10626247 08012.000723/2018-19

**MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA**

**Nota Técnica n.º 32/2019/CGCTSA/DPDC/SENACON/MJ**

**PROCESSO Nº 08012.000723/2018-19**

**Representante: Departamento de Proteção e Defesa do Consumidor - ex officio.**

**Representados: Facebook Inc. e Facebook Serviços Online do Brasil Ltda.**

**Assunto: Prática abusiva. Violação aos princípios da boa-fé, ao direito à privacidade e à informação clara e adequada sobre bens e serviços.**

**Ementa: Processo Administrativo. Infração aos direitos básicos do consumidor no que diz respeito ao reconhecimento de sua vulnerabilidade, ausência de boa-fé, ao equilíbrio entre consumidores e fornecedores, ao direito à privacidade e à intimidade. Cometimento de prática abusiva em desfavor da coletividade consumerista. Falha no dever de fornecimento de informações claras e adequadas quanto a sua política de privacidade pelas Representadas Falha na custódia adequada dos dados fornecidos pelos usuários considerando o modelo de negócios adotado. Descumprimento dos artigos 4º, caput, I, III e IV; 6º, II, III, IV e VI, art. 18, art. 31; art. 37 e art. 39, todos do Código de Defesa do Consumidor, além das disposições do Marco Civil da Internet, notadamente, os arts. 2º, inc. II e III, e 7º, incs. VI, VII, VIII, IX, e XIII. Sugestão de aplicação de sanção de multa no valor de R$ 6.600.000,00 (seis milhões e seiscentos mil reais).**

## I. RELATÓRIO

Trata-se de Processo Administrativo instaurado no âmbito do Departamento de Proteção e Defesa do Consumidor (DPDC), da Secretaria Nacional do Consumidor (SENACON), do Ministério da Justiça e Segurança Pública (MJSP) para apuração de irregularidades cometidas pelas empresas Facebook Inc. e Facebook Serviços Online do Brasil Ltda. ("Representadas"), no tocante ao compartilhamento indevido de dados de usuários.

O presente caso começou a ser investigado após o conhecimento de notícia veiculada pela mídia, em 04 de abril de 2018, na qual havia informação de que usuários do Facebook, no país, *"podem ter sofrido com o uso indevido de dados pela Cambridge Analytica. Ao todo, segundo a rede social, 87 milhões em todo o mundo podem ter tido suas informações compartilhadas pela consultoria de marketing político, sendo 70 milhões nos Estados Unidos. No Brasil, segundo nota publicada pelo Facebook em sua página na internet, este número foi de 443 mil"* (SEI 6156620).

Com a finalidade de averiguar os fatos, o Departamento de Proteção e Defesa do

Consumidor (DPDC), em 17 de abril de 2018, expediu a Notificação 19/2018/CSA – SENACON/CGCTPA/GAB-DPDC/SENACON, para que Facebook Serviços Online do Brasil Ltda. (Facebook Brasil) se manifestasse sobre eventual compartilhamento indevido de dados dos seus usuários e suas repercussões sobre os usuários brasileiros (SEI 6155038). Por meio de tal notificação, FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA. foi instada a responder aos seguintes questionamentos: "*Qual é o alcance do suposto compartilhamento irregular? Ou seja, qual é o número de usuários brasileiros afetados por ele? Qual era a finalidade da captura dos dados dos consumidores? Detalhe e esclareça; Segundo as notícias, os usuários teriam concordado em fazer um "teste" online e teriam consentido em compartilhar seus dados "para fins acadêmicos". Essa informação procede? Se não, como os dados dos usuários brasileiros foram compartilhados com a Cambridge Analytica? Informe; Informe se, além da Cambridge Analytica, os dados compartilhados foram também disponibilizados a outras empresas sem que o usuário brasileiro tenha dado consentimento específico para tal; O Facebook tem parceria, contrato ou qualquer vínculo com empresa que promova o marketing político partidário no Brasil? Em caso afirmativo, explique; Depois da assunção do compartilhamento irregular, por parte da empresa, o que o Facebook fez ou está fazendo para contornar o problema? Especifique as ações tomadas de forma minuciosa; Como o Facebook age para proteger os dados de seus usuários e de que instrumentos dispõe para que essa proteção seja efetiva?*"

Em resposta, Facebook Serviços Online do Brasil Ltda comunicou que, em respeito à atuação da Senacon teria interesse em apresentar as informações, tendo acrescentado que seria necessário, para tanto, a obtenção de esclarecimentos junto às empresas Facebook Inc., constituída e sediada nos Estados Unidos da América e Facebook Ireland Limited, constituída e sediada na Irlanda, que seriam as proprietárias e operadoras do site Facebook. Desta forma, solicitou dilação de prazo por 20 dias adicionais.

Facebook Brasil apresentou as seguintes alegações preliminares: 01) que é uma empresa brasileira, constituída e existente em conformidade com as leis do Brasil e que tem por objeto social a prestação de serviços relacionados à locação de espaços publicitários, veiculação de publicidade, suporte de venda etc.; 02) que o site http://facebook.com ("Site Facebook") é administrado e operado pelas entidades Facebook Inc. (norte-americana) e Facebook Ireland Limited, sendo a última a entidade responsável pela prestação dos serviços Facebook em todos os países, inclusive o Brasil; 03) que teria contatado Facebook Ireland e obtido as informações investigadas nos presentes autos; 04) que, segundo noticiado pela Facebook Ireland, a Cambridge Analytica, teria usado indevidamente dados de usuários do Facebook, os quais lhe foram repassados por um desenvolvedor de aplicativos, Dr. Aleksandr Kogan, em violação à Política de Uso da Plataforma Facebook, por meio de um aplicativo chamado *thisisyourdigitallife*; 05) que o aplicativo do Dr. Kogan fez uso do *Facebook Login*, um recurso da plataforma que permite que terceiros desenvolvedores de aplicativos solicitem o consentimento de usuários do Facebook para que seus aplicativos acessem categorias específicas suas; 06) que, na época, o *Facebook Login* admitia que os desenvolvedores solicitassem consentimento dos usuários para acessar categorias específicas de dados compartilhados com esses usuários por seus amigos no Facebook; 07) que entretanto, o *Facebook Login* sempre proibiu que desenvolvedores vendessem, licenciassem ou compartilhassem dados de usuários acessados do Facebook com qualquer rede de publicidade, corretora de dados ou outro serviço relacionado à publicidade ou monetização; 08) que, no caso dos autos, o Dr. Kogan transferira, em desobediência às políticas de uso da plataforma, alguns dados de usuários do Facebook que ele obteve por intermédio do aplicativo para a empresa responsável Cambridge Analytica (controlada por SCL Elections Limited), sem que houvesse autorização do Facebook e em violação à Política da Plataforma; 09) que os dados solicitados pelo Aplicativo e que foram consentidos pelos usuários eram: a) dados do perfil público, incluindo nome e gênero; b) data de nascimento; c) "cidade atual" indicada na seção sobre perfil do usuário, se informada; d) páginas que o usuário curtiu; e) lista de amigos e, quanto a estes, as mesmas informações acima (dependendo e conforme as configurações de privacidade de cada amigo), ressalvando, ainda, que os dados repassados

não envolviam senhas ou transações financeiras; 10) que o caso não se constitui em incidente de invasão de sistemas ou quebra de sigilo de dados (*data breach*); 11) que, ao ter ciência dos fatos, a Representada adotou providências como: a) encerramento dos direitos de acesso do Aplicativo do Dr. Aleksandr à Plataforma Facebook em 17 de dezembro de 2015, (tendo tomado conhecimento do caso em 12 de dezembro de 2015); b) instituição de obrigação de que fossem apagados todos os dados obtidos pelo Aplicativo; c) banimento do acesso à plataforma à empresa Cambridge Analytica e ao do Dr. Kogan; 12) que foram ainda introduzidas mudanças na Plataforma Facebook, a partir de 30 de abril de 2014, com o objetivo de restringir os dados que aplicativos como o Dr. Aleksandr eram capazes de acessar; 13) que, quanto a extensão do número de usuários atingidos no Brasil, o Facebook entendeu que 84 (oitenta e quatro) pessoas no Brasil instalaram o Aplicativo, o que representava 0,03% do total de instalações do Aplicativo no mundo e que, no máximo 443.033 (quatrocentos e quarenta e três mil e trinta e três) pessoas adicionais no Brasil foram potencialmente afetadas. O número total máximo de 443.117 (quatrocentos e quarenta e três mil, cento e dezessete) pessoas foram potencialmente afetadas no Brasil, o que representa 0,51% do número global de pessoas potencialmente afetadas; 14) que teria assumido os seguintes compromissos adicionais para tratar da privacidade de dados em sua plataforma: a) revisão e auditoria da plataforma para fins de verificação de acessos a grandes quantidades de dados de usuários e identificação de mau uso de informação pessoal identificável; b) comunicação dos usuários sobre o mau uso de dados fornecidos à plataforma; c) interrupção do acesso a um aplicativo que esteja sem uso por mais de três meses; d) maior escrutínio na disponibilização de dados por meio da plataforma Facebook Login; e) maior estímulo à participação do usuário no controle dos dados disponibilizados à plataforma; f) instituição de um programa de recompensas para quem identificar vulnerabilidades.

Na sequência, foi expedido, no dia 24 de outubro de 2018, o Ofício n° 154/2018/CSA-SENACON/CGCTSA/DPDC/SENACON-MJ ao Ministério Público do Distrito Federal e Territórios solicitando informações atualizadas acerca do andamento do Inquérito Civil Público, instaurado a partir da Portaria n. 02/2018, que busca investigar as circunstâncias e as causas do provável uso ilegal dos dados pessoais de brasileiros pela empresa Cambridge Analytica. Nada obstante, não houve resposta a este Departamento.

Em decorrência dos fatos e da potencial exposição de consumidores brasileiros, decorrente da prestação do serviço com vício, foi instaurado o presente processo administrativo sancionador, com fulcro no aparente desrespeito aos princípios básicos que regem a legislação consumerista nacional, havendo indícios de prática abusiva em decorrência de possível violação aos artigos 4º, *caput*, incisos I, III e IV; 6º, incisos II, III, IV e VI; 18; 31; 37; e 43, da Lei 8.078/90, assim como o direito à privacidade e à intimidade, previstos na Constituição Federal (Nota Técnica n. 108/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ – SEI 8211818).

Em decorrência dos fatos e da potencial exposição de consumidores brasileiros, decorrente da prestação do serviço com vício, foi instaurado o presente processo administrativo sancionador, com fulcro no aparente desrespeito aos princípios básicos que regem a legislação consumerista nacional, havendo indícios de prática abusiva em decorrência de possível violação aos artigos 4º, *caput*, incisos I, III e IV; 6º, incisos II, III, IV e VI; 18; 31; 37; e 43, da Lei 8.078/90, assim como o direito à privacidade e à intimidade, previstos na Constituição Federal (Nota Técnica n. 108/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ – SEI 8211818).

Facebook Inc. e Facebook Serviços Online do Brasil Ltda. foram devidamente intimados (Intimação nº 18/2019/CSA-SENACON/CGCTSA/DPDC/SENACON) da instauração do Processo Administrativo e notificados a apresentarem defesa administrativa (SEI 8234665).

Na sua primeira manifestação após a instauração do presente processo administrativo, Facebook Brasil – a qual informara inicialmente que realizava a intermediação com o Facebook Inc. e que contribuía com a elucidação dos fatos - passou a informar que não tinha poderes legais ou

contratuais para representar ou para receber notificações, citações ou intimações dirigidas à empresa Facebook Inc., com a qual não se confundia. Requereu que fosse determinada a intimação do Facebook Inc., por meio de carta a ser entregue no endereço da sede daquela empresa, qual seja, nos Estados Unidos da América (SEI 8293925– apenso 08012.000722/2019-55).

