



PODER JUDICIÁRIO DO ESTADO DE MINAS GERAIS

Justiça de Primeira Instância

Comarca de Belo Horizonte / 29ª Vara Cível da Comarca de Belo Horizonte

PROCESSO Nº: 5064103-55.2019.8.13.0024

CLASSE: [CÍVEL] AÇÃO CIVIL PÚBLICA CÍVEL (65)

ASSUNTO: [Indenização por Dano Moral, Indenização por Dano Moral]

AUTOR: INSTITUTO DEFESA COLETIVA

RÉU/RÉ: FACEBOOK SERVICOS ONLINE DO BRASIL LTDA.

PJE: 5064103-55.2019.8.13.0024

Autor: Instituto Defesa Coletiva

Réu: Facebook Serviços Online do Brasil S/A

Espécie: Ação Civil Pública

COMARCA DE BELO HORIZONTE/ MG

PJE: 5127283-45.2019.8.13.0024

Autor: Instituto Defesa Coletiva

Réu: Facebook Serviços Online do Brasil S/A

Espécie: Ação Civil Pública

COMARCA DE BELO HORIZONTE/ MG**SENTENÇA****I – RELATÓRIO (PJE: 5064103-55.2019.8.13.0024)**

Instituto Defesa Coletiva ajuizou ação civil pública, com pedido de tutela de urgência cautelar, em face de Facebook Serviços Online do Brasil S/A, todos qualificados nos autos, argumentando, em síntese, que em meados do mês de setembro de 2018, a rede social pertencente a empresa ré foi alvo de um ataque, no qual hackers obtiveram acesso às contas de cerca de 29 milhões de pessoas, apropriando-se de detalhes de contato dos usuários, sendo que os hackers conseguiram acessar detalhes de contato, incluindo nome, número de telefone e e-mail de 15 milhões de pessoas, sendo que outras 14 milhões tiveram ainda mais dados acessados, como nome de usuário, gênero, localidade, idioma, status de relacionamento, religião, cidade natal, data de nascimento, dispositivos usados para acessar o Facebook, educação, trabalho e os últimos dez locais onde estiveram ou nos quais foram marcados e, não obstante, meses após o vazamento acima noticiado, um novo vazamento foi divulgado pela empresa de segurança virtual UpGuard, no dia 03 de abril de 2019 e, dessa vez, o vazamento atingiu dados mais sensíveis, expondo senhas de 22 mil contas e detalhes da movimentação de mais de 540 milhões de usuários, restando evidente o interesse comercial das informações vazadas, haja vista que os dados foram encontrados nos servidores de nuvem da empresa Amazon e continham informações de curtidas, comentários, imagens, entre outras interações na rede social (DOC 8), sendo que não foi divulgado precisamente o número de usuários brasileiros que tiveram seus dados,

informações e perfis de comportamento utilizados de forma clandestina pelos hackers, devido a falha na segurança da prestação do serviço da requerida.

Consta que em 14/12/2018 a demandada anunciou um vazamento de fotos que pode ter afetado até 6,8milhões de usuários, conforme site do jornal "Folha de São Paulo" (DOC 09), sendo noticiado que os fatos foram confessados publicamente pela requerida, por meio de um comunicado oficial realizado pelo vice-presidente de gestão de produtos da rede social, Guy Rosen, que confirmou, no dia 12 de outubro de 2018, que dados pessoais de 29 milhões de usuários foram, de fato, roubados por hackers e, no mesmo sentido, o Diretor de Engenharia do Facebook, Tommer Bar afirmou publicamente, em 14 de dezembro de 2018, que aplicativos de terceiros tiveram acesso "mais amplo que o normal" as fotos dos usuários, reconhecendo a própria ré a vulnerabilidade na proteção das informações.

Sustenta que tais fatos configuram vício na qualidade do serviço ofertado pela empresa ré e, por consequência, defeito de prestação de serviço, configurando danos morais coletivos e individuais, em razão da ofensa a direitos da personalidade específicos de cada consumidor.

Arremata requerendo o deferimento pedido de tutela de urgência cautelar e, ao final, a procedência dos pedidos.

