu que apenas 2,2% de 1.689 adolescentes que fumaram compraram seus cigarros *on-line*. Da mesma forma, a promoção e a venda de produtos ilegais como drogas e substâncias entorpecentes na internet representam um risco principalmente para adolescentes.

1.1.2. Publicidade dirigida ao público infantil inserida em conteúdo *on-line*

O marketing *on-line* voltado ao público infantil, ou que seja vinculado à página da *web* destinada ao público infantil, pode ser considerado um problema, visto que, na maioria das vezes, inexistente uma separação entre conteúdo e publicidade, não deixando claro o conteúdo publicitário do anúncio para as crianças.

Segundo os documentos da OCDE, para menores de idade, especialmente crianças pequenas, conteúdos comerciais são de difícil identificação, especialmente se comparados aos anúncios destinados ao público adulto, uma vez que a criança não tem capacidade para fazer críticas ao conteúdo por ela recebido, tornando-a extremamente vulnerável às influências do marketing digital.

Advergame é um exemplo de técnica de marketing controversa que mistura publicidade com jogos ou vídeos *on-line*. Segundo estudo citado no trabalho da OCDE, crianças não têm compreensão suficiente de como o conteúdo da internet é produzido e financiado, o que traz maior dificuldade em avaliar criticamente as mensagens publicitárias. O estudo está fundamentado em análise feita pelo Departamento do Reino Unido para Crianças, Escolas e Famílias e pelo Departamento de Cultura e Mídia e Sport.

Por esse motivo, muito se tem questionado a respeito do uso de publicidade incorporada e *branding* comercial em *sites* voltados para crianças; além disso, discute-se a partir de que idade as crianças deveriam ser submetidas a práticas de marketing *on-line*.

1.1.3. Spam, banners e e-mails

O estudo revela que existe preocupação relacionada ao conteúdo de produto ou serviço promovido por algumas publicidades, que podem expor crianças a riscos ainda maiores. Nesse sentido, conteúdos inadequados às crianças, tais como *banners* ou *e-mails* contendo *spam* de cunho sexual, ou, ainda, promoção de jogos, serviços de namoro, entre outros, podem provocar a curiosidade do menor, levando-o a ter acesso a conteúdo impróprio e ocasionando até perdas financeiras para a família².

1.1.4. Publicidade de alimentos e bebidas com altos índices de açúcar, sal e gordura

Outra preocupação trazida pelo documento diz respeito ao marketing de produtos alimentícios com altas taxas de açúcar, sal ou gordura (os chamados alimentos HFSS pela OCDE – *high in fat, sugar and salt*), visto que são considerados um grande risco para a saúde da criança, podendo ser um verdadeiro incentivo à obesidade infantil.

Essa questão tem sido discutida e regulamentada em muitos países tanto na televisão quanto em *websites* que tenham como público-alvo as crianças, especificamente com medidas contra o marketing desses produtos.

1.1.5. Tempo *on-line*

² Um estudo do Conselho Nacional de Consumo Britânico e Conselho Internacional sobre Comércio Infantil indica que 9% da publicidade é destinada aos jogos e 4%, aos serviços de namoro *on-line*. Além disso, anúncios *pop-up* de pornografia são a principal fonte de conteúdo explícito, acessado por crianças que não percebem a temática do *pop-up* ao clicarem em seu conteúdo.

O documento cita outro problema enfrentado pela sociedade: o tempo gasto por crianças e adolescentes na internet. Além de ser prejudicial ao desenvolvimento social desse público, os serviços *on-line* podem trazer gastos exacerbados aos pais. Como exemplo, cita a inscrição em serviços *on-line* com taxas mensais ou o gasto em jogos, quando os menores têm acesso aos meios de pagamento *on-line*.

Aponta também o fato de que ainda não existem informações suficientes sobre quantos são os *sites* que condicionam a navegação em jogos a uma taxa de inscrição, nem mesmo quanto seriam os gastos dessas crianças e adolescentes em tais ambientes.

1.1.6. Transações fraudulentas

O estudo aborda, ainda, o controle de fraudes e transações enganosas envolvendo crianças e adolescentes e as vendas a eles submetidas. Sugere que o tema deve ser alvo de discussões e de forte regulamentação no futuro próximo.

Esbarramos, nesse contexto, em outra questão envolvendo o risco de fraude a que as crianças estão submetidas, quando em um ambiente virtual: diante de uma contratação *on-line*, a criança não recebe o produto ou serviço pelo qual pagou ou, ainda, contrata-o sem saber das condições de pagamento.

As transações fraudulentas podem ocorrer quando as crianças celebram um contrato de vendas a distância, mas, tendo pagado, não recebem o produto/serviço ou efetivam assinaturas sem conseguir o cancelamento do serviço. Um exemplo notório no setor de telefonia móvel é o *download* de *ringtones* para telefones celulares. As crianças podem não perceber que pagam custos adicionais ou mesmo que tenham assinado um serviço cujas taxas são regularmente debitadas em cartões telefônicos pré-pagos³. Obviamente, o mesmo pode ser dito dos aplicativos de celulares.

As ofertas desses aplicativos nem sempre são claras em relação aos pagamentos e assinaturas, além de os valores serem diretamente debitados no cartão de crédito cadastrado para pagamento da conta telefônica, faltando aos menores conhecimento sobre os mecanismos de pagamento de um cartão de crédito.

Os riscos econômicos são agravados pela inexperiência das crianças, o que as torna alvos fáceis para fraude e golpes no ambiente virtual. Menores que ainda não

³ Em 2008, 23,7% dos adolescentes belgas declararam ter contratado serviços de *ringtones* sem saber das condições de pagamento.

possuem conta em banco ou cartão de crédito são menos propensos a incorrer em perdas financeiras imediatas. No entanto, ainda podem ser vítimas de utilização indevida dos dados que podem resultar em registros de crédito falsos.

1.2. Riscos relacionados a informações e dados pessoais

Outro risco relatado pela OCDE diz respeito ao compartilhamento de dados pessoais na internet. Nesse sentido, as crianças são um grupo particularmente vulnerável, visto sua capacidade reduzida de prever perigos e consequências da exposição de suas informações no meio digital.

1.2.1. Privacidade das informações das crianças

As crianças correm riscos relacionados à privacidade das informações quando seus dados são coletados sem que percebam, através de *cookies*, ou ainda por meio da contratação de serviços *on-line*. Assim como o comportamento dos pais e responsáveis, as crianças aprovam os termos de privacidade dos serviços *on-line* sem fazer a leitura (e compreender todos os seus termos), já que, muitas vezes, são longos e escritos em linguagem técnica o que os torna ainda mais difíceis de serem compreendidos pelas crianças.

Nesse sentido, os serviços *on-line* populares entre crianças quase sempre falham em oferecer procedimentos que assegurem aos pais as informações quanto ao tratamento dos dados de seus filhos, bem como em obter autorização expressa para tanto. Essa situação dificulta o controle dos pais no tratamento de dados dos filhos em meio digital.

1.2.2. Informação pessoal como *commodity*

As informações pessoais tornaram-se uma espécie de *commodity* no meio digital, e essa também é uma realidade para as crianças. O estudo trazido pela OCDE⁴ aponta que 95% (noventa e cinco por cento) dos adolescentes britânicos estão cientes desse fato e demonstram preocupação com as informações coletadas por *websites*. Além disso, ainda

⁴ OECD (2011-05-02), “The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them”, OECD Digital Economy Papers, No. 179, OECD Publishing, Paris. <http://dx.doi.org/10.1787/5kgcjjf71pl28-en> p. 27

de acordo com o documento, de quarenta *websites* constantemente acessados por crianças, quase dois terços requerem dados pessoais para acesso e navegação⁵.

Nesse contexto, algumas campanhas publicitárias, com objetivo de atingir o seu público-alvo, têm como forma de cativar as crianças o uso de jogos, questionários e outros conteúdos, que acabam coletando informações pessoais (da criança e de sua família), muitas vezes sem requerer o consentimento dos pais. A possibilidade de ganhar um prêmio ou receber conteúdo *on-line* gratuito é, muitas vezes, a motivação para que crianças forneçam seus dados.

Dessa forma, o documento ressalta a maior vulnerabilidade das crianças em fornecer seus dados em meio digital. Isso porque, diante da sua percepção ainda imatura sobre a vida, é extremamente difícil para elas compreenderem a intenção comercial e os riscos nela envolvidos quando do fornecimento de dados pessoais⁶.

Por conseguinte, o grande desafio nesse contexto é informar adequadamente tanto os pais quanto as crianças sobre o propósito e a extensão do uso desses dados, além de não permitir qualquer tipo de utilização de dados sem o conhecimento e a permissão dos pais ou responsáveis.

1.2.3. Compartilhamento de dados pessoais e sociabilização em meio *on-line*

Conforme o relatório da OCDE, estudos recentes apontam que crianças consideram os contextos da vida *on-line* e *offline* parte de uma mesma realidade: isso porque elas usam a internet primariamente como forma de socializar com pessoas que já conhecem pessoalmente, compreendendo o mundo *on-line* um espaço privado de atividade social entre seus pares.

Uma forma muito utilizada de compartilhar informações pessoais nessa faixa etária se dá por meio de mídias sociais, plataformas de *blog* e outros meios e aplicações comuns ao cotidiano. Através da postagem contendo informações, imagens e vídeos, essas crianças compartilham uma gama de informações, não só sobre elas, como também sobre seu meio social e sua família.

⁵ Em 70%, é requerido o nome; em 53%, o endereço de e-mail; em 43%, a data de nascimento; em 40%, o código postal; em 24%, o endereço residencial; em 24%, o telefone celular.

⁶ Um estudo trazido pelo Escritório Australiano Comissário de Privacidade (Australian Office of the Privacy Commissioner) indicou que australianos jovens são mais suscetíveis em prover dados pessoais em detalhes em vista de receber algum desconto ou prêmio *on-line*. Ver: OECD (2011-05-02), "The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them", OECD Digital Economy Papers, No. 179, OECD Publishing, Paris. <http://dx.doi.org/10.1787/5kqcf71pl28-en> p. 27

Nesse sentido, elas podem presumir, de forma incorreta, que todas as informações submetidas ao universo digital são restritas às pessoas imediatamente próximas a elas, sem contar com a possibilidade de ter seus dados compartilhados com uma imensidão de pessoas.

Dessa forma, existe o risco de crianças concederem informações *on-line*, o que pode colocá-las em situações de risco. Tal risco advém da sensação de pertencimento quando presentes nas redes sociais. Dados mostram que o uso dessas redes por jovens é cada dia menos cuidadoso e cresce aceleradamente⁷.

Nesse contexto, estudos demonstram que, apesar de jovens acreditarem ter privacidade na vida *on-line*, um número grande deles compartilha, cada vez mais, suas informações pessoais nas redes. De acordo com dados trazidos pelo estudo⁸, entre 2000 e 2005 a porcentagem de jovens americanos que compartilha informações pessoais nas redes cresceu cerca de 24% (vinte e quatro por cento). Ainda nesse sentido, outro estudo americano⁹ concluiu que 81% (oitenta e um por cento) dos jovens inscritos na rede MySpace postavam com frequência fotos suas, e que, desses jovens, 93% (noventa e três por cento) indicavam sua cidade natal em tais postagens.

Ressalta-se ainda que, de acordo com informações do relatório da OCDE, apesar de muitas mídias sociais como Facebook, Bebo e MySpace requisitarem idade mínima (classificação etária) de 13 (treze) anos para o registro na rede, um número crescente de crianças abaixo dessa idade tem criado contas nas mencionadas redes¹⁰.

Nesse sentido, a falsa sensação de privacidade que a opção de perfis fechados dá nessas redes sociais faz com que os jovens se sintam cada vez mais seguros para postar

⁷ De acordo com a pesquisa, o uso das redes sociais pelos adolescentes é bem conhecido pela sociedade atual. Em 2007, 51% dos adolescentes americanos criaram um perfil em alguma rede social e 21% fazem uso regular dessa plataforma. Nesse sentido, o número é maior entre meninas (69% de meninas contra 50% de meninos, com idade entre 15 e 17 anos). O uso de redes sociais aumenta conforme a criança cresce: 27% das crianças têm entre 8 e 11 anos, 55% têm entre 12 e 15 anos e 67% têm entre 16 e 17 anos.

⁸ De acordo com Wolak, 2006, citado em ISTTF, 2008, Appendix C, p. 40. Vide: OECD (2011-05-02), "The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them", OECD Digital Economy Papers, No. 179, OECD Publishing, Paris. <http://dx.doi.org/10.1787/5kgcjf71pl28-en> p. 28

⁹ De acordo com Pierce, 2007, cited in ISTTF, 2008, Appendix C, p. 40. Vide: OECD (2011-05-02), "The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them", OECD Digital Economy Papers, No. 179, OECD Publishing, Paris. <http://dx.doi.org/10.1787/5kgcjf71pl28-en> p. 28

¹⁰ No Reino Unido, em 2009, 22% dos usuários de internet disseram ter uma rede social, um aumento de 16% comparado a 2008 (Ofcom, 2010, p. 5, 74). Entretanto, o número de jovens usuários que tornaram o perfil privado tem aumentado: 83% dos usuários entre 8 e 12 anos afirmam ter bloqueado a visualização de usuários desconhecidos no perfil, comparado a 67% dos jovens na mesma faixa de idade em 2008. Vide: OECD (2011-05-02), "The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them", OECD Digital Economy Papers, No. 179, OECD Publishing, Paris. <http://dx.doi.org/10.1787/5kgcjf71pl28-en> p. 28

fotos, vídeos e informações pessoais. Esse fato também traz uma falsa sensação de segurança aos pais, já que 93% (noventa e três por cento) dos pais de crianças que utilizam essas redes estão cientes das referidas postagens¹¹.

Ressalta-se, nesse contexto, que as informações pessoais de usuários podem ser postadas por outras pessoas. Como exemplo, citamos as *tags*, que são marcações de outros indivíduos em fotos, vídeos e informações em perfis variados. Tal prática é comum entre jovens, e, na maior parte das vezes, não é necessária a permissão da pessoa “marcada” para que as informações apareçam em seu perfil¹².

Ainda nessa toada, importante destacar que o uso de informações e dados pessoais de crianças na internet pode também ser um risco em relação a terceiros com intenções criminosas. Segundo estudo trazido pela OCDE, em 2006 a Comissão Federal do Comércio dos Estados Unidos reportou 1.498 denúncias de vazamento de dados de pessoas menores de 18 (dezoito) anos; isso representa 2% de todas as ações criminosas envolvendo roubos de identidade naquele ano¹³.

Destaca-se que os dados de crianças e adolescentes podem ser usados também como forma de conhecer os locais acessados por eles, dando informações a respeito de sua casa, escola e locais de lazer, não só por outros indivíduos com intenções maliciosas, mas também pelos próprios *websites*, tais como Facebook, Google e outros, que utilizam essas informações para finalidades diversas. No caso do uso de celulares, tal fato pode ser ainda mais evidente, gerando o rastreamento de todos os passos dados pela criança, sem qualquer limite em relação à sua privacidade.

1.2.4. O paradoxo da proteção de dados

¹¹ De acordo com Pew Internet & American Life Project, 2007, p. 3. Vide: OECD (2011-05-02), “The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them”, OECD Digital Economy Papers, No. 179, OECD Publishing, Paris. <http://dx.doi.org/10.1787/5kgcjf71pl28-en> p. 28.

¹² Ainda nesse sentido, estudos comprovam que pouco mais de 40% dos jovens tiveram suas fotos postadas em perfis diversos sem sua permissão (Dooley et al., 2009, p. 141). Outro estudo revela ainda que 6% dos jovens reportam fotos embaraçosas postadas em redes sociais sem suas devidas permissões (Lenhart, 2007, cited in ISTTF, 2008, Appendix C, p. 51). Vide: OECD (2011-05-02), “The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them”, OECD Digital Economy Papers, No. 179, OECD Publishing, Paris. <http://dx.doi.org/10.1787/5kgcjf71pl28-en> p. 29.

¹³ De acordo com Youn, 2008, citado em Dooley et al., 2010, p. 155. Vide: OECD (2011-05-02), “The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them”, OECD Digital Economy Papers, No. 179, OECD Publishing, Paris. <http://dx.doi.org/10.1787/5kgcjf71pl28-en> p. 29.

Crianças também têm direito à privacidade, tanto *on-line* quanto *offline*. É necessário, por exemplo, que elas possam socializar *on-line* com seus pares sem a constante supervisão dos pais ou responsáveis. Nesse sentido, é possível que exista um paradoxo entre a privacidade a elas necessária e a proteção indispensável dos pais no meio cibernético.

Nesse contexto, a OCDE traz exemplos de controle parental na internet e do paradoxo entre a privacidade e a supervisão de pais e responsáveis. Algumas ferramentas de controle parental trazem dados detalhados sobre a atividade *on-line* de crianças aos pais e responsáveis, bem como escolas e bibliotecas oferecem programas que evoluem e ficam cada vez mais funcionais, demonstrando com precisão o comportamento das crianças no meio digital, tudo como estratégia de segurança cibernética.

