LGPDP: O INÍCIO DA VIGÊNCIA DO QUE JÁ VIGIA

Mario Filipe Cavalcanti de Souza Santos

Advogado atuante em Propriedade Intelectual, Privacidade e Proteção de Dados, sócio do escritório Vilela Coelho Propriedade Intelectual (vcpi.com.br) São Paulo/SP, Prêmio Pernambuco de Literatura.
Atende em *mario@vcpi.com.br*

Em 26 de agosto de 2020 tivemos o delineamento para o fim de uma novela que já movimentava (e cansava) inúmeros setores da sociedade civil, do mundo jurídico e do mercado: a vigência da Lei Geral de Proteção de Dados Pessoais brasileira (Lei Federal nº. 13.709/2018).

1. O VAI E VEM DA VIGÊNCIA NO BRASIL

Promulgada desde 14 de agosto de 2018 pelo então Presidente Michel Temer, e publicada um dia depois, a Lei de Dados previa originalmente sua entrada em vigor 18 meses de sua publicação, portanto, em 15 de fevereiro de 2020, mas já em 2018 teve sua vigência alterada para a forma bipartida, pela MP nº. 869/2018 – que foi convertida pelo Congresso na Lei nº. 13.853/2019 –, passando a prever que em 28 de dezembro de 2018 entrariam em vigor os normativos para instalação da Autoridade Nacional de Proteção de Dados (ANPD) e que seus demais artigos, portanto, os aspectos jurídicos (direitos, garantias e deveres), entrariam em vigor 24 meses após sua publicação.

O vai e vem não se encerrou aí, com a sobrevinda da pandemia do SARS-Cov-2 (*Covid* 19), o debate se intensificou, tendo em vista que, de um lado a crise econômica global pedia o contingenciamento de gastos e, de outro lado, a imersão da sociedade global num mundo cada vez mais digital pedia a imediata garantia dos direitos dos consumidores à privacidade e à proteção de seus dados.

Nesse contexto que foi proposta a MP nº. 959/2020 pelo governo federal, que tinha como uma de suas matérias a postergação da *vacatio legis* (o período entre a publicação da lei e sua efetiva vigência) até 03 de maio de 2021, com essa exposição de motivos[1]:

> Esta mesma Medida Provisória também propõe o adiamento da entrada em vigor dos dispositivos previstos na Lei Geral de Proteção de Dados em consequência de uma possível incapacidade de parcela da sociedade em razão dos impactos econômicos e sociais da crise provocada pela pandemia do Coronavírus.

[1] GUEDES, Paulo Roberto Nunes. Ministro de Estado da Economia. Medida Provisória nº. 959/2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Exm/Exm-MP-959-20.pdf. Acesso em: 14/06/2020

Em 07 de agosto de 2020, a MP nº. 959/2020, que tramitava na Câmara, recebeu o Parecer Preliminar do Deputado Federal Damião Feliciano (PDT/PB) Relator, orientando pela entrada em vigor da LGPD imediatamente em 2020, conforme previsão originária. O deputado argumentava que[2]:

> Em tempos de isolamento social, as pessoas estão mais dependentes da internet e interagem por este meio e demais ferramentas associadas para diversos aspectos de seu cotidiano. Ao se utilizar mais serviços digitais, mais dados são gerados e daí a maior necessidade de proteção das informações pessoais.

Ainda observava o deputado relator que na Lei nº. 14.010/2020, cujo PL (1179/2020) foi votado antes da edição da MP nº. 959, o Congresso já havia deixado claro que as sanções administrativas presentes na LGPD só poderiam entrar em vigor em 01 de agosto de 2021, tendo sido tal ditame devidamente sancionado.

Portanto, se as sanções administrativas, que só podem ser implementadas pela ANPD (que ainda não foi instalada), restaram prorrogadas, o que impede que os ditames principiológicos e normativos que reconhecem os direitos dos consumidores e cidadãos à proteção de seus dados e da sua privacidade entre em vigor o quanto antes? Essa foi a questão levantada na Câmara.

Ocorre que, em 25 de agosto de 2020 o plenário da Câmara dos Deputados entendeu por determinar o adiamento da vigência dos "demais artigos" da Lei, portanto, dos seus aspectos principiológicos e normativos, até 31 de dezembro de 2020. Portanto, a LGPD só entraria em vigor em 2021.