O réu apresentou contestação instruída com documentos, na qual argui prefaciais de ilegitimidade ativa e passiva e falta de interesse de agir. No mérito, pugna pela improcedência dos pedidos, alegando, em resumo, que as informações publicadas pela requerido, não constituem confissão para os fins do CPC, mas a notícia de que a empresa demandada imediatamente adotou as medidas para neutralizar o ataque, garantindo a segurança das contas dos usuários, informando-os sobre o ocorrido e notificar as

autoridades legais competentes, não havendo que se falar em defeito de prestação de serviço e, por conseguinte, ausente os danos morais pleiteados. – Id 4982123019 -.

Impugnação à contestação – Id 562282998 -.

As partes apresentaram, respectivamente, seus memoriais, ocasião em que renovaram seus argumentos – Id 9741931258 - e Id 9746419801 -.

O órgão do Ministério Público apresentou manifestação nos autos – Id 8181827998 – e Id 9796238670 -.

Início o relatório da ação civil pública (PJE: 5127283-45.2019.8.13.0024)

ajuizada pelo Instituto Defesa Coletiva em face de Facebook Serviços Online do Brasil Ltda., todos qualificados nos autos, sustentando, em síntese, que conforme as publicações dos principais sites de jornalismo do Brasil (DOC. 06), no dia 13 maio de 2019, o aplicativo de mensagem instantânea WhatsApp, de propriedade da empresa ré, detectou uma vulnerabilidade em seu sistema que permitiu que hackers instalassem de maneira remota um tipo de "spyware" (software espião), para ter acesso a dados do aparelho, em alguns telefones, de forma que a requerida confirmou a referida vulnerabilidade, em comunicado oficial à imprensa, e pediu para os usuários baixarem a última versão do aplicativo e atualizarem o sistema operacional de seus telefones, para eliminar o defeito que permitiu ter acesso a contatos, mensagens e fotos, sendo que os hackers faziam uma ligação através do WhatsApp para o telefone cujos dados queriam acessar e, mesmo que o destinatário não respondesse à chamada, um programa de spyware era instalado nos dispositivos e, em muitos casos, a chamada desaparecia mais tarde do histórico do aparelho, de modo que, se ele não tivesse visto a chamada entrar naquele momento, o usuário afetado não

suspeitaria de nada, devendo ser registrado que o spyware é um software espião de computador, que tem o objetivo de observar e roubar informações pessoais do usuário que utiliza a máquina em que o programa está instalado, retransmitindo-as para uma fonte externa na internet, sem o conhecimento ou consentimento do usuário.

Consta que a demandada, por meio de uma vulnerabilidade na plataforma do aplicativo WhatsApp, deu ensejo a um amplo e grave vazamento de dados dos consumidores, comprometendo sua intimidade, privacidade, segurança física e financeira e, ainda, foi veiculado nos principais sites de notícias brasileiras (DOC. 07) que, no dia 13/08/2019, a empresa requerida teria dado causa a mais uma violação de dados pessoais de seus usuários, envolvendo a transcrição dos áudios enviados pelos consumidores da rede social no aplicativo Messenger, sendo que a agência Bloomberg informou no dia 13.08.2019 que a empresa Facebook pagou funcionários terceirizados para transcrever arquivos de áudio dos usuários do aplicativo Messenger e, a agência afirmou que recebeu a informação de pessoas que foram contratadas para realizar o serviço, mas que precisavam permanecer anônimas para não perder os empregos e, a rede social, por sua vez, confirmou ao G1 – Portal de notícias mantido pela Rede Globo - que estava transcrevendo o áudio dos usuários e disse que abandonou a prática, assim como as empresas Apple e o Google, interromperam a revisão humana de áudios, devendo ser registrado que a transcrição dos áudios de conteúdo particular dos usuários constitui fato tão grave e notório que Secretaria Nacional do Consumidor do Ministério da Justiça e Segurança Pública (Senacon) notificou a empresa requerida, no dia 14.08.2019, para prestar esclarecimentos acerca da violação à intimidade dos usuários. Em nota, a Senacon afirmou que inicia uma nova investigação sobre o Facebook, acerca do tratamento de dados dos consumidores brasileiros.

Sustenta que tais fatos configuram vício na qualidade do serviço ofertado pela empresa ré e, por consequência, defeito de prestação de serviço, configurando danos morais coletivos e individuais, em razão da ofensa a direitos da personalidade específicos de cada consumidor.

Arremata requerendo o deferimento pedido de tutela de urgência cautelar e, ao final, a procedência dos pedidos.