Ocorre que, além de muitas vezes extrapolarem os limites da privacidade e liberdade do próprio indivíduo, os programas que auxiliam pais e responsáveis a rastrear os passos de jovens e crianças *on-line* podem levar a riscos ainda maiores em relação ao uso dos dados infantis. Isso porque os próprios serviços *on-line* de rastreamento podem usar as informações obtidas para além dos motivos inicialmente declarados ou, ainda, podem ter suas informações “roubadas” por outros servidores, com intenções maliciosas.

Tal paradoxo leva a diversas discussões sobre como se deve dar a proteção de crianças e adolescentes no mundo digital. Claro que os pais precisam conhecer os ambientes acessados pela criança, zelando pela sua integridade física e mental. É evidente, porém, que essa vigilância precisa respeitar os limites de privacidade, não só a fim de garantir seus direitos fundamentais, mas também de resguardar seus passos de intenções maliciosas.

1.3 Riscos envolvendo o consumo de crianças em âmbito *on-line*

Três padrões legislativos são comumente aplicados em relação aos riscos de consumo envolvendo crianças no âmbito online: i) legislação privada, ii) legislação consumerista e iii) legislação específica de proteção às crianças. Geralmente, na legislação privada, usuários menores de idade não tem capacidade legal para aderir à contratos e não são inseridas nesse meio. Já nas legislações consumeristas, como a lei anti-*spam*, impõem-se condições aos fornecedores que protegem todos consumidores de todas as idades. Por fim, nas legislações específicas, são estudados os riscos que as

crianças se submetem no consumo *on-line* e *off-line*, medindo sua capacidade de reconhecer e desenvolver sendo crítico sobre as publicidades que tem acesso.

Nesse sentido, muitos países (como Alemanha, Coréia do Sul, Turquia, Reino Unido e Estados Unidos), mantém legislações bastante rígidas e específicas do consumo infantil, como as regulações sobre jogos de apostas. No Reino Unido, sites de jogos e apostas só podem funcionar após certificação de que contém um robusto sistema de verificação de faixa etária. Já na Austrália, nenhum site do tipo é permitido, numa tentativa de proteger as crianças e adolescentes desse tipo de conteúdo.

Em relação às publicidades online dirigidas às crianças e adolescentes, dois são os modelos contrastantes que prevalecem nas regulações de diferentes países: a regulação governamental ativa de alguns aspectos da publicidade infantil online e a confiança depositada na autorregulação da indústria.

A União Europeia se mostra como um exemplo do primeiro modelo, já que prevê diversas restrições para a publicidade dos meios de comunicação, incluindo proteções específicas voltadas às crianças. Além da proibição geral de publicidades envolvendo cigarros e tabaco para qualquer público, é proibida a promoção de bebidas alcóolicas envolvendo crianças.

Nessa mesma perspectiva, diante da premissa de que a publicidade nas mídias conhecidas não deve causar nenhum dano psíquico ou moral para crianças e adolescentes, qualquer publicidade que explore a inexperiência e inocência das crianças é sempre proibida.

Assim, qualquer comunicação comercial deve ser sempre facilmente reconhecida e a prática da famosa técnica de "*product placement*" é sempre considerada ilícita em programas infantis, inclusive aqueles inseridos em plataformas digitais e *streamings*.

Nessa toada, ressalta-se que a Escandinávia é a região europeia que possui as regras mais elaboradas sobre o marketing na internet, visando a proteção de crianças e adolescentes sobre o mercado nórdico. Toda publicidade digital inserida nas mídias desses países deve estar de acordo com os padrões legais estabelecidos nessas nações. Dentre as regras, a publicidade também deve ser reconhecida como tal por crianças e adolescentes, além de levar em conta o estágio de desenvolvimento das crianças para quem a mensagem está sendo transmitida.

Além disso, a legislação nórdica traz proibição sobre convites para que o grupo infantil e adolescente adquira produtos ou serviços pela internet e desautoriza a prática de *advergaming*¹⁴ ou de promoção de prêmios advindos de atividades *on-line*.

1.4 Publicidade *on-line*

A autorregulação trouxe regras e padrões para a proteção da criança e adolescente no âmbito da publicidade, inclusive em relação à proteção de dados infantis. Cita-se como exemplos: International Chamber of Commerce's (ICC); Advertising and Marketing Communication Practice; International Advertising Bureau UK; Federation of European Direct and Interactive Marketing (FEDMA); entre outros.

Muitos desses instrumentos são amplos e aplicados na proteção de todos os consumidores de publicidade, em qualquer faixa etária e qualquer meio de comunicação. Outros asseguram direitos em meio online ou servem como escudo para faixas etárias específicas, como no caso das legislações voltadas a crianças e adolescentes. Neste último, a regulamentação infantil varia bastante de acordo com a faixa etária e nível de compreensão do indivíduo (algumas leis são aplicadas apenas para crianças com menos de 13 ou 14 anos por exemplo), e formam uma proteção adicional àquela estabelecida pelo conjunto de lei dos países.

Existem códigos complementares à legislação vigente, elaborados por organizações publicitárias e provedores de conteúdo, que fornecem informações valiosas na busca de uma publicidade ética, como é o caso das informações fornecidas sobre bebidas e comidas com alto nível de sódio, gordura e açúcar (os alimentos conhecidos como *HFSS foods – high in fat, sugar and salt*). Tais instrumentos são utilizados nas publicidades vinculadas aos serviços de mídia *on-line* e de outras mídias audiovisuais.

Nesse sentido, a colaboração da autorregulação e correção na busca pela proteção da criança e adolescente em meio *on-line* é de eficácia inquestionável. São

¹⁴ *Advergaming* é uma fusão das palavras inglesas “advertising” – publicidade e “game” – jogo. O termo traz a ideia de uma comunicação publicitária que usa de jogos eletrônicos como ferramenta para divulgar e promover marcas, produtos e serviços. Tal estratégia é bastante utilizada atualmente e tem bastante sucesso diante do fato que o público-alvo dessas ações publicitárias encontra-se totalmente imerso no ambiente virtual, em um momento de lazer, por vezes sem se dar conta do conteúdo publicitário da mensagem.

inúmeros os avanços feitos por tal instrumento na mitigação de risco desse público na internet.

Entretanto, o cenário da autorregulação enfrenta alguns desafios, como as fronteiras nacionais, a falta de adesão das regras por alguns setores da indústria e algumas lacunas que persistem durante o processo de construção de normas. Como exemplo, podemos citar o fato de que algumas técnicas publicitárias como a publicidade embutida¹⁵, a inserção de marcas e publicidade comportamental voltadas às crianças em ambiente digital ainda são pouco mencionadas nesses trabalhos regulatórios.

1.4 Conclusões do relatório da OCDE

As crianças são submetidas a diferentes níveis de riscos em diferentes países do mundo. Tudo depende da educação e da cultura em que estão emergidas, além, é claro, das condições sociais em que vivem. Alguns países conseguem controlar tais riscos de forma mais efetiva que outros.

De acordo com a OCDE¹⁶, na Suécia e Dinamarca, ainda que exista um massivo uso da internet por parte das crianças, os riscos relacionados ao seu uso podem ser considerados menores que em muitos outros países com menos acessibilidade ao universo digital. Isso sugere que uma política forte de uso responsável e uma educação *on-line* podem melhorar a segurança e a qualidade da vida *on-line* das pessoas.

Assim como as habilidades, a cultura e a educação variam entre os públicos infantis de diferentes países, também variam seus comportamentos¹⁷. Isso porque a vulnerabilidade da criança em ambiente digital depende de suas experiências, capacidades críticas, educação e do conhecimento sobre o ambiente em que ela circula.

¹⁵ Entre as publicidades embutidas, ou “embedded advertinsing”, podemos citar a técnica de product placement, amplamente discutida neste trabalho.

¹⁶ De acordo com De Haan and Livingstone, 2009, p. 5; Livingstone and Haddon, 2009, p. 17. Vide: OECD (2011-05-02), “The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them”, OECD Digital Economy Papers, No. 179, OECD Publishing, Paris. <http://dx.doi.org/10.1787/5kgcjjf71pl28-en> p. 30.

¹⁷ A OCDE cita como exemplo a preocupação do Japão em relação aos *sites* de encontros amorosos *on-line* e a algumas páginas que incitam métodos de suicídio, uma grande questão social no país; a Finlândia, que enxerga o marketing digital e informações pessoais como uma questão que necessita ser regulamentada urgentemente; o Canadá, a Austrália e o Reino Unido, que têm enfrentado grandes problemas relacionados ao *cyberbullying*.

A consequência dos riscos a que são submetidas as crianças na internet também varia, e pode incluir complicações desde psicológicas até físicas, além de questões econômicas e sociais, que podem afetar toda a sociedade contemporânea. Dessa forma, são necessários informação e educação sobre riscos *on-line*, não só por parte da família, como também do Estado, para que políticas públicas evitem todos os riscos aqui expostos, que influenciam não só o indivíduo, mas também toda uma sociedade, sua cultura e seus valores.

2. Publicidade na internet

As transformações experimentadas no século XXI advindas da internet alcançaram também, e principalmente, a forma de consumir e de apresentar os produtos e serviços aos consumidores.

Inúmeras foram as comodidades oferecidas pela tecnologia e pelo advento das redes; junto com elas, os desafios no uso das suas ferramentas, que evoluíram sobremaneira e tornaram-se complexas, não só pelos usuários, como também pelos anunciantes e legisladores. De fato, são diversos os temas e impactos no mundo jurídico decorrentes do uso da tecnologia também em relação aos anúncios publicitários, alguns superados e normatizados e outros em lento e tímido processo de estudo e regulamentação¹⁸.

¹⁸ “Destarte, num cenário hodierno em que os consumidores estão cada vez mais sofisticados, sensíveis, seletivos e céticos, sendo cada vez mais exigentes e apresentando novos comportamentos que forcem frequentemente a eficácia do marketing praticado na rede, denota-se um desafio às empresas – especialmente quando operam na Internet – a revisitarem suas práticas comerciais e publicitárias, de modo que possam ser verdadeiramente competitivas em face da grande concorrência e, ainda, estejam realmente aptas a assumir e explicitar ao consumidor uma postura confiável, prática e de qualidade de forma a convencer o consumidor a investir no produto oferecido. Para cumprir tal meta, as empresas recorrem a recursos tecnológicos que permitem o exercício do chamado marketing segmentado, pelo qual as estratégias empresariais são remodeladas para que se faça determinado anúncio ser apresentado ao consumidor que se saiba ter a necessidade de consumir o produto ou serviço respectivo (LIMEIRA 2003, p. 9) – e isto se faz com mecanismos como *machine learning* e algoritmos. Nesse sentido, se antes a venda em domicílio era feita de porta em porta, com a entrega de catálogos de produtos pelo próprio vendedor ou por correspondência, hoje tais catálogos adentram a residência do consumidor pela tela do computador. Outrossim, muito embora a publicidade em si seja uma atividade lícita, é utilizada cada vez mais em detrimento do discernimento do consumidor, recorrendo a práticas que, no extremado propósito de seduzir o comprador a qualquer preço, podem ser consideradas abusivas, tal como se dá por exemplo com a publicidade indutiva, as distorções de informações sobre produtos e serviços, incitação a superstições, violação de valores morais, à segurança, as vendas casadas, dentre outras (LORENZETTI, 2004, p. 390)” (ROSA, Luiz Carlos Goiabeira; FALEIROS JÚNIOR, José Luiz de Moura; VERSIANI, Rodrigo Luiz da Silva. A proteção do consumidor diante das práticas publicitárias abusivas do comércio eletrônico. **Revista da Faculdade Mineira de Direito**, v. 23, n. 45, p. 244-245, 2020).

Juliano Madalena, ao traçar uma teoria geral do direito digital, afirma que os desafios relacionados à internet demandam respostas jurídicas aos questionamentos postos por esse fenômeno, sugerindo a criação de um microsistema jurídico próprio, especialmente em razão da ubiquidade. É nesse aspecto que se desenvolve a noção de infinitude. O autor afirma:

Com efeito, a virtualização é a característica que instrumentaliza a internet, mas é a ubiquidade que instiga muitas estruturas jurídicas e sociais da vida contemporânea. Instiga, pois, ao permitir a aproximação das pessoas, empresas e estados, também os distancia. A mesma internet que aproxima, afasta. Nesse ponto, Antonio Segura-Serrano discorre que em virtude da natureza virtualizada da internet, a primeira discussão a ser feita sobre a sua regulação versa sobre a sua resistência natural para ser regulada. Daí, porque ocorre a ruptura do ordenamento jurídico, principalmente quanto a sua efetividade para regular fatos da vida virtual. Efetividade, pois do ponto de vista estrutural, a norma é eficaz, mas pouco efetiva em situações virtualizadas. Um exemplo é a coibição de crimes praticados pela internet onde o agente infrator, caso detenha a técnica, poderá criar inúmeros entraves às autoridades e ao Estado. É que pela ubiquidade o ato poderá ocorrer em diversos *locus*, países, estruturas ou região¹⁹.

Em relação aos aspectos da publicidade digital, tanto o provedor quanto anunciantes, consumidores, fornecedores e legisladores devem estar atentos, em consonância e equilíbrio com as relações nesse meio estabelecidas, evitando conflitos que podem surgir a partir do uso e compartilhamento de dados, da eventual ausência de clareza das informações e dos anúncios, além de outras questões que podem ser suscitadas.

Nesse sentido, Basan afirma que a publicidade e o *e-commerce* passaram a ser repensados a partir de novos instrumentos de marketing, com uso de recursos tecnológicos, interatividade, animações, além da contratação de influenciadores digitais. Dentre as técnicas de publicidade virtual, o autor enumera os seguintes exemplos: o *microsite*, o *banner*, o *pop-up*, os *links patrocinados*, o *e-mail marketing*, o *adverlog*, o *Search Engine Marketing*, o *podcasting* e os *spams*²⁰. Podemos também citar o *advergame* como técnica de publicidade virtual que muito interessa à seara da proteção da infância.

O autor define *microsite* como “pequenos sites de marcas que se transversam em links dentro de sites de conteúdo” e *banner* como “o tipo de publicidade feita por meio

¹⁹ MADALENA, Juliano. Regulação das fronteiras da internet: um primeiro passo para uma teoria geral do direito digital. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti. **Direito digital: direito privado e internet**. 3. ed. Indaiatuba: Foco, 2020. p. 173.

²⁰ BASAN, Arthur Pinheiro. **Publicidade digital e proteção de dados: o direito ao sossego**. Indaiatuba: Editora Foco. 2020, p. 162.

de espécies de cartazes virtuais inseridos em algum lugar da página, como uma espécie de outdoor virtual”. Já o *pop-up* pode ser, conforme o autor, definido como “uma pequena janela que se abre automaticamente assim que o internauta visualiza determinada página na Internet”; o *link patrocinado* “promove-se por meio da associação entre uma marca e um site, visando oferecer o conteúdo da página ao patrocinador, divulgando ao consumidor como se tivesse mero cunho informativo”; o *e-mail marketing* “consiste no envio de mala direta através de e-mails”; o *adverlog* “promove-se por meio de uma espécie de diário eletrônico, usado para elogiar um produto ou serviço”; o *Search Engine Marketing* “é uma ferramenta paga para promover anúncios diretamente nos mecanismos de buscas, como o Google e o Yahoo”. Por fim, o *podcasting* é um arquivo “de som, onde empresas patrocinam de maneira velada os produtores de conteúdo”²¹.

De fato, é possível observar uma crescente necessidade de regulamentação da publicidade em meio digital, de modo a suprir necessidade específica aos usuários das redes, provendo proteção às informações por eles fornecidas bem como tornando-os conscientes da utilização e do uso de seus dados, tanto para questões publicitárias e promocionais quanto para eventuais outras finalidades.

A problemática vai além quando se percebe que o usuário passa a ter uma espécie de vida estendida no meio cibernético em razão do perfil criado em meios virtuais. A personalidade do indivíduo, os gostos, a aparência, as competências profissionais e a vida familiar estão, em sua grande maioria, expostos aos outros usuários, anunciantes e provedores, criando-se um perfil do usuário na rede de computadores. É através do *profiling* que os fornecedores utilizam algoritmos para direcionar a publicidade pela rede mundial de computadores.

A utilização dos dados dos consumidores para direcionamento da publicidade fez surgir a denominada “publicidade comportamental”. O debate do tema é absolutamente essencial quando se trata de publicidade digital e proteção de dados do consumidor, em especial pelo uso de *cookies* e *spams*, conforme será estudado a seguir.