Em sede de Defesa Administrativa, Facebook Brasil reiterou muitos dos argumentos expostos na manifestação anterior, bem como requereu a nulidade do processo quanto a si. No mais, alegou 01) que não é proprietário ou provedor do site Facebook, tampouco controlador ou depositário dos dados dos respectivos usuários e 02) que não ofereceu os serviços do site Facebook aos consumidores brasileiros, não sendo, portanto, responsável pela segurança do site e não tendo qualquer ingerência na plataforma; 03) em caráter eventual, que foi lícita a conduta de Facebook Inc., pois não teria ocorrido invasão de sistemas ou quebra de sigilo de dados, mas sim, a coleta de dados de usuários (dados do perfil público, incluindo nome e gênero, data de nascimento, cidade atual, páginas que o usuário curtiu e lista de amigos) do Facebook por um aplicativo de terceiros, mediante consentimento dos próprios usuários; 04) que apenas foram coletados, pelo aplicativo do Dr. Kogan, dados de usuários do Facebook, que optaram por exibi-los a outras pessoas; 05) que, ao tomar conhecimento dos fatos, Facebook Inc. teria tomado as medidas cabíveis; 06) que os usuários/consumidores manifestaram consentimento, por meio da "Declaração de Direitos e Responsabilidades" e da "Política de Dados", com o compartilhamento de seus dados com os aplicativos de terceiros que optassem por utilizar, em conformidade com as suas configurações de privacidade; 07) que o compartilhamento de dados de usuários entre o Facebook e o Aplicativo não representou em qualquer forma de descumprimento dos seus instrumentos contratuais; 08) que aproximadamente 443.000 usuários do Facebook no Brasil potencialmente podem ter tido os seus dados coletados pelo aplicativo do Dr. Kogan, mas que, contudo, não há evidências de que os dados de usuários do Facebook localizados no Brasil coletados pelo aplicativo tenham sido transferidos à Cambridge Analytica; 09) que a fala do CEO Mark Zuckerberg reconhecendo a falha na prestação dos serviços não pode ser interpretada como qualquer ato que implique reconhecimento da responsabilidade civil da plataforma em decorrência dos fatos em análise; 10) que as regras para utilização da interface "Facebook Login" proíbem quaisquer vendas ou atos de licenciamento de dados de usuários (consumidores) da plataforma Facebook, assim como o compartilhamento de tais dados com quaisquer rede de anúncios, *data brokers*, ou qualquer outro serviço relacionado à publicidade ou à monetização; 11) que a inscrição de um dado usuário na plataforma Facebook implica em aceitação dos seus termos de serviço, então referidos como Declaração de Direitos e Responsabilidades e em concordância com a Política de Dados da Plataforma Facebook; 12) que houve o consentimento dos usuários para que o aplicativo *thisisyourdigitallife* acessasse algumas de suas informações pessoais, onde tais permissões permaneceram entre os anos de 2013 e 2015, durante o qual tal aplicativo se manteve ativo na plataforma Facebook; 13) que tal aplicativo "poderia acessar dados de amigos de um usuário apenas se autorizado por esse usuário e somente para amigos cujas configurações de 'Aplicativos que Outros Usam' permitam esse compartilhamento; 14) que as configurações da interface "Aplicativos que Outros Usam" foram aprimoradas para permitir maior controle, pelo usuário, sobre os dados que os seus amigos podem compartilhar com aplicativos de terceiros; 15) que o aplicativo em questão não teve acesso a nenhum dado cujo fornecimento não tenha sido objeto de consentimento pelo usuário (a exemplo do que poderia acontecer com senhas e informações financeiras); 16) que os terceiros que não utilizaram o aplicativo *thisisyourdigitallife* também teriam autorizado tal consentimento ao estabelecer, em suas configurações de privacidade, que seus amigos poderiam compartilhar tais dados com outras ferramentas disponibilizadas na plataforma Facebook; 17) que essa política de dados foi atualizada em 2015, com a finalidade de tornar mais transparentes os mecanismos de controle de privacidade disponibilizados ao usuário pela plataforma; 18) que a Política da Plataforma Facebook proíbe expressamente a venda de dados de usuários acessados a partir do Facebook (ponto esse já abordado acima), o que levou ao banimento do aplicativo do Dr. Kogan; 19) que não sabe exatamente a extensão dos dados compartilhados pelo Dr. Kogan com a Cambridge Analytica, mas que as informações

atualmente disponibilizadas indicam que apenas dados de usuários domiciliados nos EUA teriam sido compartilhados com a Cambridge Analytica; 20) que seria inaplicável o Código de Defesa do Consumidor para apurar eventuais infrações cometidas por empresas estrangeiras aos direitos de consumidores também estrangeiros; 21) que não há conduta que traduza publicidade enganosa ou abusiva praticada pela plataforma Facebook e 22) que a partir de 09 de abril de 2018, que o Facebook passou a exibir para os seus usuários uma notificação no topo de seu "Feed de Notícias", para que eles tivessem conhecimento de quais aplicativos estariam usando e quais informações estariam sendo compartilhadas com esses aplicativos. Ao fim reitera as alegações trazidas em sede preliminar e pugna pelo arquivamento do presente feito (Petição SEI 8366762 – apenso 08012.000810/2019-57).

No dia 29 de março de 2019, foi proferido o Despacho nº 319/2019/CSA-SENACON/CGCTSA/DPDC/SENACON, o qual determinou que Facebook Brasil contatasse Facebook Inc. para que indicasse o representante no território brasileiro. Também ficou assentado que, no caso de negativa de atendimento de tal determinação, seria designada a subsidiária brasileira como representante do Facebook Inc. (SEI 8389011).

No dia 30 de abril de 2019, por intermédio de Despacho Complementar (Despacho nº 434/2019/CGCTSA/DPDC/SENACON - SEI 8634694), foi proferido entendimento no sentido de se esclarecer que a conduta do Facebook Brasil de requerer notificação pessoal do Facebook Inc., empresa sediada no exterior "*andava na contramão da afirmação contemporânea do princípio da unidade econômica dos grupos societários, amplamente conhecida pela jurisprudência e pela doutrina pátria*". Entendeu-se, na oportunidade, que a legislação brasileira estabelece ser plenamente possível a prática de atos processuais destinados a empresa estrangeira por meio de empresa do mesmo grupo situada no Brasil, ainda que possuam personalidades jurídicas distintas. Assim, foi determinada a notificação de Facebook Inc. por meio dos administradores de Facebook Brasil para apresentação de defesa administrativa.

Em seguida, Facebook Brasil requereu reunião com os representantes do Departamento de Proteção e Defesa do Consumidor, a qual fora realizada em 07 de maio de 2019. Em tal ocasião, Facebook Brasil requereu que o DPDC enviasse carta para Facebook Inc. para apresentação de defesa "*pois seria a responsável por responder pela oferta dos serviços disponíveis pela plataforma, respondendo, inclusive, perante autoridades estrangeiras no que se refere às discussões envolvendo proteção de dados* ". Por sua vez, o DPDC comunicou que, de acordo com os despachos expedidos, as notificações para Facebook Inc., no domicílio de Facebook Brasil, deveriam ser consideradas válidas para os fins a que se destinam. Não obstante, e por questão de liberalidade do Órgão, seria expedida a notificação de instauração dos procedimentos para a matriz Facebook Inc.

No dia 15 de maio de 2019, Facebook Inc. apresentou defesa nos autos. Precipuamente (relato feito a partir de sua versão pública, posteriormente apresentada após determinação deste DPDC), informou que Facebook Brasil é uma sociedade independente de Facebook Inc., responsável por publicidade e vendas, e que não tem qualquer função ou ingerência no que tange às operações da Plataforma Facebook. No mérito sustentou 01) que não existem quaisquer indícios de que os dados de usuários do Facebook localizados no Brasil tenham sido transferidos para a Cambridge Analytica por um desenvolvedor de aplicativos em violação às política de uso da plataforma; 02) que todas as evidências disponíveis indicam que a transferência de dados de usuários para a Cambridge Analytica - ou sua controladora, a sociedade SCL Elections Limited (SCL) - envolveu somente dados de usuários localizados nos Estados Unidos da América; 03) que não houve quebra de sigilo de dados (*data breach*), pois os usuários teriam consentido com a obtenção de categorias específicas de seus dados a um aplicativo de terceiro, denominado *thisisyourdigitallife*; 04) que, quanto a responsabilidade sobre os dados colhidos pelo aplicativo, ela deveria recair sobre o desenvolvedor de tal aplicativo; 05) que, não se descuidando de suas obrigações legais, o Facebook vem adotando medidas de segurança responsável, o que teria feito no caso da Cambridge Analytica ; 06) que, no tocante ao recurso *Facebook Login*, tal interface acessa categorias de dados previamente especificadas, o que não incluem

informações sensíveis , e no caso dos amigos desses usuários, era possível ter acesso aos dados que esses amigos publicaram na Plataforma Facebook e que teriam consentido em disponibilizar tais dados ao usuário que instalou o aplicativo ; 07) que tomou ciência de que os dados foram compartilhados com a Cambridge Analytica pela matéria do jornal *The Guardian*, tendo acrescentado que agiu prontamente encerrando os direitos de acesso do desenvolvedor ao recurso *Facebook Login* ; 08) que, no Brasil, apenas 84 pessoas teriam instalado o aplicativo do Dr. Kogan, mas que outras 443.033 pessoas podem ter sido afetadas com o compartilhamento de dados com o aplicativo (na qualidade de amigos, ou amigos de amigos, de pessoas que aderiam ao aplicativo), o que representaria 0,51% do total de pessoas afetadas; 09) que não há evidências de que tenha ocorrido a efetiva transferência de tais dados do aplicativo do Dr. Kogan para a SCL, destacando que os dois contratos celebrados entre GSR (responsável juridicamente pelo aplicativo *thisisyourdigitallife* – isto é, o aplicativo do Dr. Kogan - e SCL não previam a transferência de dados de pessoas situadas fora dos Estados Unidos; 10) que o número de pessoas afetadas pode, na verdade, ter sido menor que o quantitativo acima pelos motivos descritos no item 2.3.3 da peça de defesa; 11) que, a partir de 09 de abril de 2018 , passou a oferecer link no topo do feed de notícias de sua plataforma - passando a permitir às pessoas verem quais aplicativos estavam usando e quais informações compartilhavam com esses aplicativos – destacando ainda que as atualizações da plataforma Graph API V2 de 30 de abril de 2014 já seria suficiente para impedir que aplicativos como o desenvolvido pelo Dr. Kogan pudessem acessar dados naquela mesma extensão ; 12) que se comprometeu a elevar o patamar quanto a forma como os desenvolvedores criam no Facebook e o que as pessoas podem esperar deles, tais como: a) auditoria de aplicativos que tiveram acesso a grande quantidade de dados dos usuários da plataforma; b) aviso aos usuários sobre o mau uso de dados; c) restrição de dados que podem ser disponibilizados pelo recurso Facebook Login sem autorização prévia do titular; d) incentivo aos usuários para um gerenciamento ativo dos aplicativos que utilizam; e) recompensa a pessoas que identificarem vulnerabilidades; f) políticas mais estritas para aplicativos que ofereçam utilidade mínima, sem melhorar significativamente a experiência do usuário; g) interrupção de acesso de aplicativos não utilizados por mais de 90 dias; 13) que os usuários tinham conhecimento dos termos de uso do Facebook, inclusive quanto à possibilidade de compartilhamento de dados seus disponibilizados a amigos quando esses últimos subscrevessem um dado aplicativo; 14) que, durante o período relevante (isto é durante o intervalo de tempo em que o aplicativo *thisisyourdigitallife* operou na plataforma ), a) houve transparência significativa no que diz respeito ao papel de aplicativos de terceiros (inclusive quanto à obtenção de dados dos usuários e de seus amigos e o que poderia ser feito para controlar o compartilhamento desses dados); b) os usuários tinham pleno controle dos dados que estavam sendo compartilhados por meio da política de privacidade; c) que o Facebook facilitou o compartilhamento desses dados de acordo com as autorizações informadas, livres e específicas através de controles de privacidade. Requer ao fim, o arquivamento do feito (SEI 8931371 – apenso 08012.001624/2019-35).

Em 15/07/2019, foi proferido o Despacho nº 629/2019/CGCTSA/DPDC/SENACON (SEI 9200792), cujo teor, no que importa, está assim redigido:

> *As representadas, por sua vez, alegam, em defesa, que nenhum dos dados de usuários do Facebook localizados no Brasil tenham sido transferidos para a Cambridge Analytica por um desenvolvedor de aplicativos em violação à política do Facebook, tendo as evidências de violação de dados sido restritas apenas aos usuários do Facebook localizados nos Estados Unidos da América.*
> *Isso colocado, constata-se que, seja com fundamento no art. 6º, inc. VIII, do CDC (aplicável ao caso), seja com fundamento nos arts. 15 c/c 373, § 1º, do CPC, o caso é de se atribuir às representadas (que desenvolvem e mantêm os códigos da plataforma) o ônus de demonstrar que houve realmente o adequado dever de cuidado no trato das informações de seus usuários que estão sob sua custódia. Esse entendimento se aplica seja no que se refere à exposição dos dados dos usuários à empresa acima*

> *mencionada, seja em relação à exposição no que se refere à exposição de tais dados por outros mecanismos desenvolvidos por meio da interface Facebook login.*
> *Ante o exposto, torno sem efeito o Despacho nº 915/2019/CSA-SENACON/CGCTSA/DPDC/SENACON, e restituo as partes o prazo de 10 (dez) dias para que indiquem, de forma circunstanciada e fundamentada, as provas que pretendem produzir nos autos.*

Em resposta, Facebook Brasil, no petitório 9297160 (apenso 08000.032920/2019-17), informou a ausência de interesse em produzir novas provas, reiterou a sua ilegitimidade passiva, bem como o pedido de arquivamento do presente caso. Para tanto, reiterou os seguintes pontos: 01) ausência de conduta ilícita de sua autoria; 02) licitude da conduta de Facebook Inc., frisando que não houve vazamento de dados, que os dados coletados se deram com consentimento e em conformidade com as configurações de privacidade de cada usuário, que os dados foram transferidos do aplicativo *thisisyourdigitallife* para terceiros em desacordo com as normas da plataforma e sem o conhecimento de Facebook Inc., que buscou adotar as medidas para imediatamente sanar o ocorrido, que não evidências de que dados de usuários localizados no Brasil tenham sido transferidos à Cambridge Analytica, que o CDC é inaplicável para fatos cujos ofendidos não estejam no país, que não há danos sofridos pelos usuários brasileiros e que não há violação nem ao art. 6º, inc. IV, e nem ao 37 do CDC.