Remetida a MP ao Senado da República, em 26 de agosto de 2020 os senadores entenderam por prejudicado o dispositivo que pedia adiamento da vigência dos demais artigos, tendo em vista que a matéria já havia sido votada no Senado anteriormente com definição de prorrogação apenas da vigência dos ditames de sanções administrativas, portanto, com isso, a Lei de Dados entraria em vigor logo que o projeto de lei de conversão fosse sancionado.

2. POR QUE DIZEMOS QUE NÃO HÁ RAZÕES PARA O ADIAMENTO DA VIGÊNCIA DA LGPD?

O vai e vem acima demonstrado, quanto à vigência dos dispositivos principiológicos e normativos da LGPD, travado entre as duas casas do Congresso Nacional e o Executivo federal, não tem nenhuma razão de ser.

Isso porque, a LGPD não é uma legislação que inaugura no Brasil os direitos dos cidadãos à proteção de seus dados pessoais e à sua privacidade, nem que dá ao empresariado e aos controladores de bases de dados responsabilidade objetiva pela violação e o tratamento inadequado desses dados.

---

[2] FELICIANO, Damião. Parecer Preliminar à MP 959/2020 *Apud* CAVALCANTI, Mario Filipe. **LGPD: que entre em vigor!** Portal Intelectual. 07/08/2020. Disponível em: https://www.portalintelectual.com.br/lgpd-que-entre-em-vigor/

A LGPD é um diploma legal aglutinador de uma série de normativos já há muito presentes no ordenamento jurídico brasileiro quanto à matéria, como vamos ver abaixo:

2.1 A Declaração Universal dos Direitos Humanos

É da DUDH que vem o gérmen do reconhecimento da relevância do direito à privacidade, como direito humano e fundamental, no âmbito da contemporaneidade e como um bem *erga omnes*. Eis as disposições:

> Art. III. Todo ser humano tem direito à vida, à liberdade e à segurança pessoal.
>
> Art. XII. ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio e na sua correspondência, nem ataques à sua honra e à sua reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.
>
> Art. XVII. 1. Todo ser humano tem direito à propriedade, só ou em sociedade com outros. 2. Ninguém será arbitrariamente privado de sua propriedade

Vê-se, portanto, que o direito à privacidade, à propriedade e à segurança pessoal, correlatos entre si e inegavelmente conectados à lógica da necessária proteção dos dados pessoais, são elevados ao patamar de direitos supranacionais e de garantias fundamentais exigíveis por qualquer ser humano, tendo em vista que interconectados com o que veio a se chamar de 'princípio da dignidade da pessoa humana'.

2.2 A Convenção Interamericana de Direitos Humanos

Na mesma esteira da DUDH, é inegável precedente à proteção de dados, o texto da Convenção Americana de Direitos Humanos (CADH), estabelecida em 1969 e amplamente conhecida como "Pacto de San José da Costa Rica", promulgada no Brasil pelo Decreto nº. 678/19923, que dispõe em seu art. 11:

> Artigo 11 - Proteção da honra e da dignidade
> 1. Toda pessoa tem direito ao respeito da sua honra e ao reconhecimento de sua dignidade.
> 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.
> 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.

Vê-se que o espírito da norma interamericana recepcionada no Brasil é o mesmo daquele expresso desde 1948 na norma da ONU: garantir o direito à privacidade e à propriedade como intrínsecos à condição de ser humano.

---

[3] BRASIL, Convenção Americana de Direitos Humanos. Decreto nº. 678/1992. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/anexo/and678-92.pdf

2.3 A Constituição Cidadã de 1988

A Constituição da República Federativa do Brasil de 1988, se baseou nos normativos internacionais acima ao eleger como princípio fundamental do próprio Estado Democrático de Direito, a **dignidade da pessoa humana** e como cláusula pétrea, portanto, imutável, dos direitos e garantias fundamentais individuais e coletivos, o **respeito à privacidade**, ao **sigilo dos dados** e à **autodeterminação do indivíduo**, senão vejamos:

> Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:
>
> III - a dignidade da pessoa humana.
> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação
>
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal
>
> LXXII - conceder-se-á habeas data:
>
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
> b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.

Inviolável, pois, a dignidade da pessoa humana e todos os aspectos dela decorrentes, como o **direito à vida privada**, à **intimidade e ao sigilo dos dados** – além de, em última hipótese, as **comunicações de dados**, portanto, a vontade do indivíduo humano sobre seus dados.