De fato, a coleta de informações sobre o perfil do consumidor na rede e suas preferências em relação a produtos e serviços, entre outros dados, torna a publicidade direcionada ao consumidor muito poderosa no sentido de que, ao conhecer o comportamento deste, o algoritmo pode ser utilizado para direcionar publicidade de produtos e serviços que, teoricamente, são de interesse desse consumidor. Daí a

²¹ BASAN, Arthur Pinheiro. **Publicidade digital e proteção de dados: o direito ao sossego**. Indaiatuba: Editora Foco. 2020, p. 162.

necessidade expressa de o consumidor consentir com o uso dos seus dados para o direcionamento da publicidade. Sobre o tema, Laura Schertel já afirmou:

Primeiramente, não há dúvida de que o pressuposto inicial de legitimidade da publicidade comportamental é o consentimento do consumidor, que deve ser informado, expresso, específico e anterior, nos moldes do sistema *opt in* (art. 7.º, VII e IX, Marco Civil e 6.º, II, CDC). Tendo em vista os riscos dessa atividade, não restam dúvidas de que um modelo de consentimento *opt out* não supriria em absoluto os seus requisitos de legitimação. Não obstante, outros critérios relacionados ao consentimento precisam ser observados para que essa prática seja tida como legítima: a) é preciso que o consentimento seja específico em relação a essa prática e se refira à autorização do monitoramento da sua navegação; assim, não basta o consumidor concordar com termos genéricos de navegação da página ou funcionamento do serviço; b) se a decisão do consumidor se basear em informações enganosas ou omissivas, o consentimento não será válido e a prática será considerada abusiva; c) se o consentimento for obtido a partir da veiculação de informações enganosas ou por meio de práticas abusivas (como, por exemplo, por meio da prática de requerer incessantemente o consentimento do consumidor a cada acesso ou não permitir que ele acesse outro *site* enquanto não consentir), ele será claramente inválido; o consentimento deve ser limitado a um curto período de tempo, devendo ser constantemente renovado; d) mecanismos de revogação do consentimento devem estar facilmente disponíveis ao consumidor²².

Diante dessas questões, surgem as divergências sobre os limites da atuação dos provedores na internet, *sites* de busca, bem como sobre a maneira como se explora a publicidade no meio digital. O fato de sermos, por diversas vezes, representados pelas informações que ali foram guardadas traz a necessidade de alcançar regulamentação eficaz e adequada a balancear os princípios constitucionais da intimidade e privacidade com os direitos de expressão e liberdade comercial.

É premente a necessidade de preservar a autonomia e a intimidade do usuário da internet. Nesse contexto, Magalhães, Faleiros Júnior e Basan complementam:

Se a formação de uma projeção da personalidade, um avatar, corpo eletrônico ou persona digital dá indícios de um novo arcabouço de valores da dignidade individual – passível de proteção e tutela jurídica –, nasce uma preocupação desdobrada das inúmeras consequências que esse indivíduo enfrentará em sua “vida tecnológica”. Se “cada ser humano possui um valor intrínseco e desfruta de uma posição especial no universo”, com uma dimensão individual e própria, dotada de valor, e outra extrínseca, orbitada por deveres para com outrem, será desumano, portanto, tudo aquilo que puder reduzir o indivíduo à condição de objeto²³.

Os autores trazem o conceito denominado *habeas mente*, a proteção à liberdade mental dos indivíduos e, com ela, a dignidade, efetivando as liberdades físicas (do corpo)

²² MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. **Revista de Direito do Consumidor**, São Paulo, v. 106, p. 37-69, jul.-ago. 2016.p. 60

²³ MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz; BASAN, Arthur. A responsabilidade civil pela perturbação do sossego na internet. **Revista de Direito do Consumidor**, São Paulo, ano 29, v. 128, p. 227-253, mar.-abr. 2020. p. 230

e psíquicas (da mente), no mundo real e virtual, à procura de um desenvolvimento independente.

Faz-se mister observar a necessidade de proteção contra as práticas e publicidades abusivas que podem ocorrer no mundo digital. É preciso ter atenção aos limites legislativos e de autorregulação da publicidade e dos negócios jurídicos que se realizam na internet, trazendo garantias dos direitos fundamentais aos consumidores já contemplados pelo nosso sistema normativo.

Tratando-se de um usuário mirim no meio digital, a questão toma maior proporção. Seria possível falar do “corpo eletrônico” de uma pessoa menor de 18 (dezoito) anos? Como proteger esse “avatar” e garantir aos usuários mirins espaço para que eles possam, respeitando sua autonomia progressiva, ter a devida compreensão a respeito dos meios utilizados para inserção de produtos pela rede mundial de computadores?

2.1. O conceito de consumidor, fornecedor e estabelecimento comercial na internet

De acordo com o art. 2º do Código de Defesa do Consumidor, “consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final”. O mesmo dispositivo equipara consumidor “a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo”.

No mesmo sentido, em seu art. 3º, o código consumerista traz a definição de fornecedor, estabelecendo-o como “toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados que desenvolvem atividade de produção, montagem, criação, construção, transformação, exportação, distribuição ou comercialização de produtos ou prestação de serviços”.

Dadas as definições dos termos pelo nosso ordenamento jurídico, importante destacar que não existe tratamento específico em relação aos consumidores e fornecedores em ambiente virtual. Dessa forma, independentemente do ambiente em que a relação comercial é estabelecida, o mesmo tratamento é destinado aos consumidores e fornecedores, seja virtual ou presencial, ressalvando o direito de arrependimento em relação à compra quando esta for realizada a distância²⁴.

²⁴ Antonia Klee conceitua comércio eletrônico como “termo utilizado para expressar toda e qualquer forma de transação comercial em que as partes interagem eletronicamente” (KLEE, Antonia Espíndola Longoni. **Comércio eletrônico**. São Paulo: Revista dos Tribunais, 2014. p. 71).

Em relação ao estabelecimento comercial virtual, este não carrega grandes discussões sobre seu tratamento em nosso ordenamento jurídico. O art. 1.142 do Código Civil definiu estabelecimento comercial como “todo complexo de bens organizado, para exercício da empresa, por empresário, ou por sociedade empresária”.

Nesse sentido, sua existência deve ser real, constituída de bens corpóreos (como imóveis, móveis) e bens incorpóreos (aqui incluindo a marca, registro de patente, entre outros). Independentemente do tipo de serviço ou produto oferecido através de plataforma da internet, o estabelecimento comercial é necessário para realização da atividade econômica.

Claro é que, dependendo do tipo de atividade desenvolvida, o chamado estabelecimento comercial pode se dar em espaço físico, *website* da internet ou aplicativo. No último caso, não existe diferença no tratamento jurídico dado aos direitos e deveres da atividade empresária, que se sujeita às regras dispostas pelo Código de Defesa do Consumidor, ainda que questionamentos sejam levantados em relação à localização do estabelecimento.

Nessa toada, ressalta-se que, ainda que a página da internet represente o estabelecimento comercial de determinada empresa, a doutrina entende necessário existir uma sede física, entre outros elementos, que permita encontrar o anunciante, caso necessário.

De acordo com Cristina Cantú Prates,

na prática, o que se verifica por parte dos legisladores e operadores do direito é a tendência de que todo estabelecimento virtual, ou seja, que comercializa na internet, se faça representar por uma sede física, endereço, telefone, nome do representante legal e CNPJ. [...] essa exigência faz sentido sob a ótica do Código de Defesa do Consumidor, eis que o fornecedor tem o dever de prestar informações claras e precisas, não somente sobre o produto vendido, mas sobre sua própria identidade²⁵.

Nesse contexto, importante ressaltar que, apesar de a lei consumerista não trazer nenhuma previsão específica relacionada ao comércio eletrônico, os princípios e as regras ali estabelecidos levam ao dever de informação ao consumidor, seja qual for o ambiente em que a atividade se desenvolva.

Assim, de acordo com o art. 31 Código de Defesa do Consumidor, a oferta e a apresentação de produtos e serviços no meio virtual também devem assegurar

²⁵ PRATES, Cristina Cantú. **Publicidade na internet**: consequências jurídicas. Curitiba: Juruá, 2015. p. 66.

informações corretas, claras, precisas, ostensivas e em língua portuguesa, com todos os atributos do produto, desde o preço até a validade e composição deste.

De outra banda, o art. 33 do Código de Defesa do Consumidor, em complemento ao dispositivo anterior, prevê a necessidade de informação sobre o nome e endereço do fabricante, em casos de oferta ou venda realizada via telefone ou reembolso postal. Diante da norma, tem-se clara a intenção do legislador, no tempo da elaboração do dispositivo, de abarcar o direito à informação do consumidor em todos os meios de transação comercial que possam existir.

2.2. *Cookies* e a obtenção de dados dos consumidores

No meio digital, um instrumento muito empregado para armazenar dados e direcionar publicidade é o *cookie*. Trata-se de um fragmento de texto armazenado por servidor da *web* no disco rígido do usuário, amplamente utilizado por páginas da internet com a finalidade de identificar e armazenar dados dos visitantes. Tais dados podem ter diversos propósitos, como facilitar o *login* no *site* por meio da conservação de senhas de acesso e preservar o idioma e as configurações escolhidas pelo usuário, bem como suas preferências de navegação.

Dessa forma, cada usuário gera uma espécie de número de identificação, que contém as informações de como o cliente utiliza a página da internet, além de seus dados, fornecidos por ele próprio, de forma a facilitar, teoricamente, o acesso do cliente à página da internet. De acordo com Cristina Cantú:

Em tese, os *cookies* não podem acessar informações do sistema. Podem apenas armazenar uma cópia dos dados que são fornecidos no momento do preenchimento de formulários e gravar informações sobre a maneira pela qual os usuários se movimentam dentro do sítio consultado e apenas nele (pelo menos em teoria nenhum sítio pode consultar *cookies* enviados por outro). Em suma: um *cookie* armazena em seu próprio disco rígido informações sobre as preferências pessoais exclusivamente referentes ao sítio que o enviou e teoricamente serve para tornar a navegação mais confortável e proveitosa²⁶.

Ana Paula Gambogi Carvalho conceitua *cookies* como

programas de dados gerados com objetivo principal de identificação do usuário e de rastreamento e obtenção de dados úteis a seu respeito, tais como seus hábitos de navegação e de consumo. Frequentemente utilizados por provedores

²⁶ PRATES, Cristina Cantú. **Publicidade na internet**: consequências jurídicas. Curitiba: Juruá, 2015. p. 162.

da internet, estes fichários de dados são enviados aos programas navegadores (*browsers*) e salvos em diretórios específicos do computador do usuário²⁷.

Nesse sentido, os *cookies* tornaram-se importante ferramenta de obtenção de informações sobre o perfil do cliente e seus interesses nas páginas da *web*. A ferramenta é bastante útil aos fornecedores no comércio eletrônico, principalmente aos provedores e anunciantes da internet, podendo inclusive ser considerada um dos principais instrumentos destes, tornando a utilidade do consumidor irrelevante, se comparada à dos fornecedores.

Isso porque a ferramenta é bastante utilizada para entender o comportamento dos clientes dentro daquele ambiente. Entre suas finalidades, é fácil compreender os gostos, as preferências, os hábitos e, principalmente, as prioridades de consumo. Estas últimas, inclusive, tornaram-se bastante proveitosas ao fornecedor, sendo fonte de informações sobre potenciais consumidores de seus produtos e serviços.

Fabiola Meira esclarece a utilidade e os riscos envolvidos na utilização dos *cookies*:

Entre as inúmeras consequências da existência de *cookies* nos computadores, pode-se citar que possuem a função de: (i) avisar o “fornecedor” que um consumidor específico retornou ao site para uma busca; (ii) automaticamente customizar a tela com as preferências daquele consumidor identificado ou até mesmo para sua última compra, que não pode ser concluída, por exemplo, pois a conexão “caiu”, visto que com o *cookie*, se o cliente quiser continuar a compra no ponto em que parou estes “lembrarão” o que possuía em seu “carrinho”, tornando desnecessário que o consumidor reinicie o processo; (iii) conservar a identificação do consumidor e própria senha quando transportado para outra página; (iv) manter a lista das páginas visitadas pelo consumidor em determinado dia e hora, ou seja, possuem todo o histórico de visitas virtuais do consumidor.

Uma das graves consequências da instalação de *cookies* diz respeito à comercialização das informações da esfera íntima do consumidor-internauta para que os fornecedores, de posse de ditos cadastros, utilizem os perfis dos usuários e, por meio de spams “bombardeiem” as caixas de correio eletrônico do internauta ofertando produtos ou serviços não solicitados²⁸.

Ainda de acordo com Cristina Cantú, “a utilidade dos cookies para a publicidade no meio eletrônico reside na salutar importância do estudo do comportamento do cliente como uma estratégia de planejamento empresarial através do filtro trazido pelo cookie”²⁹.

²⁷ CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. **Revista de Direito do Consumidor**, São Paulo, Revista dos Tribunais, n. 46, p. 114, 2004.

²⁸ SANTOS, Fabiola Meira de Almeida. **O marketing digital e a proteção do consumidor**. 2009. 183 f. Dissertação (Mestrado) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2009, p. 84.

²⁹ PRATES, Cristina Cantú. **Publicidade na internet: consequências jurídicas**. Curitiba: Juruá, 2015. p. 157.

Tal aspecto torna possível que o fornecedor entenda se a divulgação de seus produtos ou serviços é ou não interessante para aquele usuário da internet e, principalmente, quais as chances de a publicidade inserida naquele contexto resultar em lucros para aquele fornecedor.

Fabiola Meira, por sua vez, ressalta a relação entre os *cookies* e a falta de informação aos consumidores quanto à automática sujeição a esse tipo de prática comercial eletrônica, tema que fora devidamente regulamentado pela Lei Geral de Proteção de Dados. Antes da regulamentação legal, os consumidores não tinham conhecimento de que seus dados estavam sendo capturados em sua máquina, o que já denotava violação à legislação consumerista³⁰.

Nessa toada, verifica-se a possibilidade de o fornecedor tratar os dados dos consumidores conforme seus próprios interesses, incluindo ou excluindo consumidores de acordo com seus perfis (*profiling*) e escolhendo aqueles que pretendem alcançar e aqueles que não lhe são interessantes. Tal prática pode tornar-se abusiva na medida em que pode discriminar o consumidor de acordo com seu poder aquisitivo, sexo, idade, nível intelectual e outros³¹.

Nesse sentido, adverte Laura Mendes:

Ao mesmo tempo que são úteis, por possibilitar a memorização de senhas e a personalização de serviços, os *cookies* podem trazer riscos à privacidade, quando o computador passa a ser associado a um determinado usuário, a partir dos dados pessoais fornecidos a um *site* ou por meio dos dados pessoais armazenados pelo provedor de conexão que possui um contrato de prestação de serviços com o usuário. Além disso, se armazenados por um longo período

³⁰ Antes da regulamentação pela Lei Geral de Proteção de Dados Pessoais, a ABA editou o denominado Código de Ética Anti-Spam e Melhores Práticas de Uso de Mensagens Eletrônicas. Em seu art. 11º, trazia regulação sobre a coleta de informação e uso de dados dos usuários: “Artigo 11º. Para a Coleta de Informações e Dados de Consumidores ou Usuários de meios eletrônicos, deve ser observado o seguinte: a) As informações dos usuários para uso e envio de Mensagens Eletrônicas deverão ser coletadas para esse fim exclusivo através de formulários de cadastramento nos sites e/ou e-mails; participação em concursos ou promoções; formulários de ‘e-commerce’ ou qualquer outra forma que exponha explicitamente a finalidade de captação das informações; b) Constará obrigatoriamente do documento eletrônico acima referido a autorização do usuário para o posterior recebimento de Mensagens Eletrônicas e Mala Direta Digital, que jamais poderá ser presumida; c) O usuário deverá ter livre acesso e a qualquer tempo ao seu cadastro no Banco de Dados, seja para retirar seus dados do mesmo, seja para editar seus dados, seja ainda para suspender ou cancelar a autorização antes dada para o recebimento de Mensagens Eletrônicas ou Mala Direta Digital; d) É vedada a coleta de quaisquer dados que possam expor o usuário a situações de constrangimento de qualquer tipo; e) A pessoa física ou jurídica responsável pela coleta de informações deve apresentar ao usuário sua “Política de Privacidade de Dados”; f) A “Política de Privacidade de Dados” acima referida deve descrever claramente como serão utilizadas ou comercializadas as informações coletadas, assim como se serão utilizados ‘cookies’ nos navegadores de acesso à Rede Internet”.

³¹ “Verifica-se que conhecer o comportamento do consumidor surge como uma necessidade em tempos de pós-modernidade. Se de um lado a alta competitividade do mercado exige a habilidade do fornecedor em oferecer produtos e serviços que vão ao encontro das necessidades e dos interesses do consumidor; de outro, os fornecedores passam a ter uma ferramenta poderosíssima em suas mãos, que lhes permite estreitar relações com os consumidores potenciais e afastar os indesejáveis” (PRATES, Cristina Cantú. **Publicidade na internet: consequências jurídicas**. Curitiba: Juruá, 2015. p. 161).

de tempo, esses marcadores podem rastrear o comportamento do usuário *online* em diversos *sites*³².