No protocolado 9297919 (apenso 08012.002112/2019-96), Facebook Inc. alega que não há indícios de usuários brasileiros afetados no caso, acrescentando que somente dados de usuários localizados nos Estados Unidos teriam sido transferidos a SCL Elections Limited (Cambridge Analytica) por meio de um contrato com a Global Science Research (GSR), sociedade registrada em nome do Dr. Kogan e de um colega. Pondera que não foram disponibilizados dados de pessoas que não fossem cidadãos dos Estados Unidos. Assim, diz que não houve exposição de dados de brasileiros e que, reiterando exposição anterior, o quantitativo de 443.117 usuários seria apenas uma estipulação do total de pessoas potencialmente afetadas no Brasil, mas que, no entanto, a quantidade efetiva de afetados no Brasil pode ser menor . Registra que o consentimento dos usuários na plataforma Facebook Login se deu de forma regular, sendo, inclusive, utilizada por órgãos governamentais brasileiros, como o Detran/SP. Acrescenta que o aplicativo *thisisyourdigitallife* usou a plataforma Facebook Login entre novembro de 2013 e dezembro de 2015 (considerado aqui o "período relevante"), quando estava em uso o GRAPH API V1 . Aduz que os termos de uso da plataforma Facebook, na época dos fatos, autorizaria o compartilhamento de informações públicas e de listas de amigos no contexto fático em apreciação, incluída a possibilidade de o aplicativo acessar as informações não apenas de seus usuários que o subscreveram, mas também, as informações disponibilizadas pelos amigos desses usuários que subscreveram o aplicativo. Destaca que, a partir de 2015, foram implementadas políticas para fortalecer o controle, pelo usuário, das informações fornecidas à plataforma, as quais proíbem qualquer tipo de negociação de dados dos usuários por meio de *databrokers*. Infere que sua condição é de servir como mera intermediária entre os usuários e os desenvolvedores no cenário em análise, aos quais cabe comportarem-se de acordo com as leis e com as políticas do Facebook, incluída, aqui a proibição de transferência dos dados que tivessem recebido a qualquer rede de anúncios, corretor de dados etc., motivo pelo qual o aplicativo do Dr. Kogan fora banido em 17/12/2015 . Acrescenta que todas as informações repassadas à SCL Elections (Cambridge Analytica) pelo aplicativo da GSR/Dr. Kogan teriam sido deletadas na primavera de 2017 .

Junta documentos.

No apenso 08012.002112/2019-96 (SEI 9297919), Facebook Inc. apresenta nova manifestação no sentido de que: 01) não há evidência de dados de brasileiros afetados no caso Cambridge Analytica, uma vez que não há comprovação de que dados de brasileiros teriam sido fornecidos a SCL Elections Limited, a qual controla aquela, frisando, ainda, que o compartilhamento de dados da aplicação *thisisyourdigitallife* com a SCL estaria limitada a dados de usuários norte-

americanos; 02) que os dados de usuários brasileiros foram compartilhados de maneira livre e consentida pelos seus titulares conforme termos de uso da plataforma ; 03) que sua política de uso foi atualizada em meados de 2015 para tornar explícito o aviso de que o usuário tem o poder de determinar quem pode ter acesso a seus dados, tendo acrescentado, ainda, que a plataforma proíbe a venda ou o licenciamento desses dados e que o consentimento para tal compartilhamento era obtido seja pelo compartilhamento de dados, pelo usuário, seja com o aplicativo, seja diretamente pelo compartilhamento de tais dados com os seus amigos; 04) que foram adotadas as medidas cabíveis contra o titular do aplicativo, corrigindo a política de dados empregada em 2013 , com pronto banimento do aplicativo da plataforma.

Junta documentos.

Despacho 848 (SEI 10147266) juntando documentos produzidos em procedimento envolvendo a plataforma Facebook no âmbito da Federal Trade Comission norte-americana.

Por meio da Petição SEI 10219398, Facebook Brasil novamente se manifesta pela nulidade do presente procedimento, uma vez que os fatos estariam apenas relacionados a Facebook Inc.

Por meio da Petição SEI 10340250, Facebook Inc. aduz as seguintes alegações: 01) o termo de acordo firmado recentemente ainda aguarda aprovação; 02) Facebook Inc. não admite nem nega nenhuma das alegações trazidas em face de si pela FTC; 03) que os termos do acordo celebrado não estabelecem que o Facebook estaria responsável pelo episódio da Cambridge Analytica; 04) que as reclamações trazidas pela FTC estão relacionadas a fatos ocorridos nos EUA, e não no Brasil ; 05) que apenas duas das seis alegações estariam relacionadas com o episódio da Cambridge Analytica; 06) que a alegação nº 01 sustenta que, entre 2012 e 2014, Facebook teria deturpado a extensão do controle dos usuários perante terceiros; 07) que alegação nº 04 sustenta que Facebook não teria conseguido manter um programa de privacidade suficientemente robusto e não aplicou consistentemente suas políticas de plataforma desde 2012 até o momento ; 07) que, nada obstante, seus usuários teriam consentido com todas essas práticas de compartilhamento de seus dados com terceiros; 08) que as demais alegações não teriam relação com o presente caso; 09) que as alegações 02 e 03 estariam relacionadas a declaração de Mark Zuckerberg à conferência anual de desenvolvedores em meados de 2014, sobre o acesso a categorias específicas de dados que os desenvolvedores teriam no futuro ; 10) que "*a Alegação nº 5 sustenta que entre abril de 2018 e a presente data, o Facebook teria deturpado a extensão que os usuários poderiam controlar a privacidade de seus dados, com relação a uma configuração particular. Contudo, a referida data é muito posterior ao episódio Cambridge Analytica* "; 11) que "*a Alegação nº 6 sustenta que o Facebook não teria revelado aos usuários que estaria usando seus números de telefone, fornecidos para autenticação de dois fatores no momento do login, para fins publicitários*"; 12) que, no âmbito da plataforma Graph API V1 para desenvolvimento de aplicativos, reiterou que o consentimento dos usuários foi obtido de forma válida, inclusive quanto ao *default* de compartilhamento de dados compartilhados com amigos em relação aos aplicativos que esses últimos subscreviam; 13) que as mudanças para os parâmetros da plataforma Graph API V2, com maiores restrições de compartilhamento que a versão anterior, deu-se de forma totalmente espontânea por Facebook Inc., sem qualquer relação com acusações anteriores de violação a privacidade dos usuários; 14) que, "*desde março de 2018, o Facebook também adotou medidas adicionais importantes, visando agir com relação a qualquer potencial abuso pretérito e prevenir qualquer abuso futuro*", tais como análise da plataforma (para fins de avaliação de como os dados dos usuários vem sendo utilizados), aviso (a eventuais usuários afetados) sobre o mau uso de seus dados, diminuição dos dados que são ordinariamente disponibilizados por meio da plataforma Facebook Login, programa de recompensas para pessoas que identificarem vulnerabilidades, políticas de informação de usuários para melhor gerenciamento dos aplicativos que utilizam, programa de recompensas para pessoas que identificam vulnerabilidades, política inibindo a criação de aplicativos com utilidade mínima na plataforma e interrupção de acessos com aplicativos não utilizados.

Era o que cabia relatar. Passa-se a opinar.

## II. FUNDAMENTAÇÃO

### DA COMPETÊNCIA DO DEPARTAMENTO DE PROTEÇÃO E DEFESA DO CONSUMIDOR PARA PROCESSAR E DECIDIR O CASO

O presente caso trata da apuração de prática que, segundo os fatos discutidos nos autos, teria atingido a esfera jurídica de mais de quatrocentos e quarenta mil pessoas no Brasil.

Importante anotar que os órgãos integrantes do Sistema Nacional de Defesa do Consumidor (SNDC) têm competência concorrente no exercício do poder de polícia administrativo, sendo sua atuação coordenada e difusa um dos principais pilares da efetividade da defesa do consumidor no país. Esse Sistema tem suas relações pautadas na integração entre os órgãos de defesa do consumidor. Enfim, todos os participantes do Sistema Nacional possuem autonomia para atuar, observados os limites do modelo federativo adotado na Constituição Federal, como forma de garantir a proteção e defesa do consumidor, da maneira mais adequada e eficiente possível.

A Secretaria Nacional do Consumidor – SENACON, segundo o artigo 106 do Código de Defesa do Consumidor, é responsável pela coordenação desse Sistema e, por tal razão, desenvolve a integração cooperativa, solidária e sinérgica dos órgãos de defesa do consumidor. Conforme o Decreto n. 7.738/2012, a SENACON deve se concentrar na articulação da cooperação que se fizer necessária entre os órgãos de interesse de defesa do consumidor competentes e atuar neste sentido quando as circunstâncias assim demandam.

Para tanto, o Departamento de Proteção e Defesa do Consumidor (DPDC), dentro das disposições regimentais da SENACON, é o órgão competente para fiscalizar e instruir demandas que envolvam relevante interesse geral e atinjam o âmbito nacional, bem como para aplicar sanções administrativas, nos termos da lei.

Dessa forma, os comandos expressos pelo artigo 55, § 1º, e pelo artigo 106, incisos VI e VII, do Código de Defesa do Consumidor, bem como pelo artigo 4º, *caput*, do Decreto n. 2.181/1997, determinam caber ao Departamento de Proteção e Defesa do Consumidor a análise de questões que tenham repercussão nacional e interesse geral, competindo aos órgãos regionais e locais de defesa e proteção ao consumidor, assuntos de cunho restrito às respectivas circunscrições territoriais e casos individuais específicos.

Assim, firma-se a competência do Departamento de Proteção e Defesa do Consumidor para processar e decidir o presente caso.

### DA PERTINÊNCIA SUBJETIVA DE FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA. AO POLO PASSIVO DA RELAÇÃO PROCESSUAL DESENVOLVIDA NO PRESENTE CASO

Ao longo dos autos, Facebook Brasil alega que não seria responsável pela prática das condutas apuradas no caso, pedindo a sua exclusão do feito, sob o fundamento de que os fatos em apuração, em tese, seriam de responsabilidade da matriz Facebook Inc.

Tal alegação não merece acolhida.

Com efeito, faz-se referência aos fundamentos aduzidos no Despacho

434/2019/CGCTSA/DPDC/SENACON (SEI 8634694), desde já reiterados.

No mais, cumpre registrar a literalidade do art. 11, (*caput* e § 2º) da Lei 12.965/2014 (Marco Civil da Internet), que assim dispõe (grifos acrescidos):

> *Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.*
> *(...)*
> *§ 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro* ***ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil****.*

Aliás, o eg. Tribunal de Justiça do Estado de São Paulo já se manifestou favoravelmente a esta tese por meio do seguinte julgado *verbis*:

> *O Facebook Brasil possui legitimidade para figurar no polo passivo da ação. A afirmação de que os produtos e serviços são disponibilizados pelos operadores Facebook Inc. e Facebook Ireland Limited* ***não prevalece para afastar a responsabilidade do apelante, uma vez que todos fazem parte do mesmo grupo econômico****.*
> *Assim, considerando a existência do grupo empresarial, a teoria da aparência e a solidariedade que* ***impera em razão da relação de consumo, a alegação de ilegitimidade de parte não deve ser acolhida****.* (excertos da fundamentação do voto condutor do seguinte julgado: TJSP; Apelação Cível 1009886-12.2014.8.26.0100; Relator (a): Alvaro Passos; Órgão Julgador: 2ª Câmara de Direito Privado; Foro Central Cível - 17ª Vara Cível; Data do Julgamento: 26/11/2018; Data de Registro: 27/11/2018, grifos acrescidos).

Assim, de se rejeitar o pedido de exclusão de Facebook Serviços Online do Brasil Ltda.

Não havendo mais questões de cunho processual a serem respondidas, passa-se, agora, à análise do mérito do caso.

## QUESTÃO DE ORDEM: SOBRE A ALEGAÇÃO DE NULIDADE TRAZIDA PELAS REPRESENTADAS QUANTO À EXTENSÃO DOS FATOS EM APURAÇÃO.

Neste ponto, é importante esclarecer que os fatos que constituem objeto de apuração estão relacionados à forma pela qual as Representadas trataram dos dados dos cerca de quatrocentos e quarenta e três mil usuários da plataforma Facebook em território nacional em relação ao aplicativo do Dr. Kogan (denominado *thisisyourdigitallife*) e se isso se constituiu em prática abusiva.