2.4 A Lei do Cadastro Positivo – Lei Federal nº. 12.414/2011

Ao sancionar uma Lei que regulasse o cadastro de dados relativos aos pagamentos realizados pelo consumidor, a Presidente Dilma Rousseff promulgou uma legislação que, de um lado permitiu maior garantia aos empresários quanto identificação da tendência de adimplemento dos empréstimos tomados pelos consumidores, mas também garantiu aos consumidores direitos de que seus dados sejam utilizados dentro de uma **finalidade contratada**, não podendo jamais serem

divulgados, repassados, vazados, vendidos, cedidos, transferidos a terceiros, para finalidades não previstas.

Tão firme é o entendimento da legislação no sentido da exclusividade do **tratamento dos dados** no atendimento da **finalidade do cadastro**, que tal dicção está estampada já do primeiro artigo, sendo revisitada pelos arts. 3º e 7º da lei, senão vejamos:

> Art. 1º Esta Lei disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, sem prejuízo do disposto na Lei nº 8.078, de 11 de setembro de 1990 - Código de Proteção e Defesa do Consumidor.
>
> Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei.
>
> Art. 7º As informações disponibilizadas nos bancos de dados somente poderão ser utilizadas para:
> I - realização de análise de risco de crédito do cadastrado
> II - subsidiar a concessão ou extensão de crédito e a realização de venda a prazo ou outras transações comerciais e empresariais que impliquem risco financeiro ao consulente

Clarividente a preocupação do texto legal com a especificação da **finalidade do tratamento dos dados**, bem como com o engessamento de seu tratamento, no esteio da atividade contratada. Temos aqui, então, uma nítida **limitação às atividades do controlador dos dados** e lançados os regramentos que podem ser estendidos para todo e qualquer caso de tratamento de dados de consumidor no Brasil: a vigência e efetivação do **princípio da finalidade**, sendo reconhecido como direito do consumidor ser informados obre a finalidade do tratamento de seus dados, vejamos:

> Art. 5º São direitos do cadastrado:
> V - ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento.
> VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados.

2.5 O Marco Civil da Internet no Brasil – Lei Federal nº. 12.965/2014

No mesmo sentido da legislação acima, três anos depois a Presidente Dilma Rousseff promulgou legislação com o intento de estabelecer "*princípios, garantias, direitos e deveres para o uso da internet*" e é fático que, sob esse desiderato, construiu-se em verdadeira disciplina legislativa da proteção de dados e da privacidade de particulares, sobretudo de consumidores, no país.

É que, ao estabelecer os princípios da disciplina do **uso de redes digitais** no país, aquele diploma legislativo garantiu o seguinte, senão vejamos:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei

Vê-se claramente que a proteção dos dados pessoais e a proteção da privacidade dos indivíduos se tornou, mais do que princípio, ditame normativo expresso muito antes de se falar em LGPD.

Indo mais longe, o Marco Civil estabeleceu como direitos e garantias dos particulares a **inviolabilidade de sua intimidade**, sob pena de indenização pelos danos morais ou patrimoniais decorrentes de sua violação, assim como a **utilização dos dados na finalidade contratada** veja-se:

> 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.
>
> 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:
>
> justifiquem sua coleta;
> não sejam vedadas pela legislação; e
> estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet

Ainda nesse espeque, importante aclarar que a disposição do art. 7º, inciso IX do Marco Civil (MCI) aperfeiçoou a disposição legal do art. 4º da Lei do Cadastro Positivo, para assim dispor, senão vejamos:

> Art. 7º. (...) são assegurados os seguintes direitos:
>
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais

Na Seção II do MCI, intitulada “Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas”, aquele diploma legal assim estabeleceu:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da

> intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> 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.

Portanto, vemos que inegável a força da legislação brasileira, tanto nos ditames da Constituição da República (CRFB), quanto naqueles da Lei do Cadastro Positivo (LCP), como no Marco Civil da Internet (MCI) quanto à proteção dos dados pessoais, o seu tratamento dentro dos limites definidos, a estipulação da finalidade de tratamento de forma clara, devendo o consumidor decidir por anuir ou não de forma consciente, livre e informada, bem como a responsabilização dos controladores dos dados pelo desvirtuamento de todos esses princípios e normativos legais.