Evidencia-se, portanto, a invasão à privacidade e intimidade do consumidor, que tem seus dados e comportamentos rastreados, muitas vezes sem permissão para tanto e sem nem sequer ter conhecimento sobre esse fato. Tal circunstância representa transgressão de diversos dispositivos da legislação vigente, tais como o art. 5º da Constituição Federal e, mais precisamente, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018)³³.

A preservação da privacidade e da intimidade e o direito à informação são consagrados na Constituição Federal, além dos recentes deveres impostos às empresas que manipulam dados de consumidores na internet. De fato, agora o tratamento de dados fornecidos por consumidores *on-line* só pode ocorrer mediante autorização, conforme

³² MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. **Revista de Direito do Consumidor**, São Paulo, v. 106, p. 37-69, jul.-ago. 2016. p. 59

³³ Nesse sentido, afirma Basan: “Em verdade, o uso do monitoramento permite ao fornecedor saber, dentre outras informações relevantes, se o consumidor é novo ou está retornando no acesso à página virtual, qual foi o tempo de acesso, os períodos de acesso mais comum, além da origem geográfica do internauta. Obviamente, todas as informações são utilizadas posteriormente para promover o convencimento do ato de consumo. Conforme se nota, surgem polêmicas questões envolvendo a proteção de dados, que é evidentemente violada a partir do momento em que as empresas, por meio dos *cookies*, promovem a vigilância do usuário em rede. Além disso, outra questão ilícita relacionada a essa prática é utilização dos perfis dos usuários para a promoção de publicidades de produtos e serviços não solicitados, os *spams*. Assim, tendo como base as regras contidas no CDC e, ainda mais, as previsões contidas na LGPD, **não se admite que os *cookies* sejam utilizados automaticamente em desfavor dos consumidores, coletando informações e alimentando banco de dados, sem a necessária informação das finalidades e sem exigida a permissão do consumidor, na figura do consentimento esclarecido**” (grifo nosso). BASAN, Arthur Pinheiro. Publicidade digital e proteção de dados: o direito ao sossego. Indaiatuba: Editora Foco, 2020. p. 163.

disposto pelo art. 7º da Lei Geral de Proteção de Dados³⁴, e nos limites por ela estabelecidos.

O conhecimento de informações pessoais e sensíveis sobre a intimidade dos usuários da rede através de *cookies*, desde informações como nome, endereço e profissão, as páginas acessadas, preferências de consumo e dados bancários, depende do consentimento expresso do portador dos dados, ou diante das hipóteses tratadas no referido artigo.

Sobre as utilidades dos *cookies* na internet, é perfeitamente possível (e fácil) que muitos consumidores sejam enganados quanto à destinação dos dados por ele fornecidos ao entrar em uma página da *web*. Dessa forma, para que exista harmonia com as regras estabelecidas pela nova Lei Geral de Proteção de Dados e com a lei consumerista, é necessário que os *cookies* sejam claramente explicados ao consumidor, bem como todas as suas utilidades, trazendo perfeito entendimento aos usuários que fornecem suas informações pessoais.

³⁴ “Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I – mediante o fornecimento de consentimento pelo titular; II – para o cumprimento de obrigação legal ou regulatória pelo controlador; III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (*Redação dada pela Lei nº 13.853, de 2019.*) IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. § 1º Revogado (*Redação dada pela Lei nº 13.853, de 2019.*) § 2º Revogado (*Redação dada pela Lei nº 13.853, de 2019.*) § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. § 4º É dispensada a exigência do consentimento previsto no *caput* deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei. § 5º O controlador que obteve o consentimento referido no inciso I do *caput* deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei. § 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular. § 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (*Incluído pela Lei nº 13.853, de 2019.*)”

Laura Mendes já afirmava a necessidade de consentimento expresso do consumidor para a utilização dos *cookies*, com fundamento no Código de Defesa do Consumidor e no Marco Civil da Internet. Vejamos:

À luz do direito básico do consumidor à proteção de dados pessoais, é importante analisar quais os pressupostos de legitimidade para a utilização de *cookies*. Partindo da condição de legitimidade do tratamento de dados pessoais nas relações de consumo, segundo a qual o processamento de dados pessoais deve ser autorizado pelo consumidor (art. 7.º, VII e IX, Marco Civil), ao menos que seja imprescindível para o cumprimento do contrato, é preciso analisar em que situações será exigido o consentimento pelo consumidor e em que situações o consentimento será dispensado.

Adaptado ao mundo virtual e baseado nas funções que os *cookies* podem exercer para facilitar a comunicação e a navegação, o pressuposto da necessidade da execução do contrato pode ser reinterpretado. Isto é, se o *cookie* for utilizado exclusivamente para a transmissão de comunicações na Internet ou for estritamente necessário para a realização de um serviço *online* solicitado pelo consumidor, não lhe acarretando riscos, não será necessário o seu consentimento.

Por outro lado, sempre que o *cookie* visar outras funções, será necessária a obtenção do consentimento prévio do consumidor. Esse é o caso, por exemplo, dos *cookies* das redes sociais (*social plug-in tracking cookies*), que são capazes de monitorar tanto os membros como os não membros dessas redes. Além disso, os *cookies* utilizados para realizar a publicidade comportamental (*third party advertising*) também não são isentos do consentimento, pois, ao visarem a coleta de dados pessoais para terceiros, naturalmente não são essenciais para a relação entre o usuário e o *site*. Por isso, todos os *cookies* de terceiros exigem o consentimento prévio do consumidor, antes de serem instalados. Por fim, os *cookies* dos *sites* chamados de *first part analytics* também necessitam do prévio consentimento do consumidor. Esses *cookies* geralmente são usados pelos responsáveis dos *websites* para estimar o número de visitas ou para monitorar a navegação do usuário.

Para passar pelo pressuposto objetivo de legitimidade, os *cookies*, em nenhum dos casos, podem apresentar graves riscos para os usuários. Isto é, em nenhuma hipótese é legítimo submeter o usuário a uma vigilância ininterrupta, transformando-o em mero objeto de monitoramento, o que, naturalmente, violaria o seu direito à intimidade e à vida privada e o princípio da dignidade, protegidos constitucionalmente. Além disso, em qualquer dos casos é preciso que seja divulgada por meio da política de privacidade ou no contrato de prestação de serviços da empresa publicado no *site* a forma de utilização dos *cookies* e para quais finalidades eles são instalados (7.º, VI, VIII e XI, Marco Civil, e art. 6.º, III, do CDC)³⁵.

No âmbito da comunidade europeia, a Diretiva 2009/136 alterou importantes diretivas europeias relativas à utilização da proteção da privacidade e dos usuários das redes e comunicações eletrônicas³⁶. Em relação aos *cookies*, a alteração do art. 5º da Diretiva 2002/58 trouxe a seguinte redação ao dispositivo:

³⁵ MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. Revista de Direito do Consumidor, São Paulo, v. 106, p. 37-69, jul.-ago. 2016.

³⁶ Sobre as alterações introduzidas pela Diretiva, afirma Cíntia Rosa: “Esta revisão teve como pontos principais: – garantir o acesso à Internet e às comunicações eletrônicas a todos os cidadãos europeus em prol de uma sociedade da informação inclusiva, com destaque para os portadores de necessidades especiais; – mais qualidades nos serviços prestados pelos provedores de acesso à Internet e aplicativos de Internet; – elevar o grau de harmonização das regras dos Estados-Membros quanto à proteção de dados pessoais e ao

Artigo 5.º Confidencialidade das comunicações

1. Os Estados-Membros garantirão, através da sua legislação nacional, a confidencialidade das comunicações e respectivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações electrónicas publicamente disponíveis. Proibirão, nomeadamente, a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de interceptação ou vigilância de comunicações e dos respectivos dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa, excepto quando legalmente autorizados a fazê-lo, de acordo com o disposto no n.º 1 do artigo 15.º O presente número não impede o armazenamento técnico que é necessário para o envio de uma comunicação, sem prejuízo do princípio da confidencialidade.
2. O n.º 1 não se aplica às gravações legalmente autorizadas de comunicações e dos respectivos dados de tráfego, quando realizadas no âmbito de práticas comerciais lícitas para o efeito de constituir prova de uma transacção comercial ou de outra comunicação de negócios.
3. Os Estados-Membros velarão por que a utilização de redes de comunicações electrónicas **para a armazenagem de informações ou para obter acesso à informação armazenada no equipamento terminal de um assinante ou utilizador só seja permitida na condição de serem fornecidas ao assinante ou ao utilizador em causa informações claras e completas, nomeadamente sobre os objectivos do processamento**, em conformidade com a Directiva 95/46/CE, e de lhe ter sido dado, pelo controlador dos dados, o direito de recusar esse processamento. Tal não impedirá qualquer armazenamento técnico ou acesso que tenham como finalidade exclusiva efectuar ou facilitar a transmissão de uma comunicação através de uma rede de comunicações electrónicas, ou que sejam estritamente necessários para fornecer um serviço no âmbito da sociedade de informação que tenha sido explicitamente solicitado pelo assinante ou pelo utilizador (grifo nosso).

A diretiva é conhecida como *cookies directive*, tendo ficado esclarecido que, no âmbito da comunidade europeia, a utilização do *cookie* não é proibida, mas deve ser regulamentada, havendo sempre o consentimento prévio e esclarecido do usuário para que a prática seja admitida³⁷⁻³⁸.

direito à privacidade, já garantidos pela Dir. 2002/58/CE, independentemente da tecnologia adotada (em especial, os dispositivos de identificação ou localização por radiofrequência – RFID devem respeitar estes direitos fundamentais); – impõe, aos provedores de acesso à Internet e de aplicativos de Internet, a obrigação de adotar medidas para evitar que sejam instalados *spyware* nas máquinas dos usuários de maneira inadvertida; – em consequência, impõe um dever de informação destes provedores; – as regras aplicadas ao *spam* são estendidas aos serviços SMS, MMS e outros semelhantes; – estimula a cooperação entre os Estados-Membros para o combate de *spam* ilícitos e *spyware* transfronteiriço, dentre outros” (LIMA, Cíntia Rosa Pereira de. Direito ao esquecimento e internet: o fundamento legal no direito comunitário europeu, no direito italiano e no direito brasileiro. **Doutrinas Essenciais de Direito Constitucional**, v. 8, p. 511-543, ago. 2015. p. 519).

³⁷ “Tendo em vista a regulamentação do uso de *cookies* por esta diretiva que alterou o art. 5 (3) da Directiva 2002/58/CE, esta diretiva é conhecida como *Cookies Directive*. Assim, a utilização destes *softwares* não é totalmente proibida, mas deve ser limitada segundo as regras estabelecidas, ou seja, mediante o consentimento prévio e esclarecido do usuário (que teve informações claras e completas sobre a prática). Mas não só, observada também a finalidade para qual a informação foi coletada” (LIMA, Cíntia Rosa Pereira de. Direito ao esquecimento e internet: o fundamento legal no direito comunitário europeu, no direito italiano e no direito brasileiro. **Doutrinas Essenciais de Direito Constitucional**, v. 8, p. 511-543, ago. 2015. p. 520).

³⁸ Ainda sobre os *cookies* na comunidade europeia, Cíntia Rosa esclarece: “Em uma obra que analisa os sete anos de proteção de dados pessoais na Itália, faz-se um balanço sobre a proteção dos dados pessoais na legislação italiana e sugestões para o futuro. Nesta oportunidade, destacou-se o atual esforço para regular

Veremos a seguir que a Lei Geral de Proteção de Dados exige expressa autorização dos pais para que haja tratamento dos dados de crianças e que os adolescentes, teoricamente, podem consentir com o uso dos seus dados e, conseqüentemente, com o uso dos *cookies*.

2.3. Spam

Spam, termo originário da língua inglesa, é designado para descrever mensagens eletrônicas recebidas, mas não solicitadas pelos usuários de páginas na internet. Pode, nesse contexto, significar “Sending and Posting Advertisement in Mass”, ainda que outras definições sejam encontradas para a sigla.

Na prática, são mensagens eletrônicas de conteúdos cibernéticos que chegam ao consumidor sem que tenham sido solicitadas ou permitidas, podendo causar incômodos e problemas aos navegantes da internet. No magistério de Fabíola Meira, o *spam* é

a técnica de marketing digital mais conhecida, mais antiga e também a mais criticada. Trata-se de envio de mensagens eletrônicas com anúncios publicitários não solicitadas pelo usuário da rede e que lhe acarretam inúmeras dificuldades, tais como recebimento de vírus, saturação da caixa postal, invasão de privacidade, entre outros graves problemas da Era Digital³⁹.

Nesse sentido, Basan acrescenta que não apenas as mensagens enviadas por correio eletrônico podem ser consideradas um *spam*. Devem-se acrescentar, aqui, as mensagens enviadas através de computadores, *smartphones*, notificações de aplicativos, entre outras possibilidades:

[...] o spam não se limita unicamente à mensagem enviada por correio eletrônico, isto é, parte-se da ideia de que essa prática perturbadora deve ser considerada também a partir de outras vertentes, de modo que se pode qualificar como spam qualquer tipo de publicidade não solicitada e importunadora enviada por meio de tecnologias de informação e comunicação, como por meio de computadores, smartphones, smartwatch, através de e-mail, short message servisse (mensagem sms), ligações telefônicas, notificações em aplicativos, etc. Inegavelmente, a questão deve ser tratada com vistas à

o *marketing* no contexto das novas tecnologias, em especial os *cookies*. A sugestão é alcançar um ponto de equilíbrio entre a tutela da pessoa mediante a proteção de seus dados e os interesses mercadológicos. Por isso, proibir realmente não seria a melhor saída, mas limitar a utilização desta tecnologia em favor do *marketing* na medida em que se condiciona a utilização dos *cookies* ao prévio consentimento esclarecido e informado do usuário e segundo a finalidade proposta. Tanto a *riservatezza*, quanto a proteção dos dados pessoais, deve ser tutelada mediante a ponderação em cada caso concreto. O direito ao esquecimento ora é fundamentado na primeira; ora, na segunda” (LIMA, Cíntia Rosa Pereira de. Direito ao esquecimento e internet: o fundamento legal no direito comunitário europeu, no direito italiano e no direito brasileiro. **Doutrinas Essenciais de Direito Constitucional**, v. 8, p. 511-543, ago. 2015. p. 522).

³⁹ SANTOS, Fabíola Meira de Almeida. **O marketing digital e a proteção do consumidor**. 2009. 183 f. Dissertação (Mestrado) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2009, p. 90.

imposição de limites aos abusos da publicidade virtual, que, além de assediar indevidamente ao consumo, é perturbadora de sossego⁴⁰.

O Código de Ética Anti-Spam e Melhores Práticas de Uso de Mensagens Eletrônicas da Associação Brasileira de Anunciantes (ABA) define *spam* como segue:

“Spam” é a designação para a atividade de envio de Mensagens Eletrônicas e Mala Direta Digital que não possam ser consideradas nem Marketing Eletrônico, nem Newsletter, e nas quais se verifique a simultânea ocorrência de pelo menos 2 (duas) das seguintes situações: a) Inexistência de identificação ou falsa identificação do Remetente; b) Ausência de prévia autorização (opt-in) do Destinatário; c) Inexistência da opção “opt-out”; d) Abordagem enganosa – tema do assunto da mensagem é distinto de seu conteúdo de modo a induzir o destinatário em erro de acionamento na mensagem; e) Ausência da sigla NS no campo Assunto, quando a mensagem não houver sido previamente solicitada; f) Impossibilidade de identificação de quem é de fato o Remetente; g) Alteração do Remetente ou do Assunto em mensagens de conteúdo semelhante e enviadas ao mesmo Destinatário com intervalos inferiores a 10 (dez) dias.

Assim, tais mensagens são recebidas através de e-mail ou pela navegação nas redes sociais e em outros *websites*. Seu conteúdo é majoritariamente publicitário, com a finalidade de promover marca, produto ou serviço, podendo, entretanto, conter intenção criminosa ao difundir notícias falsas ou requerer dados financeiros e pessoais dos usuários.

As mencionadas mensagens indesejáveis têm grande poder de massificação, podendo atingir um número significativo de usuários na internet, por diversos meios: e-mails, canais de bate-papo, grupos de interesse, mensagens de texto em telefones celular e outros meios de comunicação. De fato, as mensagens são disparadas aos usuários, sem que tenham demonstrado interesse em recebê-las.

É incontestável que o *spam* afeta a todos os usuários da rede, em maior ou menor grau. Em virtude da sua grande propagação, é causa de aborrecimento e transtorno pelos navegantes, caracterizando, inclusive, prejuízos ao consumidor, que, de acordo com Cristina Cantú, “paga a conta da remessa indevida dos e-mails”⁴¹.

Ainda nesse sentido, são diversos os dispositivos de nosso ordenamento transgredidos pelo uso inadequado da ferramenta. Os princípios constitucionais da intimidade e privacidade, o direito consumerista à informação e a proteção advinda da recente Lei Geral de Proteção de Dados abarcam o tema.