Todavia, é importante deixar claro que, contrariamente ao alegado pelas Representadas nos autos, a forma de obtenção do consentimento do usuário é questão umbilicalmente intrincada com a análise do mérito acerca da ocorrência, ou não, de prática abusiva, nos termos do art. 39 do Código de Defesa do Consumidor, aplicável ao caso haja vista a existência de consumidores afetados em território

brasileiro. O mesmo se aplica ao desenho das configurações-padrão de privacidade do usuário e à forma pela qual as informações sobre a política de uso da plataforma eram fornecidas aos seus consumidores (especialmente quanto ao compartilhamento de dados de amigos – ou amigos de amigos - de usuários que tenham feito adesão ao aplicativo do Dr. Kogan, compartilhamento este que, segundo as Representadas, já teria sido objeto de autorização *ex ante*, quando da adesão do consumidor às políticas de uso da plataforma Facebook).

A exposição abusiva dos dados dos usuários, conforme será visto, é apenas o resultado de uma série de fatores que, para o bem ou para o mal, estão associados ao modelo de negócios que rege a plataforma Facebook.

A análise e decisão sobre a abusividade na disponibilização dos dados dos usuários ao aplicativo do Dr. Kogan (sem prejuízo da discussão se houve, ou não, o fornecimento de dados desses usuários à SCL) impõe, como se pode ver, que sejam analisados os pontos referidos presente tópico, que são logicamente antecedentes a tal disponibilização, não havendo qualquer nulidade neste particular.

Essa relação entre esses antecedentes lógicos e a abusividade da prática será melhor aprofundada nos tópicos que seguem.

## DA PROTEÇÃO CONSTITUCIONAL, DOS PRINCÍPIOS BÁSICOS DA DEFESA DO CONSUMIDOR NO QUE SE REFERE AOS SEUS DADOS PESSOAIS E DA EXTENSÃO E GRAVIDADE DOS FATOS ENCONTRADOS

A Constituição Federal (CF) de 1988 situa o Direito do Consumidor no rol dos direitos e garantias fundamentais do cidadão e da coletividade (art. 5º, inciso XXXII) e estabelece que é dever do Estado promover, na forma da lei, a defesa do consumidor, além de determinar ser a proteção do consumidor baliza para a atividade econômica, nos termos do art. 170, inciso V, da Carta Magna.

O CDC é um microssistema jurídico que determina a prevalência dos Princípios da boa-fé e da transparência nas relações de consumo, com o intuito de garantir a harmonização dos interesses das partes. Nesse sentido, o Código instituiu o princípio da proteção da confiança do consumidor, o qual possui como um dos seus principais aspectos "*a proteção da confiança na prestação contratual, que dará origem às normas cogentes do CDC, que procuram garantir ao consumidor a adequação do produto ou serviço adquirido, assim como evitar riscos e prejuízos oriundos destes produtos e serviços*" (MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor**. São Paulo: Ed. Revista dos Tribunais. 3. Ed. 1999, p. 126 e 127).

A transparência, confiança, harmonia nas relações de consumo, reconhecimento da vulnerabilidade do consumidor, assim como a harmonização de interesses, com base na boa-fé e no equilíbrio nas relações entre consumidores e fornecedores, são princípios que estão expressamente previstos no artigo 4º do Código de Defesa do Consumidor, como se extrai do texto legal:

> *Art. 4º - A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios:*
> *I – reconhecimento da vulnerabilidade do consumidor no mercado de consumo;*
> *(...)*
> *III – harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento*

> *econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (art. 170 da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores.*

No presente caso, tem-se uma relação de consumo em que as representadas são consideradas fornecedoras para fins do art. 2º do CDC, na medida em que colocam à disposição dos consumidores brasileiros os serviços e produtos associados à plataforma Facebook, sendo aqueles, *a priori*, destinatários finais de tais serviços e produtos, ainda que esses últimos não sejam remunerados pelos consumidores (neste sentido: STJ, REsp 1444008/RS, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 25/10/2016, DJe 09/11/2016).

Neste particular, é importante destacar que, no que se refere à proteção dos dados pessoais dos usuários/consumidores da plataforma Facebook no âmbito do caso explorado nos autos, é irrelevante, para a caracterização dos prejuízos ao consumidor, que esses dados tenham sido efetivamente disponibilizados pelos desenvolvedores do aplicativo do Dr. Kogan à Cambridge Analytica.

Por oportuno, confiram-se as lições de Danilo Doneda, ao estabelecer a proteção dos dados pessoais como atualização do direito à privacidade constitucionalmente assegurado, especialmente no cenário atual de uso cada vez mais intensivo de *big data*, inteligência artificial e outras novas tecnologias (ainda que as origens históricas da proteção jurídica específica de dados pessoais – especialmente na Europa - estejam arraigadas em um mundo ainda analógico – i.e., anterior ao advento do uso cotidiano da internet - e estejam mais ligadas às relações entre cidadão e Estado de que às relações entre agentes privados – no caso: fornecedores e consumidores):

> *O tratamento de dados pessoais, em particular por processos automatizados, é, ao mesmo tempo, uma atividade que apresenta riscos cada vez mais claros. Risco que se concretiza* ***na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais; na eventualidade de esses dados não serem corretos e representarem erroneamente seu titular; na sua utilização por terceiros sem o conhecimento ou autorização de seu titular; na eventualidade de serem utilizados para fins discriminatórios, somente para citar algumas hipóteses concretas. Daí a necessidade de mecanismos que possibilitem à pessoa deter conhecimento e controle sobre seus próprios dados – que são, no fundo, expressão direta de sua própria personalidade****.*
> *(...)*
> *Os bancos de dados que contêm dados pessoais, tão comuns em nossos dias, proporcionam uma nova definição dos poderes e direitos sobre as informações pessoais e, consequentemente, sobre a própria pessoa. Aumenta o número de sujeitos que podem ter acesso a um conjunto sempre mais detalhado e preciso de informações sobre terceiros, o que faz com que o estatuto jurídico desses dados se torne um dos pontos centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo.*
> *(...)*
> *A legislação infraconstitucional mais recente, por sua vez, fornece fortes indicativos de que uma interpretação que leve em conta o caráter fundamental das garantias da posso em relação aos seus dados pessoais é, hoje, elemento integrante da cidadania. O Marco Civil da Internet, Lei 12.965/2014, prevê entre os princípios do uso da Internet do Brasil em seu artigo 3° a proteção da privacidade, bem como a proteção de dados pessoais, na forma da lei. A partir destas considerações, verifica-se que os direitos do usuário da Internet no Brasil, enunciados no artigo 7° da referida Lei, dispõem de forma específica sobre muitos aspectos relacionados à proteção de dados, chegando mesmo a enunciar, ainda que de forma reflexa, alguns de seus princípios*

> *clássicos, como o da finalidade e o da transparência.*
> *(...)*
> *O esforço a ser empreendido pela doutrina e pela jurisprudência seria, em nosso ponto de vista, basicamente, uma interpretação dos incisos X e XII do art. 5° que seja mais fiel ao nosso tempo, reconhecendo a íntima ligação que passam a ostentar os direitos relacionados à privacidade e à comunicação de dados. Uma tal leitura demonstra-se particularmente pertinente e relevante após a consideração de novos documentos normativos como o Marco Civil da Internet e da LGPD, ambas tecendo uma série de garantias e prerrogativas inerentes à cidadania e que defluem diretamente do reconhecimento do direito fundamental à proteção de dados. Dessa forma, a garantia da proteção dos dados pessoais, em si próprios considerados, com caráter de direito fundamental representa o passo necessário à integração da personalidade em sua acepção mais completa e adequada à Sociedade da Informação*. (DONEDA, Danilo. O Direito Fundamental à Proteção de Dados Pessoais. *In*: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Orgs.). **Direito Digital: Direito Privado e Internet**. 2. Ed. São Paulo: Editora Foco, 2019. p. 35-54, grifos acrescidos).

O que importa, para os presentes fins, é investigar se houve a quebra das legítimas expectativas dos consumidores contratantes da plataforma no que se refere à tutela do direito fundamental à proteção de seus dados pessoais. Para tanto, resta investigar se alguém (seja o desenvolvedor do aplicativo *thisisyourdigitallife*, seja a Cambridge Analytica) teve acesso indevido a tais dados, considerada a forma de obtenção do consentimento desses consumidores (o que será melhor respondido nos próximos tópicos). Ademais, cumpre acrescentar que:

01) a responsabilização administrativa por violação às normas de defesa do consumidor (art. 55 do CDC) não se confunde com a investigação da responsabilidade civil (aquiliana) por tais fatos (a princípio, independentes entre si), a qual sequer é competência deste DPDC. Assim, os pressupostos da responsabilidade aquiliana – como, *v.g.,* a existência de dano indenizável - não são investigados aqui. Novamente: o que se perquire é, se à luz dos fatos explorados, houve, ou não, prática abusiva em desfavor do consumidor;

02) os aspectos relacionados à disponibilização, ou não, dos dados fornecidos ao aplicativo do *thisisyourdigitallife* à Cambridge Analytica são irrelevantes para a caracterização da abusividade da prática. Isso será desenvolvido em tópico próprio;

03) Ainda assim, o encerramento do aplicativo decorreu muito mais da sua exposição na imprensa do que de uma atitude civilizada das entidades envolvidas (SEI 6366459- apenso 08012.001050/2018-14) – o que será visto mais a seguir.

**ANÁLISE DO CASO PROPRIAMENTE DITA. SOBRE O MODELO DE CONFIGURAÇÃO-PADRÃO DA PLATAFORMA FACEBOOK PARA OBTENÇÃO DO CONSENTIMENTO DO USUÁRIO NO QUE SE REFERE AO COMPARTILHAMENTO, COM DESENVOLVEDORES DE APLICATIVOS QUE OPERAM NA PLATAFORMA, DE DADOS DE AMIGOS (OU DE AMIGOS DE AMIGOS) DE USUÁRIOS DESSES APLICATIVOS. IMPLICAÇÕES DA ADOÇÃO DESSE MODELO NA FIXAÇÃO DO NÍVEL DE RESPONSABILIDADE DAS REPRESENTADAS NO QUE SE REFERE À PROTEÇÃO DOS DADOS DOS CONSUMIDORES DA PLATAFORMA À LUZ DO CDC E DO MARCO CIVIL DA INTERNET E AVALIAÇÃO DAS CONDUTAS DAS REPRESENTADAS.**

Dentre as alegações e provas colacionadas aos autos, ficou claro que, no âmbito da

plataforma Facebook, prevalece um modelo de obtenção do consentimento do usuário no sentido de promover, como *default*, o compartilhamento automático de dados desse usuário com os desenvolvedores de aplicativos aos quais os amigos desse usuário tenham subscrito. Exemplificativamente, se Ana é amiga de Clara, e se Clara subscreveu a um aplicativo hipotético chamado "Pessoas que gostam de gatos", como regra, os desenvolvedores desse aplicativo terão acesso não apenas aos dados compartilhados por Clara (que passou a utilizar o aplicativo), mas também aos dados de Ana, que não utilizara aplicativo nenhum. Dito de outra forma, como regra, se uma pessoa compartilha os seus dados com o desenvolvedor de um aplicativo (p. ex., quando passa a usá-lo), automaticamente (segundo as configurações-padrão da plataforma), esse desenvolvedor tem acesso aos dados dos amigos dessa pessoa.

Embora tal modelo não seja algo ilícito *per se* (e abstraída, por ora, qualquer discussão sobre como as informações sobre esse modelo são repassadas ao consumidor/usuário), ele será essencial para estabelecer o nível de cuidado que deverá ser exercido pelas representadas ao lidar com os dados desses consumidores.

Neste particular, o que se tem é que a Representada utilizou um *nudge* (um estímulo de comportamento) em que o compartilhamento instantâneo de informações de amigos de usuários que tenham aderido a um determinado aplicativo se dá num mecanismo *opt-out*, em vez de *opt-in*. Ainda, segundo Richard Thaler e Cass Sunstein, um nudge "*é um estímulo, um empurrãozinho, um cutucão; é qualquer aspecto da arquitetura de escolhas capaz de mudar o comportamento das pessoas de forma previsível sem vetar qualquer opção e sem nenhuma mudança significativa em seus incentivos econômicos. Para ser considerada um nudge, a intervenção deve ser barata e fácil de evitar. Um nudge não é uma ordem. Colocar as frutas em posição bem visível é um exemplo de nudge. Simplesmente proibir a junk food, não"*. (THALER, Richard; SUNSTEIN, Cass. **Nudge: O empurrão para a escolha certa.** Trad. Marcello Lino. Rio de Janeiro: Elsevier, 2009, p. 8).