2.6 O CDC e a Responsabilidade do Fornecedor de Bens e Serviços pelo Tratamento Adequado dos dados dos consumidores

Como é por todos sabido, no Brasil a Lei Federal nº. 8.078/1990, o Código de Defesa do Consumidor, visa tutelar a relação de consumo e, nesse desiderato, impõe ao fornecedor a necessidade de prestar serviços e fornecer produtos sem falhas ou vícios, sob pena de responsabilização civil, inclusive entendendo como "**serviço defeituoso**" aquele que não garante ao consumidor a segurança que dele poderia ser esperada, vejamos:

> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.
>
> § 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:
> I - o modo de seu fornecimento;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - a época em que foi fornecido

Ora, tal disposição do Código de Defesa do Consumidor brasileiro tutela eficientemente os casos de violação de dados.

Isso porque, inegável que quando os dados dos consumidores são coletados mediante a aquisição de um bem ou a prestação de um serviço, é evidente que tais dados devem ser utilizados tão somente para essa finalidade.

Sobre isso já decidiram os Tribunais pátrios, vejamos:

> RECURSO – Apelação – 'Ação de indenização por danos materiais e morais' – Insurgência contra a r. sentença que julgou parcialmente procedente a

> demanda – Inadmissibilidade – Incontroversa existência de relação jurídica entre as partes – Evidenciada existência de fraude na realização de transações bancárias, em elevados valores, através do sistema de 'internet banking' – Banco apelante que responde não só pela segurança das ferramentas disponibilizadas em ambiente virtual, bem como pelo sigilo das informações pessoais de seus clientes – Apelante que não se desincumbiu de seu ônus probatório, previsto no artigo 373, inciso II, do CPC/2015 – Transações ilegítimas – Casa bancária que responde objetivamente por danos relativos a fraude, nos termos da Súmula 479 do STJ – Valores indevidamente debitados da conta corrente da apelada, que devem ser integralmente restituídos – Sentença mantida – Honorários advocatícios bem fixados e majorados – Recurso improvido
>
> (TJ-SP - AC: 10009777320178260197 SP 1000977-73.2017.8.26.0197, Relator: Roque Antonio Mesquita de Oliveira, 18ª Câmara de Direito Privado, Data de Publicação: 14/03/2019)
>
> APELAÇÃO CÍVEL. RESPONSABILIDADE CIVIL. AÇÃO DE REPARAÇÃO POR DANOS MATERIAIS E MORAIS. FALHA NA PRESTAÇÃO DO SERVIÇO. WEB HOSTING. FALHA NA PRESTAÇÃO DE SERVIÇO. CONFIGURAÇÃO. Hipótese em que o conjunto probatório dos autos conforta a versão do autor, apontando para a ocorrência de falha na prestação de serviços prestados pela ré. Sentença mantida. (...) DANO MORAL. CONFIGURAÇÃO. Caso concreto em que a empresa autora teve sua imagem abalada, em razão da falha na prestação de serviço realizado pela ré, causando lesão à sua reputação e imagem. Caracterizado o dano moral puro, exsurgindo, daí, o dever de indenizar. Sentença mantida. QUANTUM INDENIZATÓRIO. MANUTENÇÃO. (...) Sentença mantida. APELAÇÃO DESPROVIDA
>
> (TJ-RS - AC: 70054358205 RS, Relator: Paulo Roberto Lessa Franz, Décima Câmara Cível, Data de Publicação: Diário da Justiça do dia 18/07/2013)

Deveria, portanto, o empresário inferir que, embora os dados sejam o novo insumo de mercado, se a intensão é a sua utilização para quaisquer finalidades que lhe garanta retorno financeiro, para além dos limites contratados, todos os consumidores titulares desses dados deveriam ser reconhecidos como seus acionistas, a quem deveria esse mesmo empresário remeter a parte que caiba.

Há quebra de confiança, portanto, e defeito na prestação do serviço quando ocorre a **desvirtuação da finalidade contratada**, portanto, quando esses dados são utilizados para outras finalidades, inclusive por terceiros.