⁴⁰ BASAN, Arthur Pinheiro. Publicidade digital e proteção de dados: o direito ao sossego. Indaiatuba: Editora Foco, 2020. p. 163.

⁴¹ PRATES, Cristina Cantú. **Publicidade na internet: consequências jurídicas**. Curitiba: Juruá, 2015. p. 173.

Exemplificando, podemos citar a concorrência desleal que pode derivar do uso do *spam*, uma vez que, ao optar por esse tipo de divulgação, torna desigual a competição daquelas empresas que usam dos meios mais caros e tradicionais (e legais) para difusão de publicidade, ou ainda o desrespeito ao direito dos usuários, de informação sobre o uso de dados pelo *spam*.

Cristina Cantú Prates⁴² enumera diversas iniciativas de regulamentação jurídica acerca do tema no Brasil. Segundo a autora, foram apresentados dez projetos de lei na Câmara dos Deputados e a mesma quantidade no Senado Federal. De acordo com o número de projetos em tramitação, é possível perceber que o assunto tem chamado a atenção das casas legislativas, mostrando a crescente necessidade de regulamentação de tais ferramentas e meios de propagação de publicidade dentro da internet.

Nesse sentido, podemos observar a variedade de assuntos que envolvem a seara jurídica e a necessidade de legislação específica. Observa-se, da mesma maneira, a importância de que a legislação acompanhe o ritmo no qual essas ferramentas se desenvolvem, adaptando as leis às novas realidades da atualidade tecnológica. A razão é clara: ainda que existam diversas legislações abrangentes que protegem a integridade do usuário da internet, os avanços tecnológicos muitas vezes são mais dinâmicos que o processo legislativo.

2.4. As celebridades dos meios digitais: influenciadores digitais

O influenciador digital pode ser definido como um produtor de conteúdo que utiliza seus canais em redes sociais, tais como YouTube, Facebook, Instagram e Twitter, para tratar de temas que são de sua *expertise* ou interesse. Ao difundir o seu conteúdo, usuários da rede que têm o mesmo interesse passam a “seguir” o influenciador, que insere seus produtos digitais com assiduidade para manter o canal, com vídeos, áudios e fotografias, bem visitado.

De fato, tal qual uma celebridade da televisão ou do rádio, os produtores de conteúdo influenciam o comportamento dos seus seguidores, que passam a imitar e compartilhar suas ideias, utilizar as marcas indicadas ou comprar os produtos desenvolvidos pelos próprios influenciadores (como livros de receitas, cursos, entre outros). Assim, os influenciadores passam a receber boa quantia em dinheiro ou outras

⁴² PRATES, Cristina Cantú. **Publicidade na internet: consequências jurídicas**. Curitiba: Juruá, 2015. p. 180.

compensações e muitos deles desenvolvem a profissão de youtuber, com forte patrocínio de marcas famosas.

Para se ter uma breve noção da força dos influenciadores digitais, cite-se o canal de Whindersson Nunes⁴³, que conta com mais de 41 (quarenta e um milhões) de inscritos e é disputado por muitos fornecedores para *merchandising* ou outras formas de publicidade de seus produtos.

Vale notar que o espaço dos influenciadores é segmentado e formado por grupos de interesse nas redes sociais, alcançando um público-alvo e chamando a atenção de diferentes marcas que identificam semelhanças entre a audiência do *influencer* e a sua marca.

No entanto, conforme já dissemos, os fornecedores utilizam os influenciadores digitais para difundir suas marcas e produtos, mas muitas vezes não é possível a identificação da publicidade, em total desrespeito ao princípio insculpido no art. 36 do Código de Defesa do Consumidor.

Nesse cenário, a publicidade testemunhal, concebida por meio dos influenciadores digitais, além do *product placement* e do *merchandising*, tem tomado grande parte do mercado publicitário, transformando-se em uma das principais fontes de promoção de produtos e serviços. A sensação de autenticidade passada nas mensagens publicitárias dissimulando relatos pessoais do uso de produtos pode gerar sucesso de vendas dos produtos, mas cria falsa ideia de credibilidade na mente dos consumidores.

Nesse sentido:

O uso dos chamados “influenciadores digitais” é uma importante ferramenta de expansão de marcas, levando ao crescimento dos negócios. De acordo com o Business Insider UK, “o marketing realizado através desses influenciadores pode alcançar um lucro entre \$5 a \$10 bilhões de euros em 2022”. O sucesso do marketing realizado através dos influenciadores digitais se dá em razão da busca pela conexão mais autêntica entre as marcas e seus consumidores. Indiscutivelmente, funciona como uma ferramenta dada ao consumidor, que pode escolher quando e qual informação receber, sem precisar que o mercado o faça por ele. Ao mesmo tempo, marcas baseiam-se na ilusão de proximidade, amizade e confiança que reúne pessoas em uma rede de interesses similares. De acordo com Trzaskowski, o uso de influenciadores pelas empresas cresceu diante da percepção de que consumidores confiam mais nos seus pares do que nelas, o que resultou em combinação de marketing perfeita⁴⁴.

⁴³ Disponível em: <https://www.youtube.com/user/whinderssonnunes/videos>. Acesso em: 20 set. 2021.

⁴⁴ Tradução livre. No original: “The use of digital influencers is now an important tool in the quest to expand a brand and increase business. According to Business Insider UK, ‘influencer marketing ad spend is poised to reach between \$5 billion and \$10 billion in 2022’. The success of digital influencers’ marketing is based on the search for more authenticity in the connections a brand makes with its customers. Arguably, it acts as a “power shift” tool enabling the consumer to choose when and what information to gather, rather than relying on the business to provide the right information. Brands rely on the idea of proximity, the illusion

Denota-se que o mercado publicitário percebeu uma grande oportunidade de introduzir mensagens com intenção promocional de modo discreto e transmitindo credibilidade com os influenciadores digitais.

Isso porque, ao transmitir mensagens por meio dessas pessoas que atraem determinados grupos específicos de consumidor, com estilo de vida compatível com o produto ou serviço anunciado, a credibilidade da mensagem publicitária aumenta consideravelmente.

Além disso, no âmbito da internet, é complexa a prova de possíveis abusos na técnica de publicidade testemunhal, uma vez que a relação financeira entre o influenciador digital e o representante do produto ou serviço nem sempre é clara. A percepção e a prova dessa relação são sempre difíceis de obter e é tênue a linha divisória entre a relação promocional do *influencer* e as suas reais considerações, livres de intenção promocional, sobre o produto ou serviço.

Nesse sentido, Christine Riefa e Laura Clausen afirmam que,

[e]ntretanto, os influenciadores digitais passaram a deixar de esclarecer se a opinião sobre determinado produto ou marca por eles divulgados seria fruto ou não de uma relação comercial com uma empresa. Um dos maiores problemas dessa prática, comum atualmente, reside no fato de que se tornou extremamente difícil de determinar, e ainda mais complicado de provar, que o influenciador foi pago para expressar determinada opinião de um produto ou serviço por alguma empresa. Nesse sentido, o estudo mais recente realizado pela Comissão Europeia revela que consumidores expressam confiança em conseguir determinar quais os conteúdos têm intenção comercial e quais não, enquanto os resultados em relação aos seus comportamentos revelam uma história completamente diferente⁴⁵.

Desse modo, percebemos os desafios que permeiam a fiscalização e aplicação das regras consumeristas no mundo cibernético, induzindo o consumidor a erros em muitas

of connection, friendship and trust that forms in a network of people who share similar interests. According to Trzaskowski the use of influencers has grown due to the realisation that consumers trust their peers more than businesses and thus traders have thought to influence the ‘buzz’ created amongst individuals” (RIEFA, Christine; CLAUSEN, Laura. Towards Fairness in Digital Influencers’ Marketing Practices. **Journal of European Consumer and Market Law (EuCML)**, April 12, 2019. Disponível em: <https://ssrn.com/abstract=3364251>. Acesso em: 20 set. 2021).

⁴⁵ No original: “However, digital influencers have been found to inadequately disclose whether their review or endorsement has been paid for or that they have a financial relationship or interest in connection with any of the products featured. 10 One of the main issues with this practice is that it is very difficult to detect and even harder to prove that someone has been paid by a business to write a specific review. 11 The latest study from the European Commission reveals that consumers are normally confident that they are able to recognise commercial content on social media, but the results of the behavioural experiment tell a different story” (RIEFA, Christine; CLAUSEN, Laura. Towards Fairness in Digital Influencers’ Marketing Practices. **Journal of European Consumer and Market Law (EuCML)**, April 12, 2019. Disponível em: <https://ssrn.com/abstract=3364251>. Acesso em: 20 set. 2021).

situações diante da dificuldade em reconhecer a publicidade oculta em testemunhos de influenciadores digitais.

Tanto assim que o Conar já analisou, nos últimos anos, casos em que a publicidade não era clara ao consumidor. Vejamos:

Caso Authenticgames e Habib's/Ragazzo – Nasceram novos bebês! Minicraft cidade#10

Mês de julgamento: Março/2020

Representação: 301/19

Autor: Conar por iniciativa própria

Anunciante: Authenticgames e Habib's/Ragazzo

Decisão: Sustação e advertência

Fundamento: Artigos 1º, 3º, 6º, 23, 28, 37 e 50, letras “a” e “c”, do Código e seu Anexo H

Ação publicitária com o título acima, **veiculada em redes sociais em canal destinado ao público infantil, carece de clara identificação como publicidade**, conforme recomendado pelo Código em seus artigos 9º e 28. Por isso, a direção do Conar propôs representação ética, questionando também se há estímulo ao consumo excessivo pela associação da refeição e a aquisição de diversas unidades de brinquedo. A Habib's/Ragazzo enviou defesa ao Conar explicando que a veiculação foi ato espontâneo da AuthenticGames, que não enviou manifestação ao Conar.

A relatora iniciou seu voto lembrando que identificar a natureza publicitária de postagens de influenciadores digitais tem sido um grande desafio para a ética publicitária. “Isso porque, na internet, mais conhecida como #terra de ninguém#, em teoria tudo pode”, escreveu ela.

No caso em tela, a relatora considera que a Habib's/Ragazzo não pode se eximir de responsabilidade, até pelo fato de ter outras campanhas publicitárias desenvolvidas com a AuthenticGames, com o mesmo influenciador que aparece na publicidade objeto desta representação.

No mérito, ela deu razão à denúncia, considerando que há falta de clareza sobre a finalidade da peça, apelo imperativo de consumo dirigido a menor de idade e associação antiética entre brinquedo colecionável e o consumo de três refeições compostas por hambúrgueres ou esfihas, refrigerante e batata frita.

Por isso, propôs a sustação da ação agravada por advertência à Habib's/Ragazzo e AuthenticGames. Seu voto foi aceito por unanimidade (grifos nossos).

Caso: Nestlé, Masterfoods, Mondelez, Fini Hershey, Chocolates Garoto e Luccas Neto – Castelo de chocolate com Kit Kat e Oreo

Mês/ano julgamento: Abril/2020

Representação: 040/2020

Autor: Conselho Superior do Conar

Anunciante: Nestlé Brasil, Masterfoods Brasil, Mondelez Brasil, Fini, Hershey do Brasil, Chocolates Garoto e Luccas Neto

Decisão: Advertência ao influenciador e arquivamento da representação em face dos fabricantes

Fundamento: Respectivamente artigos 1º, 3º, 6º, 37 e 50, letra “a”, do Código e seu Anexo “H” e artigo 27, nº 1, letra “a”, do Rice

O Conselho Superior do Conar propôs representação contra ação publicitária em redes sociais do influenciador Luccas Neto, na qual ele se utiliza de guloseimas de vários fabricantes para montar uma miniatura de castelo. A representação foi motivada por denúncia enviada ao Conar pelo Ministério Público do Distrito Federal e Territórios, que questionou se não há estímulo ao consumo excessivo de doces por crianças e adolescentes e se a natureza publicitária da ação está claramente expressa.

Todas as fabricantes, excetuando-se a Hersheys, enviaram defesa ao Conar, nas quais informam não terem participado de qualquer forma da ação objeto

desta representação. O influenciador também enviou defesa, em que ratifica a informação de que as fabricantes não solicitaram ou pagaram pela ação, sendo ela de sua livre iniciativa.

Para a relatora, restou demonstrado que não se tratou de publicidade contratada, tampouco de conteúdo patrocinado, pelo que propôs o arquivamento da denúncia contra as fabricantes.

Em relação ao influenciador Luccas Neto, a relatora recomendou a advertência. Seu voto foi aceito por unanimidade.

Mês/Ano Julgamento: Junho/2019

Representação n°: 106/18, em recurso extraordinário

Autor(a): Conar mediante queixa de consumidor

Anunciante: Ferrero do Brasil e Luccas Neto

Decisão: Alteração e advertência

Fundamentos: Artigos 1º, 3º, 6º, 9º, 28, 30, 37 e 50, letra “a”, do Código e seu Anexo H

Queixa de consumidora residente em Guariba (SP) motivou esta representação, contra vídeo veiculado em redes sociais no qual o influenciador Luccas Neto desembala 50 Kinder Ovos. Acompanhado por uma criança, ele vai mostrando os brinquedos contidos dentro dos ovos e ingerindo uma grande quantidade de chocolate. Para a consumidora, há claro desrespeito na peça publicitária em relação às recomendações do Código para a publicidade de produtos e serviços destinados a menores de idade. Além disso, como notou a direção do Conar, cabe questionamento sobre a correta identificação publicitária do anúncio.

Em sua defesa, o influenciador negou tratar-se de publicidade e sim de *unboxing*, formato corriqueiro no meio. Informou não ter sido contratado pela Ferrero, tendo ele próprio adquirido os produtos mostrados. Estas informações foram ratificadas em defesa enviada pela Ferrero.

Tais alegações convenceram os integrantes da Segunda e Quarta Câmaras que, por maioria de votos, deliberaram pelo arquivamento da representação, seguindo proposta do relator.

A direção do Conar recorreu da decisão levando-a à Câmara Especial de Recursos. Lá, por maioria de votos, deliberou-se pela alteração agravada por advertência aos anunciantes, atendendo à proposta do autor do voto divergente. Ele levou em conta a natureza do produto – uma guloseima destinada a crianças de pouca idade –, o evidente estímulo ao consumo exagerado do produto e o fato de a Ferrero não ter adotado qualquer providência para retirar o vídeo do ar, o que lhe seria possível, dado ser a proprietária da marca.

Apenas a Ferrero recorreu da decisão, apoiando o seu pedido no fato de ter ficado comprovado que ela não contratou a veiculação. Estas e outras alegações não convenceram a maioria dos 48 conselheiros que participaram da reunião plenária do Conselho de Ética, onde são julgados os recursos extraordinários. Por 20 votos a 18, deliberou-se pela manutenção da recomendação anterior.

Ainda nesse sentido, com a pandemia do Coronavírus, um fenômeno foi percebido e consolidado entre consumidores na internet: diante das medidas de distanciamento social, quarentenas e *lockdown*, houve aumento e fortalecimento das chamadas *lives*, realizadas por intermédio das redes sociais, que movimentaram artistas e empresas, trazendo novas formas de publicidade através das pessoas públicas.

Ainda de acordo com Michael César Silva, Caio César do Nascimento Barbosa e Glayder Daywerth Pereira Guimarães:

No Brasil, patrocinadores vislumbraram as *lives* de artistas como meio altamente rentável de promover seus produtos e serviços. Enquanto, a

plataforma do Instagram conta com o recurso para promoção de aulas, lançamento de livros, bate-papos descontraídos ou explicativos, exercícios de ginástica, etc., o YouTube se tornou uma ferramenta com escopo de proporcionar a realização de “shows em casa” por artistas, que se encontram impedidos de realizar suas apresentações devido ao Coronavírus, com a indústria do entretenimento sendo o setor que mais passou a utilizar o referido recurso.

Segundo a revista EXAME, as buscas pelas *lives* na plataforma do YouTube cresceram 4.900% no Brasil durante a quarentena, as quais se converteram em eventos diários, em que as pessoas passaram a acompanhar de forma pontual as transmissões ao vivo dos artistas, popularizando-as. O YouTube, inclusive, criou a campanha “#Fique em Casa e Cante Comigo”, proporcionando uma coletânea de shows exibidos em tempo real, com diversos artistas⁴⁶.

A título exemplificativo, os autores destacam o ocorrido com Gustavo Lima, que alcançou a posição de cantor brasileiro com mais seguidores na rede social *Instagram*, justamente em razão de suas primeiras *lives*, que lhe proporcionaram grande notabilidade, culminando, inclusive, em Representação Ética no Conar (RE n. 078/20), com vistas a apurar a integridade das ações publicitárias incluídas em suas *lives*.