O réu apresentou contestação instruída com documentos, na qual argui prefaciais de ilegitimidade ativa e passiva e falta de interesse de agir. No mérito, pugna pela improcedência dos pedidos, alegando, em resumo, que as informações publicadas pela requerido, não constituem confissão para os fins do CPC, mas a notícia de que a empresa demandada imediatamente adotou as medidas para neutralizar o ataque, garantindo a segurança das contas dos usuários, informando-os sobre o ocorrido e notificar as autoridades legais competentes, não havendo que se falar em defeito de prestação de serviço e, por conseguinte, ausente os danos morais pleiteados. – Id 4982123019 -.

Impugnação à contestação – Id 3682153281 -.

Na audiência de conciliação, esta restou infrutífera – Id 5896528002 -.

As partes apresentaram, respectivamente, seus memoriais, ocasião em que renovaram seus argumentos – Id 9741910846 - e Id 9746444061 -.

O órgão do Ministério Público apresentou manifestação nos autos – Id 4005973082 – e Id 9790350487 -.

Passo ao julgamento simultâneo das ações.

É o relatório. DECIDO.

II - FUNDAMENTAÇÃO

Início o julgamento da ação civil pública (PJE: 5064103-55.2019.8.13.0024) ajuizada pelo Instituto Defesa Coletiva em face do Facebook Serviços Online do Brasil S/A, objetivando a condenação deste no pagamento de indenização por dano moral coletivo e individual, sob o argumento de defeito de prestação de serviço consistente no vazamento de dados sensíveis dos usuários do serviço.

O feito encontra-se devidamente instruído com a prova documental, ao qual, no caso dos autos, é suficiente para o deslinde da causa, não havendo necessidade de produção de provas oral e pericial, impondo-se o julgamento antecipado da lide, nos termos do artigo 355, inciso I, do CPC.

PRELIMINAR

A prefacial de ilegitimidade ativa não merece acolhida, visto que a presente ação busca a proteção de direitos difusos, coletivos e individuais homogêneos, objetivando proteger os interesses da coletividade, protegidos, em princípio, pelo Instituto demandante e, por fim, deve ser

salientado que a presente demanda não se trata de representação processual, mas de substituição processual nos termos do artigo 82, inciso IV, do CDC e artigo 5º, inciso V, da Lei n.º 7.347/85.

A propósito, trago à colação julgado do STJ acerca do tema:

RECURSO ESPECIAL. PROCESSO CIVIL COLETIVO. LEGITIMIDADE ATIVA DAS ASSOCIAÇÕES. ATUAÇÃO COMO REPRESENTANTE E SUBSTITUTA PROCESSUAL. RE n. 573.232/SC. AÇÃO COLETIVA ORDINÁRIA. REPRESENTAÇÃO. NECESSIDADE DE AUTORIZAÇÃO ESPECÍFICA. AÇÃO CIVIL PÚBLICA. DIREITOS INDIVIDUAIS HOMOGÊNEOS. SUBSTITUIÇÃO PROCESSUAL. DESNECESSIDADE DE AUTORIZAÇÃO NOMINAL. TARIFA POR LIQUIDAÇÃO ANTECIPADA. POSSIBILIDADE DA COBRANÇA ATÉ 10/12/2007, COM INFORMAÇÃO EXPRESSA. VERIFICAÇÃO EM LIQUIDAÇÃO. (...) Na presente demanda, a atuação da entidade autora deu-se, de forma inequívoca, no campo da substituição processual, sendo desnecessária a apresentação nominal do rol de seus filiados para ajuizamento da ação. 8. Nesses termos, tem-se que as associações instituídas na forma do art. 82, IV, do CDC estão legitimadas para propositura de ação civil pública em defesa de interesses individuais homogêneos, não necessitando para tanto de autorização dos associados. Por se tratar do regime de substituição processual, a autorização para a defesa do interesse coletivo em sentido amplo é estabelecida na definição dos objetivos institucionais, no próprio ato de criação da associação, não sendo necessária nova autorização ou deliberação assemblear. (...) (STJ - REsp: 1325857 RS 2011/0236589-7, Relator: Ministro LUIS FELIPE SALOMÃO, Data de Julgamento: 30/11/2021, S2 - SEGUNDA SEÇÃO, Data de Publicação: DJe 01/02/2022).

Rejeito a preliminar.