2.7 Algumas decisões do STJ, do STF e de alguns Tribunais pátrios

Sobre a matéria, entendemos por relevantes as seguintes decisões das Cortes Maiores do Brasil:

SUPERIOR TRIBUNAL DE JUSTIÇA:

> *"RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL.* ***BANCO DE DADOS. COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE INFORMAÇÃO. VIOLAÇÃO. DANO MORAL IN RE IPSA****. JULGAMENTO: CPC/15.*

(...) 5. ***A gestão do banco de dados impõe a estrita observância das exigências contidas nas respectivas normas de regência – CDC e Lei 12.414/2011*** *– dentre as quais se destaca o dever de informação, que tem como uma de suas vertentes o dever de comunicar por escrito ao consumidor a abertura de cadastro, ficha, registro e dados pessoais e de consumo, quando não solicitada por ele. 6. O consumidor tem o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que lhe são assegurados pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas. 7.* ***A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor – dentre os quais se inclui o dever de informar – faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade****. 8. Em se tratando de compartilhamento das informações do consumidor pelos bancos de dados, prática essa autorizada pela Lei 12.414/2011 em seus arts. 4º, III, e 9º, deve ser observado o disposto no art. 5º, V, da Lei 12.414/2011, o qual prevê o direito do cadastrado ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais 9.* ***O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado****; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais. 10.* ***Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos****. 11. Hipótese em que se configura o dano moral in re ipsa. 12. Em virtude do exame do mérito, por meio do qual foram rejeitadas as teses sustentada pela recorrente, fica prejudicada a análise da divergência jurisprudencial. 13. Recurso especial conhecido em parte e, nessa extensão, desprovido"* (Grifou-se).

(STJ – Resp 1758799/MG, Terceira Turma, Rela. Ministra Nancy Andrighi, DJ: 19/11/2019)

RECURSO ESPECIAL. CONSUMIDOR. CERCEAMENTO DE DEFESA. NÃO OCORRÊNCIA. CONTRATO DE CARTÃO DE CRÉDITO. CLÁUSULAS ABUSIVAS. COMPARTILHAMENTO DE DADOS PESSOAIS. NECESSIDADE DE OPÇÃO POR SUA NEGATIVA. DESRESPEITO AOS PRINCÍPIOS DA TRANSPARÊNCIA E CONFIANÇA. ABRANGÊNCIA DA SENTENÇA. ASTREINTES. RAZOABILIDADE. (...)

3. É abusiva e ilegal cláusula prevista em contrato de prestação de serviços de cartão de crédito, que autoriza o banco contratante a compartilhar dados dos consumidores com outras entidades financeiras, assim como com entidades mantenedoras de cadastros positivos e negativos de consumidores, sem que seja dada opção de discordar daquele compartilhamento.

4. A cláusula posta em contrato de serviço de cartão de crédito que impõe a anuência com o compartilhamento de dados pessoais do consumidor é

> abusiva por deixar de atender a dois princípios importantes da relação de consumo: transparência e confiança.
> 5. A impossibilidade de contratação do serviço de cartão de crédito, sem a opção de negar o compartilhamento dos dados do consumidor, revela exposição que o torna indiscutivelmente vulnerável, de maneira impossível de ser mensurada e projetada.
> 6. De fato, a partir da exposição de seus dados financeiros abre-se possibilidade para intromissões diversas na vida do consumidor. Conhecem-se seus hábitos, monitoram-se a maneira de viver e a forma de efetuar despesas. Por isso, a imprescindibilidade da autorização real e espontânea quanto à exposição.
> 7. Considera-se abusiva a cláusula em destaque também porque a obrigação que ela anuncia se mostra prescindível à execução do serviço contratado, qual seja obtenção de crédito por meio de cartão.
> 8. Não se estende a abusividade, por óbvio, à inscrição do nome e CPF de eventuais devedores em cadastros negativos de consumidores (SPC, SERASA, dentre outros), por inadimplência, uma vez que dita providência encontra amparo em lei (Lei n. 8.078/1990, arts. 43 e 44).
> 11. Recurso especial parcialmente provido
>
> (REsp 1.348.532 – SP, Rel. Min. Luís Felipe Salomão, 4ªT, Dj: 10/10/2017)

SUPREMO TRIBUNAL FEDERAL

Em 06 de maio de 2020, o STF julgou por 10 votos a 1, a confirmação das liminares deferidas em cinco Ações Diretas de Inconstitucionalidade ajuizadas contra a MP nº. 954/2020 promulgada pelo Presidente Jair Bolsonaro que obrigava as empresas privadas de telecomunicações a repassar ao governo federal por meio do IBGE, dados pessoais dos consumidores, sob o argumento de endossar as estatísticas do SARS-Cov-2 (*Cobid* 19).