Nessa toada, de acordo com os autores,

[a] Representação Ética nº 078/20 foi instaurada após dezenas de denúncias de consumidores ao CONAR, que, ao analisar, julgou pela necessidade de abertura por dois motivos: i) falta de identificação clara do público-alvo, uma vez que não possuía restrições a menores de idade; ii) influência ao consumo exagerado e irresponsável de bebidas alcoólicas, contrário ao anexo “P” do Código Brasileiro de Autorregulamentação Publicitária (CBAP), que assevera a necessidade de responsabilidade social nos anúncios publicitários, que não devem induzir o exagerado ou irresponsável consumo de bebidas alcoólicas⁴⁷.

Nesse sentido, necessário ressaltar a discussão concernente à possibilidade de responsabilidade civil do influenciador em relação à ocorrência de danos advindos da veiculação de publicidade ilícita no mercado de consumo digital.

De acordo com Michael César Silva, Caio César do Nascimento Barbosa e Glayder Daywerth Pereira Guimarães,

[e]m consonância com exposto, o digital influencer, também, deverá observar nessas relações jurídicas e, em sua atuação no mercado de consumo digital, os preceitos normativos da função social dos contratos – consagrada no artigo 421 do Código Civil – sendo igualmente reconhecida como norma de ordem pública e de interesse social.

Destarte, as relações jurídicas e socioeconômicas necessitam, de modo imperioso, atentarem-se ao interesse coletivo como forma de preservar o

⁴⁶ SILVA, Michael César; BARBOSA, Caio César do Nascimento; GUIMARÃES, Glayder Daywerth Pereira. Responsabilidade civil dos influenciadores digitais em tempos de coronavírus. *In*: LONGHI, João Victor; FALEIROS JÚNIOR, José Luiz de Moura; GUGLIARA, Rodrigo. **Proteção de dados pessoais na sociedade da informação**: entre dados e danos. Indaiatuba: Foco, 2021. p. 314.

⁴⁷ SILVA, Michael César; BARBOSA, Caio César do Nascimento; GUIMARÃES, Glayder Daywerth Pereira. Responsabilidade civil dos influenciadores digitais em tempos de coronavírus. *In*: LONGHI, João Victor; FALEIROS JÚNIOR, José Luiz de Moura; GUGLIARA, Rodrigo. **Proteção de dados pessoais na sociedade da informação**: entre dados e danos. Indaiatuba: Foco, 2021. p. 314.

contexto social que priorize a sociedade como um todo e não apenas os interesses meramente individualistas. Nesse giro, os efeitos sociais decorrentes da relação entre anunciante e fornecedor devem ser compatibilizados aos seus interesses exclusivos, resguardando-se a coletividade de eventuais condutas inadequadas que porventura possam vir a causar danos.

Portanto, toda e qualquer publicidade veiculada no mercado de consumo pelos influenciadores digitais, deverá considerar os princípios da boa-fé objetiva e da função social dos contratos, sob pena de imputação de responsabilidade civil⁴⁸.

Os autores completam salientando a diferença entre o caráter “roteirizado” das celebridades, que recebem um *script* ou *briefing* do produto ou serviço, emprestando a representação do seu nome e imagem para promover a marca, e o caráter livre da publicidade vinculada aos influenciadores digitais, que possuem uma maior liberdade criativa para desenvolver o roteiro publicitário.

2.4.1. Conar: o manual de boas práticas para influenciadores digitais

Diante da quantidade de casos envolvendo a publicidade feita por influenciadores digitais, e na tentativa de amenizar os problemas e as discussões daí advindos, o Conar lançou, em 8 de dezembro de 2020, um guia de publicidade para influenciadores digitais.

O Guia foi elaborado pelo Grupo de Trabalho para a Publicidade Digital, que contou com a participação de especialistas, representantes da Associação Brasileira dos Anunciantes (ABA), da Associação Brasileira das Agências de Publicidade (Abap), da Associação Brasileira das Emissoras de Rádio e Televisão (Abert), da Interactive Advertising Bureau Brasil (IAB) e do Conselho de Ética e Corpo Técnico do Conar.

O documento define a publicidade por influenciador⁴⁹ e estabelece três elementos essenciais para que se configure publicidade:

Em geral, três elementos cumulativos são necessários para caracterizar a referida publicidade:

- i) a divulgação de produto, serviço, causa ou outro sinal a eles associado;
- ii) a compensação ou relação comercial, ainda que não financeira, com Anunciante e/ou Agência; e
- iii) a ingerência por parte do Anunciante e/ou Agência sobre o conteúdo da mensagem (controle editorial na postagem do Influenciador).

O terceiro requisito previsto, a ingerência por parte do Anunciante e/ou Agência, também chamada de controle editorial, configura a contratação

⁴⁸ SILVA, Michael César; BARBOSA, Caio César do Nascimento; GUIMARÃES, Glayder Daywerth Pereira. Responsabilidade civil dos influenciadores digitais em tempos de coronavírus. *In*: LONGHI, João Victor; FALEIROS JÚNIOR, José Luiz de Moura; GUGLIARA, Rodrigo. **Proteção de dados pessoais na sociedade da informação**: entre dados e danos. Indaiatuba: Foco, 2021. p. 320.

⁴⁹ “**Publicidade por Influenciador**: é assim considerada para a autorregulamentação publicitária a mensagem de terceiro destinada a estimular o consumo de bens e/ou serviços, realizada pelos chamados Influenciadores Digitais, a partir de contratação pelo Anunciante e/ou Agência.”

(formal ou informal), por meio da qual se solicite ou sugira a divulgação publicitária, com maior ou menor detalhamento de conteúdo, tempo, frequência ou forma de postagem a serem propostos ao Influenciador. Não é considerado controle editorial o mero contato do Anunciante junto ao Usuário, com a simples apresentação do produto, orientação quanto ao consumo ou cuidados necessários no caso de sua eventual e incerta divulgação, em observância às normas éticas e legais aplicáveis⁵⁰.

Sendo assim, em qualquer publicidade feita em meio digital por meio de influenciador, é essencial que seja informado o conteúdo publicitário ao consumidor, tudo graças ao princípio da identificação da publicidade, já amplamente estudado⁵¹.

De se notar que o Conar entende absolutamente necessária a ingerência do fornecedor no conteúdo publicitário, bem como a compensação financeira, ainda que seja na forma de cupom de desconto, envio de produtos ou pagamento em dinheiro. Assim, nas hipóteses em que o *influencer* não tenha sido previamente contratado pelo fornecedor para fazer a publicidade do produto ou serviço, não há falar em publicidade.

A questão é delicada e merece atenção. De fato, não se pode impedir que pessoas utilizem os canais de redes sociais (Youtube, Instagram, Facebook) para falar sua opinião a respeito dos produtos e serviços colocados no mercado de consumo. Ora, sendo essa opinião positiva, mesmo que sem autorização expressa do fabricante, não se pode impedir a fala do consumidor, desde que este, de fato, trate do produto ou serviço de forma verdadeira e sem desrespeitar os limites legais estabelecidos para a publicidade.

Do mesmo modo, sendo a opinião negativa ou neutra, também não se pode tolher a liberdade de expressão do consumidor para fazê-lo através de redes sociais, desde que,

⁵⁰ Disponível em: <http://conar.org.br/index.php?codigo&pg=influenciadores>. Visita em 20 set. 2021.

⁵¹ Sobre a identificação da publicidade, orienta o Manual: “1.1 **Identificação**: o referido conteúdo deve ser claramente identificado como publicitário. Quando não estiver evidente no contexto, é necessária a menção explícita da identificação publicitária, como forma de assegurar o cumprimento deste princípio, por meio do uso das expressões: ‘publicidade’, ‘publi’, ‘publipost’ ou outra equivalente, conforme exemplos na tabela anexa, considerando o vocábulo que for compreensível para o perfil de seguidores com quem se pretende comunicar. Levando em conta o volume e diversidade de conteúdos nas redes, enfatiza-se a necessidade atual de adoção padronizada da aplicação dos termos ou ferramentas de identificação publicitária, como forma de garantir a pronta percepção sobre a natureza da mensagem divulgada. 1.1.1 **Forma**: sempre que possível, é recomendável o uso de ferramenta de identificação disponibilizada pelas plataformas. Alternativamente, recomenda-se a menção explícita dos termos indicados, de forma ostensiva e destacada, podendo tal menção ser feita em qualquer elemento das postagens, inclusive legenda, desde que a informação sobre a natureza publicitária seja visível de plano, sem, entretanto, prejudicar a mensagem publicitária. 1.1.2 **Crianças e adolescentes**: considerando a característica da publicidade por influenciadores, imersa ou integrada ao conteúdo editorial circundante, todos os envolvidos na divulgação da publicidade devem ser particularmente cuidadosos para que a identificação da natureza publicitária seja aprimorada, assegurando o reconhecimento pelas crianças e adolescentes do intento comercial, devendo ser perceptível e destacada a distinção da publicidade em relação aos demais conteúdos gerados pelo influenciador”.

da mesma forma, sejam observados os limites legais e que a opinião seja embasada em fatos reais.

No entanto, entendemos que deve o fornecedor notificar o influenciador sempre que estiver ciente do uso indevido da sua marca, ou em situações recorrentes de falta de respeito à legislação vigente⁵².

Sobre recebimento de brindes, cortesia, convites e afins, embora o Conar compreenda que não há filtragem do conteúdo por parte do fornecedor, o envio dos “mimos” ao influenciador deve ser informado ao consumidor. Vejamos a orientação do manual:

2. Mensagem Ativada (“recebidos/brindes”): é assim considerada a referência feita por Usuário a produto, serviço, causa ou outro sinal característico a eles associado, a partir de conexão ou benefício não remuneratório oferecido por Anunciante ou Agência, sem que tenha havido controle editorial sobre a referência. Exemplificadamente: as postagens de retribuição, agradecimento por brindes (“recebidos”), viagens, hospedagens, experiências, convites, etc. Para os fins da autorregulamentação publicitária, os referidos conteúdos não configuram anúncios, por não possuírem natureza comercial, com os três requisitos acima descritos. Entretanto, considerando que tal conteúdo submete-se ao princípio da transparência, ao direito à informação e tendo em conta que tal conexão ou benefício pode afetar o teor da mensagem, é necessária a menção da relação que originou a referência. Pode ser necessária, ainda, a orientação pelo Anunciante e/ou Agência, a ser observada pelo Influenciador, acerca da regulamentação aplicável.

2.1. Engajamento: pode inserir-se nesta modalidade o conteúdo gerado pelo Usuário mediante oferta de brindes ou benefícios por meio de ações promocionais, concursos, “desafios” ou assemelhados que estimulem a postagem do Usuário a partir de engajamento. Para a conformidade da publicidade dos Anunciantes e suas marcas que promovam a ativação de tais postagens é peça chave que esteja baseada em mecânicas promocionais compatíveis com a regulamentação de distribuição gratuita de prêmios e que reflita o respeito às regras do Código Guia de Orientação – Publicidade Por Influenciadores de Autorregulamentação, no quanto aplicável e, em particular, para os segmentos sensíveis ou com restrição de consumo.

⁵² É nesse sentido a orientação do Manual: “3. **Conteúdo Gerado pelo Usuário sem relação com o Anunciante ou Agência:** em regra, a menção de produtos, serviços, marcas, causas e/ou sinais característicos pelos Usuários, feita de modo espontâneo (sem que tenha sido precedida de qualquer interação, comunicação ou contato com o Anunciante e/ou a Agência) não constitui publicidade. A conduta ativa dos Anunciantes e Agências compartilhando as mensagens de usuário em seus próprios perfis e canais oficiais implica em divulgação autônoma, deixando de constituir mera postagem do usuário, configurando tal postagem do Anunciante novo conteúdo de natureza publicitária e sujeito a conformar-se a todas as regras aplicáveis. 3.1 **Boas práticas:** nos segmentos sensíveis ou que possuam restrição de comercialização, consumo e divulgação comercial, o Anunciante poderá, ao ser notificado de possível conteúdo irregular postado por usuário, considerar a importância de enviar mensagem educativa ao autor da postagem sobre a regulamentação existente ou, quando membro do CONAR, beneficiar-se da assessoria da entidade para tal contato. Também se inserem nesta sessão as interações realizadas pelos perfis oficiais de Anunciantes com conteúdos gerados por Usuários (comentários, curtidas/‘likes’, entre outras interações). Caso se venha *a posteriori* apurar que aquele conteúdo abranja divulgação potencialmente prejudicial envolvendo marcas e produtos identificáveis, poderá ser considerada a importância da adoção das medidas disponíveis para alteração ou remoção do endosso (curtida, comentário ou outras formas de interação) por parte dos perfis oficiais de Anunciantes, também neste caso com a possibilidade de ele, quando membro do CONAR, recorrer à assessoria da entidade para o contato com o autor da postagem original”.

O manual ainda reforça a necessidade de os influenciadores respeitarem a legislação específica sobre publicidade no Brasil, e obriga os fornecedores a oferecerem orientações necessárias ao cumprimento das normas, nos seguintes termos:

1.2 **Regras gerais e específicas do CBAP:** aplicam-se ao teor das publicidades por Influenciadores contratados, devendo o Anunciante e/ou a Agência envidar os maiores esforços e adotar as melhores práticas para informar o Influenciador sobre os cuidados que devem acompanhar a divulgação e zelar pelo cumprimento das regras. Fica também o Influenciador incumbido do conhecimento e conformidade com as normas aplicáveis, em especial que o seu depoimento, ao retratar uma experiência pessoal, seja genuíno e contenha apresentação verdadeira do produto ou serviço anunciado.

Por fim, vale notar que, em relação à publicidade digital dirigida ao público infantil, o Ministério Público de São Paulo e a Google do Brasil firmaram termo de composição para adequar a publicidade destinada ao público infantil no meio digital.

O termo de composição foi firmado em ação civil pública em que se discutia publicidade dirigida ao público infantil. A ação havia sido proposta pelo Ministério Público do Estado de São Paulo contra a Google do Brasil pelo uso de estratégias abusivas de publicidade dirigida ao público infantil, realizada por meio da campanha “Você Youtuber Escola Monster High”.

De acordo com o documento, a Google e o Conar produzirão um Manual de Boas Práticas com foco em publicidade infantil no ambiente digital, que deverá conter princípios gerais norteadores da publicidade direcionada ao público infantil na internet, bem como casos hipotéticos ilustrativos que representem um rol exemplificativo de formas adequadas de comunicação publicitária dirigida às crianças. Por fim, salienta-se que ainda não se tem notícia da entrega e análise do Manual de Boas Práticas voltado para o público mirim.

3. Da Lei Geral de Proteção de Dados Pessoais

A Lei Geral de Proteção de Dados Pessoais (LGPD), reconhecendo a vulnerabilidade de todas as pessoas em relação ao tratamento de suas informações pessoais, foi aprovada com a finalidade de trazer um **dirigismo informacional**, conforme

afirma Bruno Ricardo Bioni⁵³, e busca corrigir a assimetria e garantir a autonomia do cidadão no que se refere aos seus dados pessoais.

Impossível não reconhecer a maior vulnerabilidade de crianças e adolescentes nessa seara, dada a ausência de capacidade civil para a compreensão de seu conteúdo e alcance. Por essa razão, a Lei nº 13.709/2018, em consonância com a Constituição Federal, com o Estatuto da Criança e do Adolescente e com o Código Civil, reservou espaço para tratar da proteção da criança e do adolescente. Vejamos:

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

O dispositivo é amplo e merece atenção especial do intérprete. Em primeiro lugar, vamos trabalhar o significado e alcance do “princípio do melhor interesse” em relação à proteção de dados pessoais bem como os destinatários da proteção legal, a extensão e forma do consentimento para o tratamento dos dados dos infantes.

⁵³ “Conclui-se que as relações do mercado de consumo demandam um novo tipo de dirigismo – *dirigismo informacional* – que se afasta daquele do século passado – dirigismo contratual. Deve haver uma *releitura ambivalente* do paradigma da autodeterminação informacional – *procedimental e substantiva* – que embora mantenha o papel de protagonismo do consentimento, empresta-lhe um novo roteiro normativo: *a percepção de que o titular dos dados pessoais amarga uma (hiper)vulnerabilidade, o que demanda, respectivamente, o seu empoderamento para emancipá-lo e a sua intervenção para assisti-lo*” (BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. p. XXVII).

3.1. O melhor interesse e a proteção dos dados pessoais

Já vimos que o princípio do melhor interesse é de suma importância na seara do direito de infância e, ao mesmo tempo, é conceito vago e enfrenta inúmeras dificuldades de aplicação no caso concreto.

Conforme dissemos, o melhor interesse não deve ser visto como princípio orientador para o alcance da felicidade, mas a garantir a individualidade, a autonomia progressiva e o desenvolvimento de cada criança, o que deve ser amplamente aplicado à proteção de dados.

Assim, a Lei Geral de Proteção de Dados Pessoais andou bem ao inserir o princípio do melhor interesse em relação à proteção e ao tratamento de dados pessoais, tendo em vista a autonomia progressiva da criança e do adolescente no que se refere às suas informações pessoais e à necessidade de proteção pelos pais ou responsáveis.