Ainda segundo os mesmos autores, "*parece razoável dizer que as pessoas fazem boas escolhas nos contextos em que têm experiências, boas informações e feedback rápido – por exemplo, escolher sabores de sorvete. As pessoas sabem se gostam de chocolate, baunilha, café, alcaçuz ou de algum outro sabor. Elas não se saem tão bem nos contextos em que têm pouca experiência, poucas informações ou um feedback lento ou raro – por exemplo, na escolha entre uma fruta e um sorvete (um caso em que os efeitos de longo prazo são lentos e o feedback é fraco) ou na escolha de tratamentos médicos ou de opções de investimento*" (THALER, Richard; SUNSTEIN, Cass. **Nudge: O empurrão para a escolha certa.** Trad. Marcello Lino. Rio de Janeiro: Elsevier, 2009, p. 26).

Isso colocado, no presente caso, a simples adoção de um sistema de *opt-out*, em vez de um sistema de *opt-in,* tem implicações significativas. Afinal de contas, num sistema de *opt-in*, a quantidade de potenciais afetados no presente caso teria se limitado a oitenta e quatro usuários ou a um quantitativo não muito superior a isso (justamente aqueles usuários brasileiros que subscreveram o aplicativo *thisisyourdigitallife*), enquanto o sistema de *opt-out* implicou em um quantitativo superior a quatrocentos e quarenta mil usuários com seus dados expostos a tal aplicativo. Afinal de contas, é inverossímil acreditar que, num sistema em que sejam adotadas configurações-padrão de *opt-in*, os amigos de alguém que passasse a usar um aplicativo respondessem afirmativamente a cada solicitação de compartilhamento de dados que esse aplicativo fizesse a esses amigos. Ainda, é de se esperar que, caso esse fosse o modelo de negócios adotado pelas Representadas, a plataforma Facebook dificilmente teria a dimensão e porte (em capital, investimento e em capilaridade e quantidade de usuários) que possui atualmente.

E é esse mecanismo que se encontra subjacente à dinâmica de um *nudge*: fazer com que pessoas tomem decisões que não seriam tomadas na ausência dos mesmos. Não há nada de ilícito nisso, obviamente. Utiliza-se tal mecanismo em várias instituições existentes no país, tais como regimes complementares de previdência (com adesão automática de servidores e fixação de um plano *default*,

mas com possibilidade de desligamento e de alteração do plano de investimento contratado), no próprio Código de Defesa do Consumidor (ao tratar, nos arts. 103 e 104, dos efeitos da litispendência e da coisa julgada nas ações coletivas para a defesa de interesses individuais homogêneos), dentre outras.

Todavia, isso impõe uma maior responsabilidade ao aplicador do *nudge*. E não é à toa que os agentes decisores responsáveis pela gestão de fundos de pensão e de outros ativos se submetem a um escrutínio estrito tanto no Brasil como em vários lugares do mundo, seja em relação a acionistas minoritários, seja em relação aos participantes dos fundos, seja em relação a outros agentes e organizações que não tenham incentivos para uma participação relevante nesses processos decisórios.

Aqui, cabe, ainda, uma consideração adicional: essa responsabilidade não é eliminada nem mesmo por uma política de *full disclosure* (isto é, de total transparência) informacional.

Ainda que procedam as alegações dos Representados no sentido de que houve total transparência com os usuários quanto ao *default* de compartilhamento instantâneo de informações (o que será analisado a tempo e modo) , o contrato firmado entre o usuário e os titulares da plataforma se constitui em um contrato relacional – cuja execução se protrai no tempo. Não é possível antever se as consequências de sua execução, no presente caso, realmente estariam dentro do escopo do legítimo interesse das partes no momento da contratação e, além disso, há vasta literatura e evidências no sentido de que consumidores, em geral, tem dificuldades em dimensionar adequadamente as consequências futuras de decisões presentes, tomadas no momento da adesão aos termos de uso da plataforma.

Nesse cenário, dois pontos merecem destaque:

01) contratos relacionais (isto é, aqueles cuja execução de protraem ao longo do tempo), por definição, não oferecerão sempre *feedbacks* razoavelmente previsíveis aos seus participantes, pois, dada a existência de custos de transação e da racionalidade limitada das partes envolvidas, é inevitável que, eventualmente, tais contratos serão "completados" para eventos que, a princípio, podem não estar cobertos no leque de direitos e obrigações estabelecidos e de riscos alocados *ex ante* pelos contratantes. Deve ser destacado, ainda, que, quaisquer que sejam as alocações de direitos e obrigações decorrentes dessas decisões tomadas *ex post*, essas decisões sempre virão dotadas de externalidades, o que impõe cautela redobrada para que decisões de tal estirpe não deturpem *ex post* as expectativas das partes no momento da contratação *ex ante* – especialmente quanto a alocação de riscos a serem suportados pelos contratantes - e para que elas não criem insegurança jurídica e imponham um aumento sistêmico dos custos de transação;

02) mesmo políticas que envolvam o máximo de transparência informacional, ainda que feitas com o intuito de municiar o consumidor para que tome a melhor decisão possível, normalmente falham no atendimento dessa finalidade. Não bastasse, ainda que se tentem políticas de simplificação da linguagem das informações fornecidas, esse problema não é eliminado. Dito de outra forma, em muitos casos, tanto oferecer informações completas (o que pode ser um custo significativo para o usuário), como oferecer informações simples (com o risco de descarte de outras informações que, hipoteticamente, podem ser relevantes) não resolverão o problema da adequada compreensão dos termos do contrato (cf. BEN-SHAHAR, Omri; SCHNEIDER, Carl E. **More Than You Wanted to Know. The Failure of Mandated Disclosure.** Princeton: Princeton University Press, p. 121 *et seq*.).

Ainda, quanto a essa dificuldade de se dimensionar adequadamente as repercussões futuras de decisões presentes, merece destaque o pensamento de Amanda Flávio de Oliveira e Bruno Braz de Castro, *verbis*:

> *Enquanto o modelo neoclássico "presume que uma pessoa pode perfeitamente processar a informação disponível sobre cursos alternativos de ação, e pode classificar resultados possíveis em ordem de utilidade esperada" (ELLICKSON, 1989,*

> *p. 23), evidências comportamentais revelam que o modo como as preferências são apresentadas ao agente influem, ao menos em parte, em sua decisão final.*
> *Há importantes evidências de que os indivíduos, em vez de analisarem friamente os valores absolutos das alternativas que lhe são apresentadas, são mais sensíveis ao valor relativo de sua situação em face de algum nível de referência. Essa ciência é conhecida como o "viés do status quo", em razão de o indivíduo preferir o estado que percebe como o status quo em detrimento de algum estado alternativo (HANSON; KYSAR, 2008, p. 143).*
> ***Uma faceta do viés de status quo é a inércia: os indivíduos tendem a se manterem nas opções apresentadas a eles como padrão (default), e uma simples alteração no padrão pode influenciar o comportamento decisório*** *(KOROBKIN, 1998, p. 608). Não por acaso, a escolha da situação padrão é uni instrumento essencial. para a "arquitetura da escolha" de Thaler e Sunstein* (OLIVEIRA, Amanda Flávio de; CASTRO, Bruno Braz de. Proteção do consumidor de crédito: uma abordagem a partir da economia comportamental. **Revista de Direito do Consumidor**, v. 93, p. 240, mai.-jun. 2014., grifos acrescidos)

Também são oportunas as palavras de Bruno Bioni:

> *Dada a racionalidade limitada do ser humano, é pouco provável que ele esteja capacitado para tanto. Com efeito, a bounded rationality prescreve justamente que as habilidades cognitivas do ser humano são limitadas, minando a sua capacidade de absorver, memorizar e processar todas as informações relevantes para um processo de tomada de decisão. Já se faz impossível memorizar os inúmeros atores que compõem a referenciada rede social de publicidade, quanto mais compreender como os dados pessoais serão por eles tratados, já que cada um deles tem as suas respectivas políticas de privacidade. Soma-se, ainda, o complicador da compreensão de como a agregação dos dados pessoais desenrolar-se-á a ponto de extrair informações mais detalhadas sobre seus titulares. A complementar tal quadro problemático, há barreiras psicológicas que mistificam por completo a capacidade de o indivíduo controlar as suas informações pessoais. A primeira delas é a chamada teoria da decisão da utilidade subjetiva. O ser humano tem a tendência de focar nos benefícios imediatos, o que, de acordo com o arranjo e os modelos de negócios da economia informacional, é representado pelo acesso a um produto ou serviço on-line se de sopesar os possíveis prejuízos à privacidade, que são temporariamente distantes. De fato, os possíveis danos com relação à perda do controle sobre as informações pessoais só podem ser experimentados no futuro.*
> *(...)*
> *A própria lógica do trade-off da economia dos dados pessoais é traiçoeira, portanto, frente a tal arquitetura de escolha de decisões, notadamente por essa idiossincrasia entre gratificações imediatas e prejuízos mediatos/distantes. A crença de que o cidadão é um sujeito racional e capaz de desempenhar um processo genuíno de tomada de decisão para controlar seus dados pessoais é posta em xeque por toda essa complexidade envolta ao fluxo das informações pessoais.* ***Ele está em uma situação de vulnerabilidade específica em meio a uma relação assimétrica que salta aos olhos, havendo uma série de evidências empíricas a esse respeito****.*
> *(...)*
> *Trata-se, portanto, de se afastar de uma estratégia regulatória puramente liberal, que é incoerente com a posição de vulnerabilidade do sujeito em causa. Necessário se faz uma maior intervenção, seja do ponto de vista do desenho normativo ou da formulação de políticas públicas em lato sensu para que se empodere o sujeito*

> *vulnerável e, por outro lado, que não se foque apenas na instrumentalização do controle dos dados pessoais a ponto de se pensar em uma normatização substantiva da privacidade informacional*.
> (BIONI, Bruno Ricardo. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento**. Rio de Janeiro: Forense, 2019 p. 144-147 e 166).

Se soluções que partem do pressuposto de uma racionalidade perfeita do consumidor não são suficientes para lidar, de forma completa, com a sua condição de parte vulnerável nos contratos envolvendo as Representadas investigadas nos autos, os instrumentais da economia comportamental podem servir como ferramenta suplementar para a ajudar a compreender a extensão da vulnerabilidade, conforme visto acima (nesTe sentido: OLIVEIRA, Amanda Flávio de; CARVALHO, Diógenes Faria de. Vulnerabilidade comportamental do consumidor: por que é preciso proteger a pessoa superendividada. **Revista de Direito do Consumidor**, v. 104, p. 181-201, mar.-abr. 2016).

Isso, por sua vez, demanda a atuação de outros mecanismos para a adequada interpretação de negócios jurídicos celebrado, destacado que o art. 112 do Código Civil, determina que, *nas declarações de vontade se atenderá mais à intenção nelas consubstanciada do que ao sentido literal da linguagem*.

De qualquer forma, esse é o diagnóstico do modelo de consentimento adotado pelas Representadas. Nas próximas linhas, será feita uma análise desse modelo de configuração-padrão em apuração no presente feito à luz da legislação vigente e das considerações ora tecidas, especialmente para fins de fixação do nível esperado de atuação das Representadas e as consequências cabíveis em caso de ausência de atendimento dessas expectativas.

Inicialmente, é importante colacionar os seguintes dispositivos do Marco Civil da Internet (Lei 12.965/2014), os quais conferem maior densidade ao direito à privacidade e à intimidade (art. 5º, inc. X, da CF), incidentes diretamente sobre as relações privadas:

> *Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:*
> *I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;*
> *(...)*
> *VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;*
> *VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;*
> *VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:*
> *a) justifiquem sua coleta;*
> *b) não sejam vedadas pela legislação; e*
> ***c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;***
> ***IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;***
> *(...)*
> ***XI - publicidade e clareza de eventuais políticas de uso dos provedores de***

> ***conexão à internet e de aplicações de internet;***
> *(...)*
> ***XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.***
> *Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.*
> *(...)*
> *Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional,* ***deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.***
> *§ 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.*
> ***§ 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.***
> *§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.*
> *§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo (grifos acrescidos).*

Como se pode ver, tal legislação, em vigência na época em que o aplicativo *thisisyourdigitallife* estava disponível na plataforma Facebook, já assegura a proteção da privacidade e dos dados de usuários de aplicações fornecidas no âmbito da *internet*. Em que pese haver atualmente a Lei Geral de Proteção de Dados brasileira em período de *vacatio legis*, havia legislação específica aplicável ao caso, cuja interpretação deve se dar em consonância com o Código de Defesa do Consumidor. Também é importante deixar claro que os arts. 4º, caput, I, III e IV; 6º, II, III, IV e VI, art. 18, art. 31; art. 37, *caput*, e art. 39, na medida em que tal prática se aproveita da vulnerabilidade do consumidor acima narrada e o expõe a método desleal nos serviços e produtos que lhe são ofertados.