Contra essa MP foram impetradas Ações Diretas de Inconstitucionalidade por 4 partidos políticos e pelo Conselho Federal da OAB[4], sob o argumento comum de que tal MP, ao obrigar[5]

> as empresas de telefonia fixa e móvel a disponibilizar à Fundação IBGE a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas, viola os dispositivos da Constituição Federal que asseguram a dignidade da pessoa humana, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas e o sigilo dos dados.

O Voto proferido pela Ministra Relatora Rosa Weber, seguido pela esmagadora maioria do plenário do Supremo, é, justamente, de derrubada da MP do Executivo

[4] Partido Social Democracia Brasileira (PSDB) – ADI nº. 6388; Partido Socialista Brasileiro (PSB) – ADI nº. 6389; Partido Socialismo e Liberdade (PSOL) – ADI nº. 6390 e Partido Comunista do Brasil (PCdoB) – ADI nº. 6393, CFOAB – ADI nº. 6387.

[5] SECOM-STF. ***Supremo começa a julgar compartilhamento de dados de usuários de telefonia com o IBGE***. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442823&ori=1. Acesso em 17/06/2020

federal, tendo em vista a sua falta de clareza sobre a finalidade específica, bem domo da amplitude do tratamento desses dados dos consumidores:

> Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a norma não oferece condições para a avaliação da sua adequação e necessidade. Desatende, assim, a garantia do devido processo legal.

Importante frisarmos que em seu Voto, a Exma. Ministra relatora, além de contextualizar a relevância das questões atinentes ao tratamento de dados pessoais, tornou cristalina a proteção que tais dados possuem como matéria constitucional, valorada como preceito fundamental da Carta Política, sendo extremamente relevante o seu cumprimento tanto pelos agentes públicos, quanto pelos privados, vejamos:

> Entendo que as condições em que se dá a manipulação de dados pessoais digitalizados, por agentes públicos ou privados, consiste em um dos maiores desafios contemporâneos do direito à privacidade.
>
> A Constituição da República confere especial proteção à intimidade, à vida privada, à honra e à imagem das pessoas ao qualificá-las como invioláveis, enquanto direitos fundamentais da personalidade, assegurando indenização pelo dano material ou moral decorrente de sua violação (art. 5º, X). O assim chamado direito à privacidade (right to privacy) e os seus consectários direitos à intimidade, à honra e à imagem emanam do reconhecimento de que a personalidade individual merece ser protegida em todas as suas manifestações.
>
> A fim de instrumentalizar tais direitos, a Constituição prevê, no art. 5º, XII, a inviolabilidade do 'sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução penal.

Vê-se, portanto, que o que o Supremo Tribunal Federal decidiu em maio do corrente ano é que a matéria da proteção de dados encontra-se devidamente recepcionada pela própria Constituição da República, desde 1988, por meio da disposição do art. 5º, nos incisos já citados no presente artigo.

TRIBUNAL DE JUSTIÇA DE SÃO PAULO

Sobre a responsabilidade objetiva pelo tratamento inadequado dos dados pessoais e sensíveis do consumidor, o TJSP já havia julgado em 2009:

> "RESPONSABILIDADE CIVIL - Ação de indenização por danos morais - Cerceamento de defesa - Inocorrência - **Ré que repassou dados cadastrais acerca dos rendimentos do autor a terceira estranha e com fins sem qualquer ligação a outra relação de consumo - Abuso do objeto cadastral em detrimento da privacidade do autor -Dano moral in re ipsa** - Quantum que não merece reparo - Correção monetária, por outro lado, que deve incidir a partir da data em que o valor foi arbitrado - Incidência de juros mantida a partir da citação - Encargos da sucumbência Reciprocidade - Inocorrência - Gratuidade processual que não pode ser revogada com base em futura

> indenização - Litigância de má-fé -Inocorrência - Recurso provido em parte". (Grifou-se).
>
> (TJSP - AC: 3.55.607400-0, Relator: De Santi Ribeiro, Órgão julgador: 1ª Câmara de Direito Privado Data de Julgamento: 02/07/2009, Data de Publicação: 18/08/2009)

Veja-se excerto do voto do Relator escrutinando a responsabilidade pelo tratamento inadequado dos dados, ainda que em caso de violação da base:

> "Nessas circunstancias, tem-se que um preposto da ré, valendo-se do acesso às informações cadastrais dos clientes, repassou a terceira estranha e com fins sem qualquer ligação a outra relação de consumo, os rendimentos declarados pelo autor no ato de abertura de crediário junto à ré, em manifesto abuso do objeto cadastral em detrimento da privacidade do autor. É abuso que gera dano moral puro, in re ipsa, que dispensa a comprovação da sua extensão, já que evidenciados pelas circunstancias do fato.".