Por outro lado, a aplicação do princípio pode gerar dúvidas quanto ao efetivo direcionamento a ser oferecido aos dados pessoais. Poderiam, por exemplo, os dados pessoais de crianças e adolescentes que estão à espera de adoção ser objeto de tratamento por parte do controlador e do operador? A resposta é afirmativa, com o devido cuidado e a preservação da sua identidade, nos termos do art. 101 do Estatuto da Criança e do Adolescente e do art. 7º, inciso IV e § 3º, da Lei Geral de Proteção de Dados Pessoais.

Ademais, o tratamento desses dados deve ser direcionado ao melhor interesse da criança, isso porque tais informações são de suma importância para a análise da situação de crianças e adolescentes que estão em medidas de proteção e desenvolvimento de políticas públicas voltadas para essa faixa etária.

O mesmo deve ser dito em relação aos casos de violência, desistência escolar, vacinação, saúde e outras informações de cunho pessoal. Todos esses dados são de extrema importância para o direcionamento das políticas públicas voltadas para a infância e adolescência⁵⁴, tudo em consonância com o art. 7º, III, IV, VII e VIII, da Lei Geral de Proteção de Dados Pessoais.

⁵⁴ Indiscutível a utilização de dados pessoais para a formulação de políticas públicas. Sobre o assunto, assevera Ricardo Alexandre de Oliveira: “Pensemos, por exemplo, nas *smart cities*, termo comumente utilizado para cidades com alto grau de automação e conexão por meio da internet das coisas (IoT) em serviços de interesse público, como trânsito, serviço de saúde ou infraestrutura urbana. Diferentemente do que poderíamos encontrar há algumas décadas atrás, atualmente um agente público pode dispor de informações importantes para a sua gestão na palma de sua mão, incluindo dados pessoais. Tal fato não é negativo, se considerarmos que o acesso à informação por um gestor público possibilitaria, se houvesse interesse político, o aumento de grau de eficiência do Estado” (OLIVEIRA, Ricardo Alexandre de. Lei

Por outro lado, conhecendo o seu público por meio das informações pessoais, os fornecedores poderiam oferecer, com melhor direcionamento, novos produtos e serviços, bem como atuar de forma mais eficiente na publicidade e oferta para o público infantil, o que poderia desrespeitar o princípio do melhor interesse.

Já analisamos a necessidade de cuidados em relação às mensagens publicitárias direcionadas ao público infantil nos meios digitais, de modo que a criança possa identificar o caráter publicitário das mensagens patrocinadas.

Além disso, na publicidade digital, os dados das crianças não podem ser capturados sem o consentimento dos pais, muito menos para direcionar mídias de “seu interesse” ou fundamentadas em seus “hábitos de navegação”, vedado ainda o direcionamento para *links* ou URLs comerciais de produtos e serviços.

3.2. Os destinatários da Lei Geral de Proteção de Dados Pessoais

Conforme dissemos, o *caput* do art. 14 da Lei nº 13.709/2018 afirma que o tratamento de dados pessoais de **crianças** e de **adolescentes** deverá ser realizado em seu melhor interesse, nos termos do referido artigo e da **legislação pertinente**.

A **legislação pertinente** referida pelo dispositivo legal deve ser entendida, essencialmente, como o Estatuto da Criança e do Adolescente e o Código Civil. Isso porque a lei menorista trouxe um rol de direitos fundamentais que deve ser respeitado em relação aos dados pessoais dos destinatários, e o Código Civil trata da teoria das incapacidades e do exercício de poder familiar.

Por outro lado, o § 1º do art. 14 da Lei Geral de Proteção de Dados Pessoais dispõe que o tratamento de dados pessoais de **crianças** deverá ser realizado mediante consentimento específico e em destaque por pelo menos um dos pais ou pelo responsável legal.

Da dicção legal podemos entender que a lei brasileira optou por não exigir o consentimento específico dos pais ou responsável para os **adolescentes** com a finalidade de tratamento dos dados pessoais. Sendo assim, é possível afirmar que o consentimento do próprio adolescente pode ser considerado suficiente para o tratamento dos seus dados? O dispositivo deve ser analisado à luz da sistemática do Estatuto da Criança e do Adolescente e do Código Civil.

3.3. Consentimento na Lei Geral de Proteção de Dados Pessoais

O art. 7º da Lei Geral de Proteção de Dados Pessoais determina que o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

- I – mediante o fornecimento de consentimento pelo titular;
- II – para o cumprimento de obrigação legal ou regulatória pelo controlador;
- III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
- IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária
- IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
- X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Por outro lado, o art. 5º, XII, define consentimento como a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”.

Demais disso, determina a lei que o consentimento deve ser fornecido por escrito, com cláusula destacada das demais cláusulas, ou por outro meio que demonstre a manifestação de vontade do titular (art. 8º). O ônus da prova de que o consentimento foi obtido em conformidade com a lei é do controlador (art. 8º, § 2º), sendo vedado o tratamento de dados pessoais mediante vício de consentimento (art. 8º, § 3º).

Adverte Bioni que a Lei Geral de Proteção de Dados Pessoais adjetivou o consentimento (livre, informado e inequívoco), exigindo dois elementos essenciais para ser considerado válido: o dever-direito a informação clara, transparente útil ao indivíduo, com uma quantidade suficiente de elementos para permitir que o consumidor saiba das qualidades e características do bem de consumo e, ainda, a sua utilização atenta aos riscos que lhe possam sobrevir⁵⁵.

⁵⁵ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. p. 193.

O mesmo autor esclarece que a Lei Geral de Proteção de Dados Pessoais utiliza adjetivos específicos para o consentimento em determinadas situações: i) quando há envolvimento de terceiros (art. 7º, § 5º); ii) em razão da natureza do dado coletado (art. 11, I); iii) quando envolve crianças e adolescentes (art. 14º, § 1º; iv) na transferência internacional para um país sem o mesmo nível de proteção de dados que o Brasil (art. 33, III).

De fato, quando exigido, o consentimento é o fundamento essencial para a autodeterminação do sujeito em relação aos seus direitos de personalidade. Analisaremos, agora, o consentimento de crianças e adolescentes pela Lei Geral de Proteção de Dados Pessoais.

3.3.1. Consentimento de crianças e adolescentes

Conforme dissemos, a regra para o tratamento de dados é o consentimento livre, informado e inequívoco, conferido pelo seu titular (art. 7º, I). Por exceção, o consentimento não será exigido nas hipóteses expressas da lei (art. 7º, II a X). Evidentemente, o mesmo dispositivo se aplica aos direitos da criança e do adolescente, razão pela qual, nas hipóteses previstas em lei, não será necessário o consentimento para o tratamento dos dados.

Mais ainda, o art. 14, § 3º, prevê a possibilidade de coleta de dados pessoais de crianças sem o consentimento quando ela for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção. Nessas hipóteses, nenhum dado pode ser repassado a terceiros sem o consentimento dos pais ou responsável.

Por outro lado, dispõe o art. 14, § 1º, que “o tratamento de dados pessoais de **crianças** deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal” (grifo nosso).

Eis o dispositivo que pode causar polêmica e dificuldade de interpretação. Ora, pela regra do art. 14, § 1º, os **adolescentes** não precisariam dar expressa anuência para coleta e tratamento dos dados. Com isso, menores impúberes (entre 12 e 16 anos) estariam aptos, conforme a lei, a consentir sem a representação paterna, e os relativamente incapazes (entre 16 e 18 anos), da mesma forma, não precisariam de assistência dos pais ou do representante legal.

Aparentemente não se equivocou na redação da norma que dispensa a assistência ou representação dos adolescentes, razão pela qual a leitura imediata da lei nos leva ao entendimento de que não se fez necessária a presença dos pais ou responsável quando o titular dos dados for adolescente, podendo o consentimento ser por ele oferecido.

Conferiu, portanto, a lei autonomia maior ao adolescente que o próprio Código Civil e o Estatuto da Criança e do Adolescente. No entanto, é necessária cautela na interpretação do dispositivo.

Na hipótese de a coleta e o tratamento de dados advirem de um negócio jurídico como, por exemplo, um contrato de prestação de serviços escolares, ainda que destinado aos adolescentes, a coleta do consentimento deve ser colhida junto com a assinatura do contrato. Isso porque as informações são provenientes de um contrato que depende de representação ou assistência dos pais, sob pena de nulidade ou anulabilidade do ato. A coleta de dados, nesse caso, é acessória ao contrato principal, devendo ser observados os requisitos do negócio jurídico principal.

Ademais, em qualquer hipótese, os dados de crianças e adolescentes devem respeitar o princípio do melhor interesse e a sua progressiva autonomia. Certamente, a casuística ajudará a trazer mais esclarecimentos ao longo da aplicação da lei, em especial quanto ao consentimento.

Outra advertência trazida pelo art. 14, § 4º, é de que o controlador não deve condicionar o consentimento à participação de crianças (e também adolescentes?)⁵⁶ em jogos ou em outros aplicativos disponíveis na internet, salvo as informações estritamente necessárias à atividade oferecida. A barganha aceita entre pessoas maiores e capazes não pode ser aqui exercida, dada a maior vulnerabilidade do grupo.

3.3.2. Forma de coleta e controle

O art. 14 da Lei Geral de Proteção de Dados Pessoais também determina que os controladores deverão manter pública a informação sobre os tipos de dados coletados,

⁵⁶ “Reiterando os princípios da finalidade, necessidade e adequação, nesse parágrafo consta que qualquer tratamento de dados de crianças, especialmente em jogos e pela internet, deve se restringir ao mínimo necessário. Entendemos que essa obrigação também pode se estender ao tratamento de dados de adolescentes, uma vez que se trata de natural extensão dos princípios da finalidade, necessidade e adequação, os quais têm ampla aplicação” (MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2019. p. 210).

bem como a sua forma de utilização e os procedimentos para o exercício de acesso e correção dos dados (art. 14, § 2º).

Sendo assim, deve o controlador esclarecer de forma inequívoca aos pais e responsáveis quais dados estão sendo coletados e de que forma serão utilizados. Não é demais lembrar que a utilização estará sempre sujeita ao melhor interesse da criança e do adolescente.

Outra questão relevante que toca a forma e o tratamento dos dados diz respeito à comunicação com o público infantil. Vejamos a redação do § 6º do art. 14:

As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Assim, sugere-se que os controladores utilizem imperativos como “fale com a mamãe e com o papai” ou mesmo cores e animações para advertir que as crianças devem se reportar aos pais para que estes apresentem o consentimento.

3.3.3. Do Marco Civil da Internet

Nessa toada, vale lembrar que o Marco Civil da Internet⁵⁷ também revelou preocupação do legislador com o uso da internet pelos menores e reforça a obrigação dos pais no dever de cuidado com os filhos. Nesse sentido, o art. 29 do Marco Civil da Internet deixa livre aos pais a opção de instalar *softwares* colocados no mercado de consumo batizados de *parental control* (ou controle parental) e que são extremamente úteis para a orientação do conteúdo na internet.

Em rápida pesquisa sobre esses dispositivos, podemos verificar algumas importantes funcionalidades. Com eles, os pais podem definir limite de tempo de utilização do computador; impedir que a criança execute programas específicos não desejados pelos pais; filtrar ou bloquear as ferramentas de diálogo *on-line*; filtrar e bloquear *sites* catalogados em categorias consideradas não adequadas, tais como *sites* de

⁵⁷ “Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei nº 8.069, de 13 de julho de 1990. Parágrafo único. Cabe ao Poder Público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações sobre o uso de programas de computador previstos no *caput*, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes.”

violência, sexo, nudez, racismo, pornografia; bem como escolher os jogos que as crianças podem brincar (de acordo com a classificação etária), entre outros.

De forma acertada, o legislador deixou a critério dos pais a instalação de *softwares* para monitoramento e orientação dos filhos (crianças e adolescentes); todas as funcionalidades aqui descritas não cerceiam a liberdade dos menores e asseguram o uso com privacidade e cautela.

Entre as funcionalidades dos *softwares* colocados no mercado de consumo, existe a possibilidade de escolher os jogos que as crianças podem brincar de acordo com a classificação etária do entretenimento. Destacamos, igualmente, a necessidade de manter a classificação indicativa de filmes e outras obras audiovisuais na internet.

Seria de bom tom que os *softwares* também pudessem identificar os endereços eletrônicos e aplicativos que coletam e tratam os dados pessoais e de que forma o fazem, para que os pais pudessem ser imediatamente advertidos de seus termos.

4. Proteção de dados *on-line* nos Estados Unidos

A regulação americana é apresentada em três diferentes documentos: o CIPA (Children's Internet Protection Act: governs the filtering of Internet access and digital citizenship education)⁵⁸, o FERPA (Family Educational Rights and Privacy Act) e o COPPA (Children's Online Privacy Protection Act).

O CIPA é o regulamento que trata da proteção de crianças na internet, em especial da filtragem do acesso e uso adequado da rede, e dispõe sobre educação e cidadania digital. É aplicável aos serviços de tecnologia que gerenciam medidas de proteção além de ser aplicável aos funcionários distritais, incluindo professores e funcionários de apoio, que são responsáveis por monitorar o uso, pelos alunos, recursos de tecnologia e educação dos alunos sobre o comportamento *on-line* adequado na rede.

O documento exige que cada distrito use a denominada “medida de proteção de tecnologia” (filtro de internet) para filtrar todos os dispositivos conectados à internet e bloquear o acesso a representações visuais consideradas obscenas ou prejudiciais a menores e a pornografia infantil

Os distritos também devem adotar políticas que abordem o monitoramento das atividades *on-line*, a segurança e proteção de dados de todas as formas de comunicação

⁵⁸ Disponível em: <https://www.fcc.gov/consumers/guides/childrens-internet-protection-act>. Acesso em: 20 set. 2021.

eletrônica direta, devem ocupar-se do acesso *on-line* não autorizado (*hacking* e outras atividades ilegais), da divulgação não autorizada ou informações de identificação pessoal, bem como educar os alunos sobre o comportamento *on-line* adequado (cidadania digital).

O FERPA regulamenta a privacidade informativa das crianças e da família e é aplicável às agências ou instituições educacionais públicas e privadas que recebem fundos por meio de programas específicos administrados pela Secretaria de Educação dos Estados Unidos.

Nesse sentido, o documento garante aos pais o acesso aos registros educacionais de seus filhos, para que estes acompanhem a vida escolar e, eventualmente, para que haja correção das informações sempre que necessário. Ademais, a escola deve ter, entre outras obrigações, o consentimento do aluno quando este completa 18 (dezoito) anos para eventual divulgação dos registros educacionais.

O COPPA, inserido no Título de Práticas Comerciais do Federal Trade Commission⁵⁹ (FTC) em 1998, traz disposições sobre a coleta de dados pessoais de crianças, bem como sobre outras práticas relacionadas à privacidade do público infantil na internet.

A proteção dos dados das crianças começou a ser discutida naquele país diante das oportunidades que surgiram na mídia ao coletar informações pessoais com intenção de dirigir publicidade a esse público. Diante do fato de a criança não compreender de pronto a intenção da coleta de dados, foi necessário criar mecanismos de proteção à sua privacidade.

O COPPA criou regras específicas para proteção de crianças com menos de 13 (treze) anos, envolvendo a coleta de dados e práticas que requerem privacidade em *websites*, aplicativos e outras páginas *on-line*. Para os fins das regras dispostas no COPPA, **criança é toda pessoa que tenha menos de 13 (treze) anos de idade**. Ainda assim, é expressa a recomendação de que o operador também observe as diretrizes do COPPA de coleta e uso dos dados de adolescentes dos 13 (treze) aos 16 (dezesesseis) anos.

Adam Thierer⁶⁰ ressalta que a questão do consentimento não é pacífica naquele país e informa que nos últimos anos alguns Estados propuseram expandir o regime do COPPA de várias maneiras. Esses esforços tentaram expandir a estrutura de consentimento dos pais para incluir todos os menores até os 18 (dezoito) anos, ampliando

⁵⁹ Disponível em: <https://www.ftc.gov>. Acesso em: 20 set. 2021.

⁶⁰ THIERER, Adam. **Kids. Privacy, Free Speech and the Internet: Finding the Right Balance**. Disponível em: <http://ssrn.com/abstract=1909261>. Acesso em: 20 set. 2021.

o leque de *sites* atendidos, aumentando a quantidade de informações que devem ser coletadas para obter o consentimento verificável dos pais, entre outras sugestões.

O autor informa que nenhuma dessas reformas foi implementada até o momento. Há uma variedade de preocupações em relação aos *sites* que os menores podem visitar, além da quantidade de informações a que eles estão expostos na rede. Aponta, ainda, que uma pesquisa feita em 2010, estima-se que até 7,5 milhões de usuários do Facebook têm menos de 13 (treze) anos de idade, e dois terços dessas pessoas têm menos de 10 (dez) anos de idade. Como a maioria dos outros grandes operadores *on-line*, o Facebook não permite que usuários menores de 13 (treze) anos se inscrevam no serviço. Na prática, porém, tais restrições são de difícil aplicação. Este é um dos fatores que lidera os formuladores de políticas públicas, além da pressão dos defensores da regulamentação pela expansão do COPPA e das regras de privacidade de crianças e adolescentes na rede.