A prefacial de ilegitimidade passiva não merece abrigo, uma vez que se extrai da causa de pedir a assertiva do autor no sentido de que o réu teria vazado dados pessoais de vários usuários do serviço fornecido por ele e, por conseguinte, configurado defeito de prestação de serviço, de forma que tal aspecto é o qual para a caracterização da legitimidade passiva. (REsp 1893387/SP, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 22/06/2021, DJe 30/06/2021).

Além disso, conforme já mencionado pelo órgão do Ministério Público - Id 8181827998 - *sabe-se que o réu pertence à empresa norte-americana Facebook, Inc., que também adquiriu a empresa WhatsApp, sendo que todas pertencem ao mesmo grupo econômico Facebook, restando nítida a relação jurídica entre elas.*

Por fim, deve ser observado o disposto no artigo 11, § 2º da Lei nº 12.965/2014:

“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.”

Rejeito a preliminar.

A prefacial de falta de interesse de agir não merece acolhida, uma vez que presente o binômio necessidade/adequação, o que se vê, sobretudo, após a formação da fase postulatória com a apresentação da contestação instruída com documentos.

MÉRITO

A relação jurídica estabelecida entre o Facebook Serviços Online do Brasil S/A e os seus usuários se encontra sob a égide do Código de Defesa do Consumidor, tendo em vista ao cumprimento dos requisitos dos artigos 2º e 3º, § 2º, todos do mesmo diploma legal.

O artigo 6º, inciso III, do Código de Defesa do Consumidor estabelece que:

"Art. 6º - São direitos básicos do consumidor:

I - a proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecido de produtos e serviços considerados perigosos e nocivos;

(...)

III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, **bem como sobre os riscos que apresentem;**" (grifo nosso).

Os artigos 14 e 37, ambos do Estatuto do Consumidor, reforçam ao fornecedor do serviço o dever de prestar informações seguras, claras e adequadas sobre o serviço ao consumidor, senão 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 de serviços, *bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.*" (grifo nosso).

A evolução da sociedade e o desenvolvimento da tecnologia, deflagra uma nova era da sociedade, denominada era das informações e compartilhamento de dados.

A Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados) regula a proteção de dados pessoais em âmbito nacional, buscando harmonizar a garantia da autodeterminação informativa (privacidade/contrato) e o reconhecimento da necessidade do tratamento desses dados pelo Poder Público e, também, pelo setor privado, ante a importância da circulação de dados no mercado.

Portanto, a Lei Geral de Proteção de Dados surge em um ambiente de evolução tecnológica e de manuseio de dados pessoais na condição de mercadoria, de forma que a observância aos direitos do titular de dados pessoais assume fundamental importância, exigindo o cumprimento do dever de protegê-lo e de informá-lo acerca de maneira (como), quando e em que condições serão utilizados, buscando possibilitar ao cidadão a segurança de que seus dados serão protegidos antes, durante e, após, o encerramento do tratamento.

Com efeito, antes mesmo da lei supracitada, embora não com o status de regulamentação a proteção de dados, a Constituição da República de 1988 fundamentalmente em seu artigo 5º, incisos X e XII instituía a tutela da dignidade da pessoa humana e a garantia dos direitos fundamentais (intimidade da vida privada, inviolabilidade do sigilo de correspondência e das comunicações e das comunicações telegráficas, de dados e telefônicas), apresentando a base para proteção de dados e, ainda, deve ser pontuado que já havia legislação que trata-se do assunto, como o Código de Defesa do Consumidor (Lei n.º 8.078/90), o Marco Civil da Internet (Lei n.º 12.965/2014), a Lei do Cadastro Positivo (Lei n.º 12.414/2011), o Decreto do Comércio Eletrônico (Decreto n.º 7.962/2013) e a Lei de Acesso à Informação (Lei n.º 12.527/2011).

Por fim, consigno que a LGPD - Lei Geral de Proteção de Dados - mantém relação estreita com Código de Proteção e Defesa do Consumidor, visto que o artigo 2º da Lei n.º 13.709/2018 alcança a defesa dos consumidores, pois a proteção dos seus dados pessoais vincula-se a sua vulnerabilidade.

Pois bem.

O caderno probatório formado nos autos revela o defeito de prestação de serviço fornecido pelo demandado aos consumidores, consistente no vazamento de dados ocorrido em setembro de 2018 – ataque por *hackers* e *acesso indevido de aplicativo de terceiros às fotos dos usuários publicadas nos "stories e as fotos carregadas* -, o que demonstra a violação desarrazoada da segurança do serviço fornecido, descumprindo o artigo 6º, incisos I e III, do CDC e artigo 6º, inciso VII e VIII, da Lei n.º 13.709/2018.