TRIBUNAL DE JUSTIÇA DO PARANÁ

Sobre a responsabilidade objetiva pelo tratamento inadequado dos dados pessoais e sensíveis do consumidor no caso de repasse desses dados a terceiros sem autorização, o TJPR já havia julgado em 2015:

> RECURSO INOMINADO. AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS E MATERIAIS. REPASSE DE INFORMAÇÕES PESSOAIS E DADOS BANCÁRIOS A OUTRAS EMPRESAS PELA EMPRESA DE TELEFONIA. COBRANÇAS INDEVIDAS REALIZADAS NO CARTÃO DE CRÉDITO DA RECLAMENTE. RESTITUIÇÃO DO INDÉBITO, EM DOBRO, DEVIDA. CONDUTA ABUSIVA. DANO MORAL. QUANTUM INDENIZATÓRIO MANTIDO. RECURSO CONHECIDO E DESPROVIDO.
> 1. In casu ficou demonstrado que após o repasse de dados pessoais e informações bancárias dos consumidores pela empresa de telefonia à corré, sem prévia autorização, a reclamante sofreu cobranças em seu cartão de crédito por serviços não solicitados.
> 2.Nestas condições, diante da conduta abusiva das reclamadas, é devida a repetição do indébito, em dobro, eis que evidente a má-fé e o intuito de obterem lucro indevido em prejuízos dos consumidores, bem como a indenização por danos morais, na medida em que a situação extrapolou a mera cobrança de dívida.
>
> (TJPR, 0002916-31.2014.8.16.0184/0, Mag. Rela. Renata Ribeiro Bau, 3ª TR, Dj: 15/10/2015)

3. NA CONCLUSÃO: A PLENA VIGÊNCIA DOS DITAMES E O DEVER DO EMPRESARIADO

Sobre todo o exposto, vê-se cristalinamente que os ditames de proteção de dados e da privacidade dos consumidores e cidadãos, embora estejam sendo tratados como "coisa nova", nada possuem de novo. Tratam-se de normativos, princípios e

diretivos presentes no ordenamento jurídico brasileiro há anos e que não sustentam a argumentação de desconhecimento do empresariado.

De modo que, as empresas que tratam dados de alguma forma no Brasil já deveriam ter colocado em suas contas de provisionamento os custos com o desenvolvimento de setores e tecnologias digitais de controle há muitos anos, não fazendo qualquer sentido nem os reclamos dos custos de instalação dessas tecnologias com a pandemia, nem o vai e vem dos Poderes Executivo e Legislativo federais.

Estão, pois, vigentes os ditames de proteção de dados e da privacidade e, embora ainda não tenhamos uma ANPD operante, o consumidor pode se valer do Poder Judiciário para ter corrigida qualquer situação de violação de seus dados, inclusive nos moldes como fizemos recentemente no processo nº. 1080233-94.2019.8.26.0100, em trâmite no Foro Central Cível da Comarca de São Paulo, Tribunal de Justiça do Estado de São Paulo, na qual figuro como advogado do consumidor Autor, que teve seus dados violados pela empresa Cyrela, no qual inclusive vige a determinação liminar[6] de que a Ré cesse com a violação perpetrada aos dados dos consumidor, com base em todos os normativos legais já existentes.

Em resumo, não há mais escapatória.

---

[6] VALENTE, Fernanda. ***Juíza multa construtora por compartilhar dados pessoais de cliente***. Consultor Jurídico. Disponível em: https://www.conjur.com.br/2019-ago-23/juiza-impoe-multa-cyrela-repassar-dados-pessoais-cliente; Portal Intelectual: ***Proteção de dados: Cyrela é processada por tratamento inadequado de dados de consumidores e sofre liminar***. Disponível em: https://www.portalintelectual.com.br/protecao-de-dados-cyrela-e-processada-por-tratamento-inadequado-de-dados-de-consumidor-e-sofre-liminar/;
ROSA, Arthur. ***Liminar evita uso de dados de consumidor***. ***Informações foram divulgadas a terceiros por empresa.*** Valor Econômico. Disponível em: https://valor.globo.com/legislacao/noticia/2019/09/29/liminar-evita-uso-de-dados-de-consumidor.ghtml