O objetivo do regulamento é trazer proteção aos dados pessoais de crianças em *websites* e serviços *on-line*, exortando sempre o envolvimento dos pais ou representantes nessas atividades e possibilitando maior proteção aos seus filhos ou representados.

Nesse sentido, ensina Adam Thierer⁶¹, afirma que um dos objetivos da COPPA era aumentar o envolvimento dos pais nas atividades online de seus filhos e proteger melhor as informações pessoais das crianças online.

O COPPA é aplicado aos operadores de dados de *websites* e serviços *on-line* **dirigidos para crianças** e, também, àqueles que são voltados ao público em geral, **mas que coletam informações sobre o público infantil**⁶².

Afinal, como é possível determinar se o *site* ou serviço é direcionado às crianças? A Federal Trade Commission (FTC) considera uma série de fatores para isso, incluindo o assunto; o conteúdo visual ou de áudio; a idade dos modelos; a linguagem ou outras

⁶¹ “Concerns about children’s privacy are an important part of this debate. The Children’s Online Privacy Protection Act of 1998 (COPPA) already mandates certain online-privacy protections for children under the age of 13. The goal of COPPA was to enhance parent’s involvement in their children’s online activities and better safeguard kids’ personal information online”. THIERER, Adam. **Kids. Privacy, Free Speech and the Internet: Finding the Right Balance**. Disponível em: <http://ssrn.com/abstract=1909261>. [Acesso em: 20 set. 2021](#).

⁶² Foi com fundamento no COPPA que o FTC em 2019 impôs multa ao Google no valor de US\$ 170 milhões por violações à privacidade de crianças no YouTube (a multa mais alta aplicada pelo órgão até hoje). Conforme o acordo firmado, a Google LLC e a subsidiária YouTube LLC teriam violado as regras do COPPA ao coletar informações pessoais de crianças utilizando *cookies* para rastrear usuários na internet sem antes identificar e obter o consentimento expresso dos pais ou responsável. Com tais dados, o YouTube, usando os identificadores, praticou a denominada publicidade comportamental direcionada a crianças e adolescentes, sem expresso consentimento dos pais (Disponível em: <https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations>. Acesso em: 20 set. 2021).

características; se a publicidade promovendo ou aparecendo no *site* é direcionada a crianças; as evidências empíricas sobre a composição do público; a audiência pretendida; e se um *site* usa personagens animados e/ou atividades voltadas para crianças e incentivos⁶³.

Ademais, é preciso enfatizar que o regulamento não é aplicado às agências governamentais ou entidades sem fins lucrativos, já que os operadores, de acordo com tal regulamentação, são considerados pessoas, sociedades ou corporações que organizam seus negócios com a finalidade de lucro⁶⁴.

Por dados pessoais de crianças devemos compreender qualquer informação pessoal coletada pelo operador, incluindo, no rol do COPPA: nome, sobrenome, endereço domiciliar ou qualquer outro endereço físico, geolocalização, informações sobre contato *on-line*, como nome de usuário, e-mail e outros, número de telefone, número de segurança social (*social security number*), número identificador de usuário de serviços *on-line* ou *websites* ou de protocolos *on-line*, fotografias, vídeos ou áudios.

O dispositivo definiu como coleta dessas informações a reunião de qualquer dado pessoal da criança, com qualquer propósito, incluindo: i) requerer ou encorajar a criança a submeter informações pessoais na internet; ii) habilitar o fornecimento da criança de seus dados pessoais, tornando-os disponíveis, de forma que possa ser identificada; e iii) monitorar as atividades das crianças *on-line*.

⁶³ BAVITZ, Christopher; GUPTA, Ritu; OBERMAN, Irina; RITVO, Dalia. Privacy and Children's Data – An Overview of the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act. **Berkman Center Research Publication No. 23**, [S.l.], nov. 2013. Disponível em: <https://ssrn.com/abstract=2354339>. Acesso em: 20 set. 2021.

⁶⁴ Em tradução livre, assim explicam Oberman, Bavitz, Gupta e Topelson: Organizações sem fins lucrativos ou agências ou instituições governamentais precisam cumprir o COPPA? Um operador, conforme definido pela COPPA, não inclui qualquer entidade sem fins lucrativos que estará isento da cobertura da Lei da Comissão de Comércio Federal. A Seção 5 da Lei da Comissão de Comércio Federal (FTC) afirma que a jurisdição de execução da FTC aplica-se apenas a “pessoas, parcerias ou corporações”. Uma “corporação” é definida como uma entidade que “está organizada para executar negócio para obtenção de lucro ou de seus membros”. Portanto, entidades sem fins lucrativos ou entidades que não são “corporações” e geralmente não são sujeitas à jurisdição da FTC e, portanto, não são obrigadas a cumprir o COPPA. De acordo com a FTC, no entanto, entidades sem fins lucrativos que operam *sites* ou serviços para o lucro de seus membros comerciais podem estar sujeitas a responsabilidade sob o COPPA. As escolas geralmente não se qualificam como instituições comerciais que estão sujeitas à jurisdição da FTC. Dito isso, se uma escola se envolver em atividades comerciais (por exemplo, venda de camisetas *on-line*), então esse comportamento pode estar sujeito a supervisão pela FTC. Da mesma forma, mesmo que uma escola não esteja sujeita à supervisão da FTC, os prestadores de serviços contratados pelas escolas estarão sujeitos a ela. Para esse fim, sempre que uma escola contrata um serviço, deve garantir que o provedor de serviços está em conformidade com o COPPA (BAVITZ, Christopher; GUPTA, Ritu; OBERMAN, Irina; RITVO, Dalia. Privacy and Children's Data – An Overview of the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act. **Berkman Center Research Publication No. 23**, [S.l.], nov. 2013. Disponível em: SSRN: <https://ssrn.com/abstract=2354339>. Acesso em: 20 set. 2021).

Da mesma forma, divulgação de dados pessoais se relaciona: i) ao lançamento de informações pessoais identificáveis⁶⁵, coletadas por operador⁶⁶, oferecidas por criança com menos de 13 (treze) anos de idade, com qualquer finalidade, exceto nas hipóteses em que o operador provê tais informações com o intuito de suporte ao próprio *website* ou serviço *on-line*⁶⁷; ii) à acessibilidade de informações pessoais identificáveis, através de postagens em páginas da internet, sejam elas do próprio operador dos dados ou de outros *websites* e serviços *on-line* como *pen pall*, compras *on-line*, *message boards* e salas de bate-papo.

De acordo com o dispositivo, diversas condições são impostas aos operadores dos dados pessoais infantis, sendo as principais:

- obter consentimento dos pais para a coleta dos dados pessoais da criança⁶⁸;
- elaborar uma política de privacidade clara e compreensiva; além de
- manter as informações obtidas de crianças em segurança e confidencialidade.

4.1. O consentimento dos pais ou responsáveis no COPPA

O COPPA ressalta diversas vezes, ao longo de sua redação, a necessidade de que os pais ou responsáveis tenham conhecimento de todas as condições de oferecimento dos dados pessoais da criança de forma clara e precisa, e de que possam revisá-las constantemente, sempre que entenderem necessário ou que atualizações forem feitas.

De acordo com seus dispositivos, o operador deve, em qualquer caso, assegurar aos representantes legais das crianças que todas as informações obtidas serão protegidas, garantindo confidencialidade, segurança e integridade de todos os dados por ele obtidos.

Ainda nesse sentido, as informações oferecidas com o consentimento dos pais e responsáveis não podem ser utilizadas como condição para participação de jogos com oferecimento de prêmios ou qualquer atividade que exija mais elementos pessoais do que aqueles necessários para participar dessas atividades.

⁶⁵ Definido pela lei como compartilhamento, venda, aluguel ou transferência de informações pessoais a terceiros.

⁶⁶ Definido pela lei, de forma geral, como a pessoa física ou jurídica que gerencia *website* ou serviço *on-line*, coletando informações pessoais de seus usuários ou visitantes para diversos fins comerciais.

⁶⁷ A lei define suporte ao *website* ou serviço *on-line* como aqueles que servem para manter ou analisar funcionalidade, performance, conformidade e segurança do serviço, autenticidade dos usuários.

⁶⁸ Nesse sentido, o consentimento dos pais ou responsáveis deve ser assegurado pelo fornecimento pelo operador sobre a coleta e eventual uso ou divulgação de informações pessoais de seus filhos, devendo obter dos representantes autorização **verificável** para qualquer das ações descritas.

As informações podem ser requeridas de diversas formas e em diversos casos. Pode ocorrer de o próprio operador desejar informar aos pais ou responsáveis sobre o uso de sua plataforma pelos seus representados, bem como a possibilidade de requerer dados pessoais dessas crianças.

Para tanto, é possível que requeiram às crianças as informações sobre o contato dos pais ou responsáveis. Diante desse caso, deverá o operador notificar: i) que coletou as informações de contato dos pais ou representantes por intermédio da criança, e que entrou em contato para informar que seus filhos ou representados fazem uso do *website* ou serviço *on-line* do operador; ii) caso venham a necessitar de dados pessoais de seus filhos, que necessitam de sua aprovação para tanto; iii) que os dados de contato dos pais ou representantes coletados pelo operador não poderão ser usados para outro fim descrito; iv) que os pais ou representantes podem recusar a permissão do uso do *website* ou serviço *on-line* ou a coleta e o uso de dados pessoais da criança, bem como que seus contatos podem ser excluídos, caso manifestem vontade. Na última hipótese, deverá o operador informar a maneira como se fará a exclusão; v) que enviou um *hyperlink* com aviso sobre as práticas utilizadas na coleta dos dados pessoais da criança, inclusive sobre a parte do *website* ou serviço *on-line* requerida.

No mesmo sentido, caso o operador já tenha obtido as informações de contato dos pais ou representantes por intermédio da criança⁶⁹ e pretenda adquirir mais dados pessoais para o uso do *website* ou serviços *on-line*, deverá também requerer o consentimento deles. Se os pais ou responsáveis não responderem em tempo razoável, deverá o operador deletar as informações de contato de seus registros.

Por fim, enfatiza-se que o consentimento dos pais e responsáveis deve ser verificável, além de retratável, o que torna necessário ao operador possibilitar que ele se dê de forma descomplicada e rápida. Ademais, tal consentimento deve ser parcial, permitindo que os pais ou responsáveis consentam com a coleta e o uso dos dados pessoais da criança e proibindo que sejam divulgados a terceiros⁷⁰.

⁶⁹ Em ambos os casos, o mero requerimento do contato *on-line* dos pais ou responsáveis para assegurar a segurança da criança diante do uso do serviço *on-line* ou *website* do operador, ou ainda para solicitar novos dados pessoais de seus filhos/representados, não exige o consentimento de seus responsáveis. Ainda nesse sentido, também é dispensado seu consentimento caso o uso do contato tenha intenção de prover informação de cunho judicial, de previsão legislativa, para prover informações a agências públicas ou para fins de investigação no âmbito judicial.

⁷⁰ Importante notar que, embora a regulação geralmente não se aplique a informações pessoais coletadas de pais sobre seus filhos, como prática recomendada os operadores devem salvaguardar informações obtidas dos pais da mesma forma que fariam se fossem coletadas diretamente de uma criança. No mínimo, espera-se que eles mantenham a confidencialidade das informações coletadas dos pais quando fornecem consentimento para a liberação de informações de seus filhos ou quando revisam as informações coletadas

4.2. Métodos verificáveis de obtenção do consentimento

O COPPA trouxe disposição expressa em relação aos métodos utilizáveis para a verificação dos esforços na obtenção do consentimento dos pais. São eles:

- os esforços em utilizar todos os métodos necessários na busca da autorização, levando em conta o uso de todas as tecnologias disponíveis na atualidade. Nesse sentido, é preciso que seja possível verificar a autoria dos pais na autorização, sempre que possível;
- existindo métodos verificáveis, deverá o operador: oferecer formulário a ser assinado pelos pais e devolvido por e-mail ou escaneado; pedir que os pais tenham controle de notificação dos pagamentos *on-line* feitos via internet, quando possível; buscar o contato dos pais por meio de videochamada ou telefonema gratuito, entre outros.

Nota-se que os parâmetros e as orientações utilizados pelo COPPA podem perfeitamente nortear a compreensão do dispositivo nacional em comento, especialmente quanto à forma de coleta do consentimento dos pais e dos adolescentes.

4.3. Os programas *Safe Harbor*

O COPPA inclui disposição que permite que grupos do setor da mídia publicitária e outros similares criem programas de autorregulação complementares ao guia da comissão. Nesse sentido, exige que a classe apresente proposta a ser analisada de acordo com os requisitos exigidos no próprio código.

Nesse cenário, é válido destacar que o Children's Advertising Review Unit (CARU), conforme analisamos, é uma forma de autorregulação responsável por proteger as crianças da publicidade enganosa e abusiva, além de garantir o uso seguro dos menores de 13 (treze) anos na internet, tendo incluído o programa *Safe Harbor* como uma extensão do COPPA, a fim de garantir que as empresas cumpram suas diretrizes e protejam os interesses das crianças.

de seu filho (BAVITZ, Christopher; GUPTA, Ritu; OBERMAN, Irina; RITVO, Dalia. Privacy and Children's Data – An Overview of the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act. **Berkman Center Research Publication No. 23**, [S.l.], nov. 2013. Disponível em: <https://ssrn.com/abstract=2354339>. Acesso em: 20 set. 2021).

Assim, estando em conformidade com tal programa, os participantes que aderem a eles estão de acordo com o COPPA e sobretudo protegidos de ações coercitivas da Comissão Federal do Comércio dos Estados Unidos (Federal Trade Commission).

Para que um programa *Safe Harbor* tenha validade, a proposta poderá ser apresentada ao COPPA, que publicará o documento no Registro Federal, para que a opinião pública tenha chance de se manifestar. Após a submissão da proposta, a comissão tem 180 (cento e oitenta) dias para apresentar análise do projeto.

Deve a comissão avaliar:

- se o programa sugerido dispõe de regras iguais ou ainda mais abrangentes em relação à proteção das crianças que as garantidas pelo COPPA;
- a adoção de mecanismo obrigatório e efetivo para avaliação independente do cumprimento das diretrizes do programa de autorregulação. O mecanismo deve conter revisão abrangente e anual sobre as políticas e práticas, além das representações dos operadores participantes;
- se foram implementadas ações disciplinares por não conformidade das regras pelos operadores sujeitos às diretrizes do programa de autorregulação. Nessa perspectiva, tais ações poderão ser relatadas em relatórios públicos⁷¹ das medidas tomadas contra os operadores infringentes, com reparação ao consumidor, pagamento voluntário ao tesouro americano ou encaminhamento de relatório ao COPPA sobre os operadores que adotam padrão ou prática de violação de diretrizes da autorregulação.

4.3.1. Requisitos exigidos para o pedido de aprovação do programa

Para que seja apresentado programa de *Safe Harbor* compatível e passível de autorização pelo COPPA, é necessário o preenchimento dos seguintes requisitos:

- demonstração detalhada do modelo de negócios do setor responsável pelo programa, além das tecnologias e dos mecanismos disponíveis para a avaliação dos operadores sujeitos, tanto na implantação quanto durante a vigência do programa de *Safe Harbor*;
- cópia do texto completo do código submetido à aprovação;

⁷¹ As ações retratadas no COPPA não são taxativas. Dessa forma, caberá a análise do caso concreto, sendo possível a adoção de outras ações disciplinares mais efetivas que as descritas no código.

- comparação das regras que apresentam correspondência com as disposições do COPPA, além da demonstração de que os dispositivos refletem as regras da Comissão.

Nesse sentido, importante ressaltar que, ainda que um programa seja aprovado pela Comissão, ele deverá se submeter a nova aprovação sempre que novas regras e mudanças forem propostas.

4.3.2. Deveres dos programas de *Safe Harbor* aprovados

Os programas aprovados deverão, anualmente, submeter à Comissão um reporte, contendo os resultados das avaliações realizadas e sanções aplicadas aos operadores. Além disso, devem atender a todas as demandas da Comissão em relação às informações adicionais possivelmente requeridas e manter registros das reclamações recebidas de consumidores, das sanções aplicadas e propostas de mudanças já submetidas à Comissão, durante a vigência dos programas.

4.3.3. Revogação da concessão do programa autorregulatório

O COPPA pode, a qualquer tempo, revogar as aprovações concedidas aos programas sempre que concluir que implantam condutas e códigos em desacordo com a Comissão. Programas de *Safe Harbor* que foram aprovados antes da publicação da emenda de março de 2013 devem submeter suas regras à Comissão novamente, a fim de provar sua conformidade com as regras atuais do documento.