Isso colocado, ainda que haja inserção, nos termos de uso da plataforma, da possibilidade de compartilhamento instantâneo de dados de usuários discutida na presente nota, tal autorização de compartilhamento se deu em caráter genérico, uma vez que, *ex ante*, permaneciam em abertos dois pontos: a) que agentes concretamente teriam acesso a esses dados (notadamente, os desenvolvedores de aplicativo na plataforma) e b) qual a finalidade do tratamento das informações fornecidas pelos consumidores da plataforma. Isso está em violação aos termos do art. 7º, inc. VIII, alín. "c", *supra* transcrito. Afinal de contas, dizer que houve consentimento específico para uma finalidade indefinida *ex ante* é o mesmo que dizer que não houve consentimento para finalidade nenhuma, uma vez que não se encontra presente o atributo da especificidade.

Isso implica dizer, ainda, que os consentimentos obtidos desta forma são ilícitos ou que tal modelo de negócios, *per se*, não deva ser adotado? Obviamente não.

Por outro lado, caso algum fornecedor queira enveredar por esta prática, em vez de por exemplo, exigir autorização pontual e episódica (ou algo que se traduzisse como um modelo de *opt-in*) para cada ato de tratamento dos dados dos usuários, terá de arcar com um nível de monitoramento,

sobre os desenvolvedores de aplicações da plataforma, muito mais eficiente do que a exigida nesse modelo de *opt-in*. Afinal de contas, os riscos à privacidade dos usuários decorrentes deste modelo mais "agressivo" de obtenção de dados de usuários são muito mais significativos do que na primeira hipótese. Tanto isso se confirma que, se forem considerados apenas os dados de brasileiros que tenham feito adesão ao aplicativo do Dr. Kogan, haveria apenas oitenta e quatro envolvidos (ou um quantitativo não muito superior a isso), enquanto que, no modelo de *opt-out* adotado pelas Representadas, esse número salta para mais de quatrocentos e quarenta e três mil.

Assim, o ordenamento brasileiro exige das Representadas que, dentro da magnitude desse modelo de negócios, adote um nível de monitoramento, sobre os desenvolvedores que operem na plataforma Facebook, que seja compatível com esse modelo. Qualquer mau uso, por um desenvolvedor, dos dados dos usuários da plataforma, terá consequências relevantes para a coletividade de seus consumidores, restando entendido, aqui, que o fornecimento de informações claras e completas (o que será objeto de avaliação em momento posterior) não se mostra suficiente para o adequado tratamento do problema ora narrado, demandando, em caráter excepcional, a intervenção estatal para a seu enfrentamento de forma menos imperfeita que a adoção, pura e simples, do modelo da escolha racional. Entre as duas alternativas (isto é, entre preservar uma falha de mercado ou correr o risco de se criar uma falha de governança, que trazem benefícios e vieses que lhes são próprios), fica-se com o risco da segunda. Embora a intervenção governamental no que se refere às novas tecnologias deve ser excepcional e devidamente avaliada - uma vez que se espera que normalmente os agentes do mercado cheguem a soluções mais eficientes para os problemas envolvendo os produtos e serviços que ofereçam do que as instituições estatais (neste sentido: HENDERSON, M. Todd; SALEN, Churi. **The Trust Revolution: How the Digitization of Trust Will Revolutionize Business and Government**. Cambridge: Cambridge University Press, p. 168 *et seq*.). Neste caso, diante das ponderações trazidas ao longo da presente nota, a intervenção estatal faz-se necessária, ainda mais tendo em vista o robusto leque de normas jurídicas incidentes sobre os fatos averiguados, bem como a circunstância de que o acordo celebrado entre a FTC e Facebook Inc. envolve medidas até mais drásticas inclusive para suas subsidiárias e para as respectivas plataformas (como a criação de quóruns qualificados para aprovação de determinadas decisões e a alteração da estrutura de sua governança - inclusive quanto à gestão da privacidade dos usuários - dentre outras) do que as sanções que o CDC brasileiro traz para as infrações administrativas que atentem contra o consumidor.

Com efeito, para o bem ou para o mal, a utilização de *big data,* da inteligência artificial, da internet das coisas, da realidade aumentada, dentre outras novas tecnologias, orientará a oferta de bens e serviços aos consumidores bem como a condução de modelos políticos (democráticos ou não) nos próximos anos (e, certamente, nas próximas gerações), merecendo atenção as afirmações de Yuval Noah Harari:

> *Pois estamos agora na confluência de duas imensas revoluções. Por um lado, biólogos estão decifrando os mistérios do corpo humano, particularmente do cérebro e dos sentimentos. Ao mesmo tempo cientistas da computação estão nos dando um poder de processamento de dados sem precedente. Quando a revolução na biotecnologia se fundir com a revolução na tecnologia da informação, ela produzirá algoritmos de Big Data capazes de monitorar e compreender meus sentimentos muito melhor do que eu, e então a autoridade provavelmente passará dos humanos para os computadores. Minha ilusão de livre-arbítrio provavelmente vai se desintegrar à medida que eu me deparar, diariamente, com instituições, corporações e agências do governo que compreendem e manipulam o que era, até então, meu inacessível reino interior.*
> *(...)*
> *Uma vez que a IA toma decisões melhor do que nós sobre carreiras e até mesmo relacionamentos, nosso conceito de humanidade e de vida terá de mudar. Humanos costumam pensar sobre a vida como um drama de tomadas de decisão. A democracia*

> *liberal e o capitalismo de livre mercado veem o indivíduo como um agente autônomo que está constantemente fazendo escolhas no que tange ao mundo.*
> *(...)*
> *Quando a autoridade passa de humanos para algoritmos, não podemos mais ver o mundo como o campo de ação de indivíduos autônomos esforçando-se por fazer as escolhas certas. Em vez disso, vamos perceber o universo inteiro como um fluxo de dados, considerar organismos pouco mais que algoritmos bioquímicos e acreditar que a vocação cósmica da humanidade é criar um sistema universal de processamento de dados — e depois fundir-se a ele. Já estamos nos tornando, hoje em dia, minúsculos chips dentro de um gigantesco sistema de processamento de dados que ninguém compreende a fundo. Todo dia eu absorvo incontáveis bits de dados através de e-mails, tuítes e artigos. Na verdade, não sei onde me encaixo nesse grande esquema de coisas, e como meus bits de dados se conectam com os bits produzidos por bilhões de outros humanos e computadores. Não tenho tempo para descobrir, porque eu também estou ocupado, respondendo a e-mails.* (HARARI, Yuval Noah. **21 lições para o século 21**. São Paulo: Companhia das Letras. Edição do Kindle)

É importante relembrar que a manutenção do ciclo de prosperidade iniciado com a terceira revolução industrial (ganhando novos contornos com a quarta) e que molda o nosso modo de viver atual (que está longe de ser algo perfeito e acabado, mas que ainda é preferível à forma pela qual a humanidade moldou suas instituições nos dez mil anos que lhe antecederam) depende da manutenção de instituições inclusivas que permitam que as pessoas troquem informações para que, por tentativa e erro, possam produzir inovações (tecnológicas, institucionais etc.) as quais, de quando em quando, têm o efeito de melhorar o bem-estar dos indivíduos. Levado às últimas consequências, o modelo de consentimento adotado pelas Representadas (que já dispõem de um notório poder de mercado), sem quaisquer salvaguardas aos usuários, vai na contramão dessa inclusividade, uma vez que isso se traduz numa autorização em branco que coloca em xeque o próprio princípio do desenvolvimento da personalidade (art. 2º, inc. III, do Marco Civil da Internet), pois, ao perder o controle do fluxo de seus dados pessoais, a individualidade do próprio consumidor começa a se dissolver e, assim, a própria estrutura dessa inclusividade.

Transcrevam-se, por oportuno, as lições de Bruno Bioni:

> *Para além da perspectiva subjetiva de que cada ser humano detém seus prolongamentos – atributos e características características próprias que o tornam singular –, encaixam-se os dados pessoais como um elemento que compõe essa singularidade. Não se pode perder de vista que todo esse desenho só tem razão de ser porque a pessoa é um ser eminentemente social. A sua singularidade-subjetividade aperfeiçoa-se na social-intersubjetividade. Em outros termos, se não houvesse o social não se justificaria o singular, pois é no meio coletivo que se faz possível considerar e identificar o "eu" – individual – frente aos outros – multidão. Portanto, tais ideias são condicionadas transcendentalmente uma pela outra. Daí por que pensar em direitos da personalidade não é uma reflexão sob uma categoria jurídica assentada em uma solidão ôntica, mas, sobretudo, uma concepção ontológica da pessoa humana. Como bem traçado por Diogo Costa Gonçalves, a pessoa se concretiza quando ela se relaciona (intersubjetividade), isto é, quando ela responde ou procura afirmar quem ela é em meio à comunidade. A noção completa dos direitos da personalidade liga-se necessariamente à tutela jurídica para que a pessoa possa se realizar e se relacionar junto à sociedade, completando justamente a locução, antes mencionada, projeção social. Do contrário, haveria uma visão míope do que é tal categoria jurídica que deve compreender as atividades de inter-relacionamento da pessoa. O ser humano não é uma ilha, ele se conforma e se desenvolve quando se relaciona com os demais*

> *"no seio da sociedade que o abriga". Nesse sentido, os dados pessoais não só se caracterizam como um prolongamento da pessoa (subjetividade), mas, também, influenciam essa perspectiva relacional da pessoa (intersubjetividade). A proteção dos dados pessoais é instrumental para que a pessoa possa livremente desenvolver a sua personalidade*. (BIONI, Bruno Ricardo. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento**. Rio de Janeiro: Forense, 2019, p. 82-83).

Esse modelo de consentimento não necessariamente implica em melhora na experiência ou no bem-estar do consumidor e permite um modelo institucional em que organizações que adotem uma perspectiva mais ponderada (para simplificação, algo que se assemelhe a um modelo de *opt-in*), mas que atendam, de forma mais satisfatória, essa matriz principiológica discutida nas linhas anteriores, estejam destinadas a perecer. Mais especificamente, a ausência de qualquer sanção às Representadas constitui-se numa sinalização, ao consumidor, de que o mercado em que as Representadas operam se encontra num processo de seleção adversa, onde, pelo nível de assimetria de informações entre fornecedores e consumidores no que se refere a aspectos associados ao bem ou serviço ofertado, esses últimos não consigam ter uma adequada dimensão dos riscos que tais bens ou serviços oferecem. Isso, ao fim, fará com que – mantidas idênticas todas as demais variáveis - esse consumidor não consiga depositar, nos fornecedores, a confiança esperada para que o uso dos potenciais benefícios de novas tecnologias (*big data*, inteligência artificial, realidade aumentada, internet das coisas etc.) sejam levados ao máximo possível.

Assim, afasta-se qualquer tese no sentido de que houve responsabilidade exclusiva do próprio consumidor ou de terceiro (sem prejuízo do exercício de eventual direito de regresso contra quem de direito), uma vez que os próprios Representados interviram na cadeia de consumo e ofertaram o serviço no âmbito do qual os fatos em apuração foram constatados, permitindo o compartilhamento indevido de dados de consumidores/usuários da plataforma Facebook com o aplicativo *thisisyourdigitallife* (o que já é suficiente para o reconhecimento da prática abusiva) em contexto cujas repercussões são potencializadas pelo modelo de consentimento adotado pela plataforma Facebook. Assim, devem ser solidariamente responsabilizados.

Ainda, é importante deixar claro que, o caráter "genérico" do consentimento obtido pela plataforma Facebook em face de seus usuários não pode ser visto como um "cheque em branco" para que esses dados sejam disponibilizados a quem quer que seja e, no caso dos autos, o comportamento das Representadas não estava em consonância com a declaração de vontade dos consumidores (notadamente aqueles que não aderiram ao aplicativo *thisisyourdigitallife*), violando, dentre outros, o art. 112 do Código Civil (que também é aplicável ao presente caso, em harmonia com o CDC), acima transcrito. As Representadas também não se desincumbiram de demonstrar que tais dados não foram eliminados e nem foram compartilhados com os responsáveis pela Cambridge Analytica, conforme visto acima. Por fim, é importante esclarecer que são as Representadas que – no âmbito do modelo de *opt-out* adotado – dispõem de maior capacidade de monitorar os desenvolvedores de aplicativos que operam na plataforma Facebook do que os próprios consumidores.

Tendo em vista o que foi colocado ao longo da presente Nota, notadamente a implicação de um dever maior de cuidado que deve ser imposto à plataforma Facebook na guarda das informações disponibilizadas pelos seus usuários, verifica-se à ocorrência de prática abusiva. Com efeito, (apesar de todas as contradições das Representadas quanto a extensão dos fatos apurados), resta evidente que dados dos cerca de quatrocentos e quarenta e três mil usuários da plataforma estavam em disposição indevida pelos desenvolvedores do aplicativo *thisisyourdigitallife* para finalidades, no mínimo, questionáveis, e sem que as Representadas conseguissem demonstrar eventual fato modificativo de que tal número foi efetivamente menor. Neste particular, é importante destacar que é incontroverso nos autos que tal aplicativo atuou em violação aos termos de uso da plataforma Facebook. Em sendo assim, é inevitável que dados de usuários brasileiros foram parar em mãos erradas e ficaram, no mínimo,

submetidos a risco concreto (e não meramente abstrato) de serem tratados para finalidades não consentidas.