Revela consignar que, o vazamento de dados acima registrado - ataque por *hackers* e acesso indevido de aplicativo de terceiros às fotos dos usuários publicadas nos *"stories e as fotos carregadas"*, foi intensamente divulgado pela mídia - Id 68747162 e Id 68747160 - e, ainda, corroborado pelo próprio demandado em sua peça de defesa que, não nega a presença de vulnerabilidade do sistema que possibilitou a ocorrência do ataque dos *hackers* e o acesso indevido às fotos dos usuários por aplicativos de terceiros, "o Ataque envolveu a exploração não autorizada e maliciosa do sistema da empresa", que "permitiu que os invasores roubassem tokens de acesso ao Facebook, que poderiam usar para acessar contas de usuários" (ID 4982123019).

Tal evento foi corroborado em nota pública divulgada pela empresa requerida, em setembro de 2018, momento em que se registrou o seguinte: "invasores exploraram uma vulnerabilidade no código do Facebook que impactou a funcionalidade "Ver Como"", o que "permitiu que eles roubassem tokens de acesso ao Facebook, os quais usaram para entrar nas contas das pessoas", afetando "cerca de 90 milhões de pessoas no mundo" (Id 68747152).

Posteriormente, em nota pública relativa ao vazamento de dados, publicada em dezembro de 2018, a demandada informou o seguinte: "normalmente, o Facebook compartilha fotos que você publicou em sua linha do tempo com esses aplicativos. No entanto, ocorreu um erro entre 13 e 25 de setembro de 2018, em que os desenvolvedores tiveram acesso a outras fotos, como as que você pode ter publicado no Facebook Stories ou apenas carregado, sem publicar." (Id 68747156).

Neste sentido, entendo que as provas produzidas nos autos demonstram, de forma consistente, o defeito de prestação de serviço fornecido pelo réu, não havendo que se falar em imprevisibilidade/inevitabilidade, visto que o evento acima analisado configura fortuito interno inerente ao risco do empreendimento desenvolvido pela requerida.

Cumpra registrar que a ocorrência de tal episódio era previsível em se tratando deste tipo de atividade e, mesmo diante da qualidade e de mecanismos de segurança que o réu deve oferecer, tal constatação não afasta a conclusão de que o sistema é vulnerável. E a falha desse sistema deve ser atribuída a quem dele usufrui como fonte de lucro. É o chamado risco da atividade, não havendo que se falar em culpa exclusiva de terceiro.

Nota-se que a demandada não nega que usuários brasileiros foram atingidos pelos vazamentos de dados, conquanto não tenha informada a quantidade de pessoas atingidas no Brasil, o que não obsta de se visualizar o potencial do dano, diante do elevado número de usuário do Facebook no Brasil, de forma que tal evento viola o direito de personalidade das pessoas/consumidores que utilizavam o serviço fornecido pela demandada.

O dano moral coletivo é categoria autônoma de dano e se caracteriza por lesão grave, injusta e intolerável a valores e a interesses fundamentais da sociedade, independentemente da comprovação de prejuízos concretos ou de efetivo abalo moral.

A propósito, acerca do tema trago à colação magistério do Professor Bittar Filho, Carlos Alberto, senão vejamos:

“Nesse sentido, no plano semântico, pode-se afirmar que “o dano moral coletivo caracteriza-se como a injusta lesão da esfera moral de uma dada comunidade, ou seja, é a violação antijurídica de um determinado círculo de valores coletivos. Assim, quando se fala em dano moral coletivo, está-se fazendo menção ao fato de que o patrimônio valorativo de uma certa comunidade (maior ou menor), idealmente considerado, foi agredido de maneira absolutamente injustificável do ponto de vista jurídico: quer isso

dizer, em última instância, que se feriu a própria cultura, em seu aspecto imaterial". (Do dano moral coletivo no atual contexto jurídico brasileiro. Revista de Direito do Consumidor, São Paulo, n. 12, p. 44-62, out./dez. 1994).

Revela consignar que o dano moral coletivo não representa uma mera soma de danos morais individuais, visto que o dano moral individual é eminentemente subjetivo, exigindo para sua configuração, a constatação do dano, lesão, angústia, dor, humilhação ou sofrimento pessoal do lesado, enquanto, o dano moral coletivo, conforme já fixou o Superior Tribunal de Justiça: "(...) é aferível in re ipsa, ou seja, sua configuração decorre da mera constatação da prática de conduta ilícita que, de maneira injusta e intolerável, viole direitos de conteúdo extrapatrimonial da coletividade, revelando-se despicienda a demonstração de prejuízos concretos ou de efetivo abalo moral. Precedentes. Independentemente do número de pessoas concretamente atingidas pela lesão em certo período, o dano moral coletivo deve ser ignóbil e significativo, afetando de forma inescusável e intolerável os valores e interesses coletivos fundamentais". (STJ - REsp: 1610821 RJ 2014/0019900-5, Relator: Ministro LUIS FELIPE SALOMÃO, Data de Julgamento: 15/12/2020, T4 - QUARTA TURMA, Data de Publicação: DJe 26/02/2021).

Neste contexto, no intuito de demonstrar o dano moral a uma coletividade, é importante que se aponte apenas a ocorrência de uma conduta empresarial violadora do ordenamento jurídico e, bem assim que o fato transgressor seja de razoável significância e ultrapasse os limites da tolerabilidade, causando sensação de frustração e impotência, ou mesmo revolta, no universo de indivíduos expostos às consequências da conduta antijurídica praticada.

No caso vertente, entendo que restou demonstrado o dano coletivo, conforme já pontuado acima, atento aos inúmeros transtornos causados à coletividade diante do defeito de prestação de serviço representado pelo

vazamento de dados pessoais de usuários brasileiros, configurada infração à confiança usuários do serviço.

Afora isso, registro que, em virtude de tais eventos, o réu sofreu punição no âmbito administrativo momento em que o SENACON – Secretaria Nacional do Ministério da Justiça e Segurança Pública - aplicou multa à empresa em questão no importe de R\$ 6.6000.000,00 (seis milhões de reais) – Id 4701048121 -, Id 4701048126 -, e Id 9671195981 -.

Por fim, atento à circunstância de que o requerido representa um conglomerado estadunidense de tecnologia, considerada uma das cinco grandes da tecnologia e uma das empresas mais valiosas do mundo, alcançando capitalização de mercado de mais de USD 450 (quatrocentos e cinquenta) bilhões de dólares, conforme informações obtidas no endereço eletrônico: <https://www.google.com/finance/quote/M1TA34:BVMF> (<https://www.google.com/finance/quote/M1TA34:BVMF>), entendo como razoável a quantificação do valor do dano moral coletivo no importe de R\$ 10.000.000,00 (dez milhões de reais), o qual deverá ser atualizado com base na tabela da Corregedoria de Justiça do Poder Judiciário deste Estado, a partir da data desta sentença, acrescida de juros de mora de 1,0% ao mês desde a citação, ficando consignado que a referida quantia será revertida ao Fundo Estadual de Proteção e Defesa do Consumido – FEPDC/MG -, nos termos do artigo 13 da Lei n.º 7.347/85.

No que pertine aos danos morais individuais relativos aos usuários diretamente atingidos pelo vazamento de dados, atento ao exame dos fundamentos acima, bem como a situação fática analisada nos autos, entendo que deve ser fixado em R\$ 5.000,00 (cinco mil reais), o qual deverá ser atualizado com base na tabela da Corregedoria de Justiça deste Estado a partir da data desta sentença, acrescida de juros de mora de 1,0% desde a data da citação.

Saliento que o cumprimento individual da sentença em relação aos danos morais, deverá ocorrer na residência de cada consumidor afetado, o qual deverá demonstrar que se adequava à condição de usuário do serviço (Facebook) à época dos fatos com vazamento dos seus dados.

Em relação ao pedido cominatório para que a requerida seja compelida a se abster de fornecer dados dos consumidores brasileiros, sem a devida autorização, conforme já mencionado pelo órgão do Ministério Público - Id 9796238670 -, não merece prosperar.

É que em nenhum dos eventos objetos desta lide, houve fornecimento espontâneo pela ré de dados pessoais sigilosos de usuários, mas sim, ocorreram vazamentos de dados causados por ataques ilícitos de terceiros e compartilhamento indevido de fotos com aplicativos de terceiros devido a uma anomalia do sistema.