Tal risco, dentro do modelo de negócios adotado pela plataforma Facebook – notadamente tendo em vista a generalidade do consentimento quanto aos destinatários dos dados e quanto à finalidade (como visto, um cheque em branco para o tratamento dos dados dos usuários da plataforma), a adoção do modelo de *opt-out* de compartilhamento automático dos dados dos usuários com os desenvolvedores de aplicativos aos quais seus amigos tenham feito adesão, e a ausência de uma política efetiva, por parte das Representadas, na proteção dos dados de seus usuários em relação aos eventos ora apurados (na prática, limitando-se a uma autorização genérica de compartilhamento de informações, a qual, por si só, é insuficiente, especialmente no presente caso) e o número de pessoas que tiveram seus dados expostos indevidamente ao aplicativo do Dr. Kogan – enseja a conclusão de que as Representadas realmente incorreram em prática abusiva em desfavor do consumidor brasileiro e, portanto, devem ser sancionadas nos termos dos arts. 55 e ss. do Código de Defesa do Consumidor.

## SOBRE A ARGUMENTAÇÃO ACERCA DA AUSÊNCIA DE FORNECIMENTO DOS DADOS DE CONSUMIDORES BRASILEIROS À CAMBRIDGE ANALYTICA (SCL)

As Representadas informam, nos autos, que os dados dos consumidores brasileiros disponibilizados à plataforma do Dr. Kogan não teriam sido disponibilizados à Cambridge Analytica.

Dito isso, é importante trazer à baila o seguinte trecho da Nota Técnica 108 (8211818):

> *Conclui-se, dessa forma, que aparentemente houve falha na prestação do serviço do fornecedor Facebook Inc. e Facebook Serviços on Line do Brasil Ltda., que permitiu que terceiros pudessem utilizar indevidamente dados sensíveis dos consumidores. A atividade desenvolvida pelos Representados de aglutinar em massa informações se constitui em risco do negócio por eles conduzido, na medida em que eles devem ser responsáveis pela segurança dessas informações, de modo que possa vir a ser eventualmente responsabilizados diretamente pelos danos causados.*

Como se pode ver, o que se investiga, no presente caso, é a ocorrência de prática abusiva, à luz do CDC e da legislação de regência (notadamente o Marco Civil da Internet, além da própria Constituição Federal), cuja autoria é atribuída às Representadas, no sentido de permitir a exposição indevida de dados dos usuários brasileiros, independente de efetivo tratamento ulterior de tais dados para fins de direcionamento de publicidade de produtos e serviços ou para fins de indução de comportamento, dentre outras aplicações possíveis.

Isso colocado, especialmente no que se refere à disponibilização, ou não, dos dados de consumidores brasileiros fornecidos ao aplicativo *thisisyourdigitallife* à Cambridge Analytica, ainda que isso seja **irrelevante para a caracterização da abusividade** da prática (embora possa influir na gravidade do ato para fins de determinação da sanção aplicável), é importante deixar claro que foi determinada, nos autos, a distribuição dinâmica do ônus da prova, a qual, nos termos do Despacho nº 629/2019/CGCTSA/DPDC/SENACON (SEI 9200792), foi assim expressada:

> *Isso colocado, constata-se que, seja com fundamento no art. 6º, inc. VIII, do CDC (aplicável ao caso), seja com fundamento nos arts. 15 c/c 373, § 1º, do CPC, o caso é de se atribuir às representadas (que desenvolvem e mantêm os códigos da plataforma) o ônus de demonstrar que houve realmente o adequado dever de cuidado no trato das*

> *informações de seus usuários que estão sob sua custódia. Esse entendimento se aplica seja no que se refere à exposição dos dados dos usuários à empresa acima mencionada* [i.e., Cambridge Analytica], *seja em relação à exposição no que se refere à exposição de tais dados por outros mecanismos desenvolvidos por meio da interface Facebook login*. (referência à Cambridge Analytica inserida aqui para fins de contextualização).

No entanto, as provas trazidas aos autos que endereçaram o tema diretamente são declarações da própria Representada Facebook Inc. e dos responsáveis pela Cambridge Analytica e pelo aplicativo do Dr. Kogan, destacado que o próprio Mark Zuckerberg, em declaração de maio de 2018 (SEI 6366459 - apenso 08012.001050/2018-14), não tem certeza da eliminação desses dados (onde tal eliminação supostamente teria se dado na primavera de 2017 no hemisfério norte, conforme SEI 9297919 - apenso 08012.002112/2019-96), tendo ele determinado a realização de auditoria nas empresas envolvidas.

Isso, por sua vez, implica dizer que os riscos de tratamento não consentido desses dados não foram eliminados.

Ainda, conforme documentação trazida pelas Representadas (SEI 9297919 – apenso 08012.002112/2019-96), há relatório que trata das atividades das empresas SCL e GSR (esta última gerenciada por Aleksandr Kogan), sinalizando, dentre outros pontos: a) que, embora não tenham sido encontradas falhas na segurança dos dados obtidos pelo aplicativo *thisisyourdigitallife* e repassados a tais empresas, não há como se afirmar peremptoriamente que tais falhas não existiram (págs. 11-12 de tal relatório – item 20); b) que há sinalização de que futuramente seria realizada auditoria independente sobre tais empresas (pág. 15 – item 27). Quanto a esse último ponto, entende-se que essa auditoria seria aquela referida por Zuckerberg na declaração acima e que, se ela foi realizada, o relatório respectivo não foi juntado aos autos, motivo pelo qual se conclui que, probatoriamente, não procedem as alegações de que tais dados foram eliminados, sempre destacado que a circunstância ora estudada não é elemento necessário, nem suficiente, para a caracterização da prática abusiva.

## SOBRE AS APURAÇÕES REALIZADAS PELA FEDERAL TRADE COMISSION (FTC) NORTE-AMERICANA NO QUE SE REFERE AO DEVER DE FORNECEDIMENTO DE INFORMAÇÕES TRANSPARENTES, CLARAS E ADEQUADAS

Conforme documentos juntados por meio do Despacho 848 (10147266), em meados de 2012 , a FTC ajuizou demanda em face de Facebook Inc. alegando, em síntese, que as informações disponibilizadas na ferramenta de configuração de privacidade do usuário seriam enganosas por não trazerem quaisquer esclarecimentos no sentido de que a restrição de compartilhamento de informações apenas a amigos ou apenas a amigos de amigos não excluía a possibilidade de compartilhamento automático de tais informações com os desenvolvedores de aplicativos aos quais tais amigos ou amigos de amigos tivessem feito adesão.

Confira-se o seguinte trecho de tal petição (tradução livre):

> *14. Nenhuma das páginas descritas nos parágrafos 10 a 13 revelou que a escolha do usuário de restringir as informações do perfil a "Somente amigos" ou "Amigos de amigos" seria ineficaz em relação a certos terceiros. Apesar disso, em muitos casos, o Facebook tornou as informações de perfil que um usuário optou por restringir a "Somente amigos" ou "Amigos de amigos" acessíveis a qualquer aplicativo de plataforma usado pelos amigos do usuário (doravante "Apps de amigos"). As*

> *informações compartilhadas com esses aplicativos de amigos incluíram, entre outras coisas, aniversário de um usuário, cidade natal, atividades, interesses, atualizações de status, estado civil, educação (por exemplo, escolas frequentadas), local de trabalho, fotos e vídeos.*
> *(...)*
> *33. Na verdade e de fato, conforme descrito no Parágrafo 31, de aproximadamente maio de 2007 a julho de 2010, em muitos casos, o Facebook concedeu aos Aplicativos de Plataforma acesso irrestrito às informações de perfil de usuário que esses Aplicativos não precisavam para operar. Portanto, a representação estabelecida no Parágrafo 32 constitui uma declaração falsa ou enganosa representação.*

Além disso, ainda conforme tal documento, Facebook Inc., quando da alteração de sua política de uso, em 2009, teria falhado em informar adequadamente os usuários do Facebook sobre as consequências da adoção do *default* das informações publicamente disponíveis sugerido pela plataforma.

Isso, posteriormente, conforme SEI 10148102, levou à celebração de um acordo com a FTC em meados dos anos de 2011 e 2012, segundo o qual havia sido ordenado que a plataforma apresentasse informações claras e precisas a respeito da extensão e alcance das opções dos consumidores na configuração de sua privacidade, dentre outras medidas destinadas a melhorar a privacidade dos usuários da plataforma Facebook.

Anos depois (vide SEI 10148126), sob o fundamento de que tal acordo não vinha sendo cumprido a contento, a FTC apresentou, em 24/07/2019, nova demanda em desfavor de Facebook Inc. perante a Justiça norte-americana. Em tal petição, é alegado que a plataforma Facebook teria se comprometido publicamente, em meados de 2014, a parar com o compartilhamento automático de dados de amigos de usuários de aplicativos da plataforma com os desenvolvedores de tais aplicativos. A FTC também alegou que a forma pela qual a plataforma Facebook divulgava informações sobre as políticas de privacidade ali praticadas continuava sendo feita de maneira enganosa aos usuários, além de continuar permitindo o compartilhamento automático de dados dos usuários (condicionado tal compartilhamento à aquiescência, pelos desenvolvedores de aplicativos da plataforma, à concordância das políticas de uso da própria plataforma), em vez de, simplesmente, banir essa prática.

Em seguida, a FTC e Facebook Inc. chegaram a um novo acordo em que essa última se compromete a uma série de obrigações, especialmente ao pagamento de uma multa de cinco bilhões de dólares, sem todavia, admitir nem negar os fatos imputados, exceto aqueles constantes no "Anexo A" ou "Attachment A", conforme Documento SEI 10148151, para fins de estabelecimento de Jurisdição.

Embora essa investigação da FTC tenha um escopo mais abrangente que o dos fatos apurados nos presentes autos, os entendimentos sobre a política de privacidade da plataforma Facebook ali trazidos são relevantes por repercutirem no caminho que leva desde à disponibilização dos dados dos usuários para a plataforma até a disponibilização ao aplicativo *thisisyourdigitallife*.

De qualquer forma, é importante ressaltar que, no acordo celebrado, ficou estabelecido que a plataforma deverá ter um novo programa de privacidade, especialmente sobre os seguintes dados pessoais (mas não limitados a eles): nome e sobrenome de usuários, geolocalização, e-mail ou outros dados de contato de usuários, números de telefone, fotos e vídeos, endereços IP, identidade do usuário (além de outros dados que possam tornar um usuário identificável), documentos emitidos por autoridades governamentais, contas bancárias, informações sobre dívidas ou créditos, data de nascimento, informações biométricas, qualquer combinação de tais informações, além de informações que não tenham sido disponibilizadas ao público por um usuário.

Isso implica, *a contrario sensu*, que as políticas de privacidade anteriormente praticadas pela plataforma não satisfaziam os melhores interesses dos consumidores norte-americanos. Isso,

somado à circunstância de que é incontroverso nos autos que a gestão dos dados usuários norte-americanos se submete aos mesmos centros de decisão a que os dados dos usuários brasileiros são submetidos (circunstância essa que levou a Representada Facebook Serviços Online do Brasil Ltda. a requerer a sua exclusão do presente procedimento, sob o fundamento de que Facebook Inc. é a responsável pela condução da plataforma Facebook), não autoriza outra conclusão senão a de que a veiculação das informações ao usuário da plataforma, à época dos fatos, era enganosa também no Brasil.

Compulsando, ainda, a documentação acostada aos autos, verifica-se, na Petição 6366459 - apenso 08012.001050/2018-14 / pgs. 145/146 - que Mark Zuckerberg admite que a plataforma falhou em manter a confiança esperada dos seus consumidores quanto aos serviços e produtos que oferece. Embora isso não implique, conforme alegado pelas Representadas, confissão quanto à matéria de fato, é um elemento de prova que merece ser cotejado com o restante do acervo probatório constante dos autos.

Isso, aliás, soa extremamente contraditório com a tese de defesa das Representadas, no sentido de que os consumidores da plataforma Facebook (especialmente aqueles que não utilizaram o aplicativo *thisisyourdigitallife*) teriam concordado com a forma de agir do Dr. Kogan. Enfim, há o reconhecimento de uma postura que não se encontra nos melhores interesses dos consumidores da plataforma. E mais: a plataforma não demonstra que houve o fornecimento de informação clara e adequada, ao seu consumidor, no sentido de que a restrição de compartilhamento de dados a apenas a amigos ou a amigos de amigos, não afastaria a adoção do *default* de compartilhamento desses dados com os desenvolvedores de aplicativos da plataforma que esses amigos e amigos de amigos (conforme o caso) passassem a usar. Em tempo, e contrariamente ao alegado no SEI 9297919 (apenso 08012.002112/2019-96), as alterações nas políticas de uso promovidas em 2013 pela plataforma foram, no mínimo, inócuas para a resolução do problema na clareza dessas informações.

Nesse ponto, as evidências trazidas aos autos (notadamente, a documentação da FTC) corroboram essa afirmação até enquanto se utilizou a plataforma de desenvolvimento Graph API V1, frisado que a implementação da plataforma Graph API V2 (que supostamente seria destinada a amenizar esse problema) se deu posteriormente ao início da conduta imputada ora apreciada e, ainda assim, de forma gradual, e sem qualquer capacidade de impedir, no âmbito do aplicativo *thisisyourdigitallife*, o compartilhamento indevido de dados dos usuários da plataforma Facebook.

De qualquer forma, independentemente da plataforma de desenvolvimento de aplicativos utilizada, é incontroverso que os dados de mais de quatrocentos e quarenta três mil usuários brasileiros (exceto aqueles que assinaram o aplicativo) chegaram às mãos do aplicativo do Dr. Kogan por força da política de informações da plataforma, com padrão de definição de preferências envolvendo o compartilhamento automático ora comentado.

Ainda, conforme petição da FTC que informa o descumprimento do acordo de 2012 (SEI 10148126), segundo a qual, cerca de quatro meses depois da celebração do acordo, a plataforma teria dissociado a tela destinada às definições de privacidade em relação às informações disponibilizadas aos amigos da tela relacionada às definições de privacidade relacionada aos aplicativos (inclusive no que se refere ao padrão de definição de compartilhamento automático de informações narrado ao longo da presente nota). Isto é, constam evidências trazidas por tal agência (vide itens 35 e ss. e capturas de tela ali anexadas), no sentido de que a plataforma Facebook teria alterado, pouco tempo depois da celebração do acordo de 2012, a forma pela qual a sua política de privacidade era mostrada ao usuário, de modo que, em forma nada transparente, esse usuário fosse induzido a acreditar que, restringindo a disponibilização de dados pessoais a apenas amigos ou a amigos de amigos, seus dados estariam imunes a qualquer possibilidade de que terceiros (desenvolvedores de aplicativos ou não) tivessem acesso a esses dados por meio dos mecanismos ordinários disponibilizados (pelo que se excluem, *v.g.*, as hipóteses de *data breach* – vazamento de dados) pela plataforma Facebook.

Em tempo, tal documentação foi juntada aos autos e, instadas a se manifestarem sobre o seu teor, nem o seu conteúdo e nem a sua autenticidade foram impugnados pelas Representadas (que se limitaram a tecer considerações sobre as imputações feitas a partir das págs. 43 e ss. – mais especificamente: a partir do item 155).

Ainda segundo tal petição:

> *O Facebook não divulgou nenhum lugar nesta página ou em qualquer lugar ao longo do caminho que os usuários tivessem que seguir para acessar a página Configurações de privacidade, que os usuários que compartilharam suas postagens com "Amigos" ou com um público "personalizado" ainda pudessem compartilhar essas postagens com qualquer um dos milhões de desenvolvedores de terceiros cujos aplicativos foram usados por seus amigos (tradução livre).*

Aliás, ainda conforme tais achados, não havia também fornecimento de tal informação sobre o compartilhamento automático também para outras postagens como fotos, vídeos etc.

E mais: Facebook anunciara, em conferência realizada em meados de 2014, que não mais faria compartilhamento automático de dados de amigos (de amigos de amigos etc.) com aplicativos que eles utilizassem. No entanto, a documentação em análise evidencia que tais dados ainda podiam ser acessados por desenvolvedores em meados de 2015 e que, mesmo durante o ano de 2014 (época em que o aplicativo *thisisyourdigitallife* ainda estava em funcionamento na plataforma), a plataforma Facebook continuava a não informar os usuários adequadamente sobre o esse modelo de compartilhamento de dados pessoais com os desenvolvedores de aplicativos.

Enfim, não procedem as alegações no sentido de que a plataforma fornecia informação clara e adequada sobre o compartilhamento de dados dos usuários com os desenvolvedores de aplicativos.

## CONSIDERAÇÕES FINAIS

Ao longo da presente Nota, pode ser visto que os Representados expuseram indevidamente dados de usuários ao aplicativo *thisisyourdigitallife*, com todas as nuances constantes da fundamentação acima trazida. Notadamente, constatam-se as seguintes condutas indevidas:

01) os Representados, pela adoção de um modelo de negócios que implicava em um padrão de configuração (decorrente de um *nudge*) de compartilhamento automático de dados de amigos (ou amigos de amigos etc.) de usuários com os aplicativos utilizados por esses últimos, deveriam ter um cuidado muito maior na gestão desses dados, uma vez que o modelo de consentimento adotado teve implicações relevantes para o número de pessoas com dados expostos (o qual é certamente muito maior do que se fosse adotado um modelo de *opt-in* para tal compartilhamento de tais dados). Neste particular, deve ser ponderado que tal lógica fez parte (pelo menos dentro do período em que se deram as condutas apuradas) do modelo de negócios da plataforma e, como tal, as Representadas também devem arcar com os riscos daí decorrentes quanto à proteção dos direitos de personalidade e da privacidade de seus usuários. Ainda quanto aos fatos em análise, as Representadas falharam em oferecer a proteção correspondente;

02) Ademais, as Representadas falharam em informar adequadamente, à época dos fatos apurados, os seus usuários sobre as implicações das configurações-padrão de privacidade, especialmente no que se refere à relação entre os dados que devem ser mostrados apenas a amigos ou a amigos de amigos etc. e sobre como isso (não) repercute em relação aos dados compartilhados com

desenvolvedores de aplicativos que esses amigos (ou amigos de amigos etc.) passem a utilizar. É forçoso concluir, aqui, que essa falha é elemento importante para a configuração da prática abusiva ora apurada e para o compartilhamento indevido de dados de usuários ora analisado.

Assim, constata-se a ocorrência de prática abusiva nos termos dos artigos 4º, caput, I, III e IV; 6º, II, III, IV e VI, art. 18, art. 31; art. 37, *caput*, e art. 39, todos do Código de Defesa do Consumidor, além das disposições do Marco Civil da Internet, notadamente, os arts. 2º, inc. II e III, e 7º, incs. VI, VII, VIII, IX, e XIII.

Sugere-se a aplicação de multa pela lesividade à coletividade de consumidores, a ser avaliada no tópico que segue.

**DOSIMETRIA DA MULTA**

A individualização da sanção administrativa deve observar os critérios estabelecidos pelos artigos 24 a 28 do Decreto Federal nº 2.181/1997, bem como pela Portaria nº 7/2016 da SENACON. A fixação dos valores das multas às infrações ao Código de Defesa do Consumidor dentro dos limites legais previstos nos art. 9º e 12 da Portaria n° 7 da SENACON será feita levando em consideração os seguintes parâmetros e critérios: Gravidade da infração; Extensão do Dano; Condição Econômica do Fornecedor e Receita Mensal Bruta.

Ocorre que, no presente caso, não foram fornecidos os seguintes dados: extensão do dano (o qual não é quantificável pecuniariamente) e receita mensal bruta (não fornecida), motivo pelo qual se afasta a aplicação da referida Portaria. Diante disso, aplica-se o art. 14, § 2º, da Portaria 07/2016 SENACON, uma vez que não é possível fixar pena em patamar razoável e proporcional com utilização dos critérios acima. Em tempo, caso se considere eventual faturamento bruto da Representada Facebook Inc. (uma das dez companhias de maior valor mundialmente), é possível que haja pena desproporcionalmente elevada.

Assim, passa-se a dosimetria com base nos critérios do art. 57, parágrafo único, da Lei 8.078/90, regulamentado pelo art. 28, do Decreto 2.181/97, que assim dispõem:

> ***Lei 8.078/90:***
> *Art. 57. A pena de multa, graduada de acordo com a gravidade da infração, a vantagem auferida e a condição econômica do fornecedor, será aplicada mediante procedimento administrativo, revertendo para o Fundo de que trata a Lei nº 7.347, de 24 de julho de 1985, os valores cabíveis à União, ou para os Fundos estaduais ou municipais de proteção ao consumidor nos demais casos. (Redação dada pela Lei nº 8.656, de 21.5.1993)*
>
> ***Decreto 2.181/97***
> *Art. 28. Observado o disposto no art. 24 deste Decreto pela autoridade competente, a pena de multa será fixada considerando-se a gravidade da prática infrativa, a extensão do dano causado aos consumidores, a vantagem auferida com o ato infrativo e a condição econômica do infrator, respeitados os parâmetros estabelecidos no parágrafo único do art. 57 da Lei nº 8.078, de 1990.*

No presente caso, o fornecedor incorreu em prática abusiva, infração esta qualificada em grau médio. A extensão dos danos e a vantagem auferida com o fato, embora não mensurados, podem ser avaliadas como não triviais, na medida em que fizeram parte de seu modelo de negócios atingindo seus consumidores de forma significativa, tendo afetado mais de quatrocentos e quarenta mil

consumidores brasileiros com a exposição indevida de seus dados ao aplicativo *thisisyourdigitallife*, com as repercussões daí decorrentes. Os infratores são empresas de grande porte.

Diante disso, sugere-se a fixação da pena-base em R$ 6.600.000,00 (seis milhões e seiscentos mil reais).

Analisando as circunstâncias atenuantes, é possível concluir que os infratores são primários (art. 25, inc. II, do Dec. 2.181/1997). Por outro lado, verifica-se que a prática teve caráter repetitivo, protraindo-se ao longo do tempo por cerca de dois anos (art. 28, inc. VI, do Dec. 2.181/1997), pelo que se reconhece a agravante. Diante da presença de uma agravante e uma atenuante, entende-se que as mesmas devem ser compensadas, ficando sugerido que a pena-base seja tornada definitiva.

Por fim, entende-se que não é o caso da aplicação de outras penalidades cominadas na Lei 8.078/90.

## CONCLUSÃO

Por conseguinte, considerando estar caracterizada a prática de infração à legislação consumerista, nos termos da Lei Federal nº 8.078/1990, do Decreto Federal nº 2.181/1997, e da Lei Federal 9.784/1999, sugere-se a aplicação de sanção administrativa de multa, no valor de R$ 6.600.000,00 (seis milhões e seiscentos mil reais).

Sugere-se, ainda:

a) A intimação das Representadas para que depositem o valor definitivo da multa em favor do Fundo de Defesa de Direitos Difusos, nos termos da Resolução CFDD nº 30, de 26 de novembro de 2013, consoante determina o art. 29, do Decreto 2.181/1997, sendo o pagamento de total responsabilidade das Representadas. As Representadas são totalmente responsáveis pelo pagamento da multa, devendo comprovar o recolhimento ao DPDC, bem como pelo CNPJ informado nos autos.

b) A expedição de ofício circular aos órgãos e entidades integrantes do Sistema Nacional de Defesa do Consumidor, dando ciência e encaminhando cópia da presente e de seu despacho de homologação.

c) Transcorrido o prazo recursal, e não tendo a empresa se manifestado, remeta-se o processo administrativo à unidade competente desta Secretaria para comprovação do pagamento ou não da multa.

d) Na ausência do pagamento da multa ou de apresentação de recurso, retorne o processo administrativo à Coordenação-Geral de Consultoria Técnica e Sanções Administrativas, para providências quanto o envio dos autos à Procuradoria-Geral da Fazenda Nacional (PGFN) para inscrição em dívida ativa.

e) Nos termos da Portaria nº 8, de 5 abril de 2017, da Secretaria Nacional do Consumidor do Ministério da Justiça e Segurança Pública, que trata do recolhimento da multa aplicada nos processos administrativos que tramitem nessa Secretaria, a Guia de Recolhimento da União (GRU) para pagamento do valor da multa aplicada no âmbito do processo deverá ser expedida pela parte interessada. A parte é responsável pelos dados lançados na GRU, inclusive quando houver impossibilidade de identificação do pagamento por incoerências no seu preenchimento. Para preenchimento da GRU, devera o fornecedor seguir as instruções do Anexo I, dessa portaria. É dever da parte juntar aos autos cópia da GRU no prazo de 5 (cinco) dias a partir do recolhimento, a fim de que seja arquivado o processo. A falta de identificação de pagamento da multa, dentro do prazo de 30 (trinta) dias, ensejará a inscrição do débito em dívida ativa da União.

À consideração superior.

**LEONARDO ALBUQUERQUE MARQUES**
Coordenador-Geral de Consultoria Técnica e Sanções Administrativas

Documento assinado eletronicamente por **Leonardo Albuquerque Marques**, **Coordenador(a)-Geral de Consultoria Técnica e Sanções Administrativas**, em 27/12/2019, às 10:12, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **10626247** e o código CRC **BEDF5BC7**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

**Referência:** Processo nº 08012.000723/2018-19 SEI nº 10626247