Logo, a obrigação de se abster de fornecer dados pessoais dos usuários, sem a devida autorização ou ordem judicial, já faz parte da política de privacidade da requerida e decorre de imposição legal (Lei Geral de Proteção de Dados Pessoais - LGPD, nº 13.709/18 e Lei 12.965/14, conhecida como Marco Civil da Internet).

Igualmente, no caso concreto, não merece abrigo o pleito de condenação do réu a veicular campanha de segurança sobre os mecanismos de proteção dos dados dos consumidores, uma vez que além envolver pedido genérico, as informações e configurações de segurança podem ser acessadas por todos os consumidores na própria rede social Facebook.

No que tange a ação civil pública (PJE: 5127283-45.2019.8.13.0024) o Instituto Defesa Coletiva Réu ajuizou a referida ação em face do Facebook Serviços Online do Brasil S/A, sob o argumento, em síntese, de teria ocorrido defeito de prestação de serviço fornecido pelo réu referente à vulnerabilidade no aplicativo WhatsApp que permitiu que *hackers* instalassem de maneira remota um *software* espião ("spyware") para ter acesso a dados de telefones celulares de usuários.

Seguindo a mesma linha de raciocínio acima articulado, observa-se que tal fato foi amplamente divulgado pela mídia (Id 81305400) e, confirmado pelo réu por meio nota pública veiculada à época dos fatos (Id 7037153020) e, também, pelo conteúdo de sua peça de defesa, instante em que, se constata, que o requerido não nega a ocorrência do ataque praticado por *hackers*.

Ora, tal circunstância demonstra a violação desarrazoada da segurança do serviço fornecido réu, descumprindo o artigo 6º, incisos I e III, do CDC e artigo 6º, inciso VII e VIII, da Lei n.º 13.709/2018.

Assim, entendo que as provas produzidas nos autos demonstram, de forma consistente, o defeito de prestação de serviço fornecido pelo réu, não havendo que se falar em imprevisibilidade/inevitabilidade, visto que o evento acima analisado configura fortuito interno inerente ao risco do empreendimento desenvolvido pela requerida.

Cumprir registrar que a ocorrência de tal episódio era previsível em se tratando deste tipo de atividade e, mesmo diante da qualidade e de mecanismos de segurança que o réu deve oferecer, tal constatação não afasta a conclusão de que o sistema é vulnerável. E a falha desse sistema deve ser atribuída a quem dele usufrui como fonte de lucro. É o chamado risco da atividade, não havendo que se falar em culpa exclusiva de terceiro.

Dessa forma, penso que restou provado que em virtude do ataque por *hackers* restou demonstrado o dano, visto que acabou ocorrendo violação ao sigilo de dados pessoais de vários usuários brasileiros, configurando descumprimento aos direitos à privacidade, intimidade, honra e imagem, consoante previstos no artigo 5º, inciso X, da Constituição da República de 1988.

De outro lado, saliento que, conquanto o demandado afirme que apenas um brasileiro teria sido vítima do ataque, inexistente prova neste sentido e, conforme visto acima, a empresa ré confirma em sua contestação e nota pública que, o ataque atingiu vários usuários também no Brasil, devendo ser pontuado que o número estimado de usuários do WhatsApp no Brasil é estimado em cerca de 147 milhões de pessoas, ficando abaixo em quantidade de usuários do mundo para a Índia, conforme ressalta o órgão do Ministério Público – Id 9790350487 -.

O dano moral coletivo é categoria autônoma de dano e se caracteriza por lesão grave, injusta e intolerável a valores e a interesses fundamentais da sociedade, independentemente da comprovação de prejuízos concretos ou de efetivo abalo moral.

A propósito, acerca do tema trago à colação magistério do Professor Bittar Filho, Carlos Alberto, senão vejamos:

“Nesse sentido, no plano semântico, pode-se afirmar que “o dano moral coletivo caracteriza-se como a injusta lesão da esfera moral de uma dada comunidade, ou seja, é a violação antijurídica de um determinado círculo de valores coletivos. Assim, quando se fala em dano moral coletivo, está-se fazendo menção ao fato de que o patrimônio valorativo de uma certa comunidade (maior ou menor), idealmente considerado, foi agredido de maneira absolutamente injustificável do ponto de vista jurídico: quer isso dizer, em última instância, que se feriu a própria cultura, em seu aspecto

imaterial". (Do dano moral coletivo no atual contexto jurídico brasileiro. Revista de Direito do Consumidor, São Paulo, n. 12, p. 44-62, out./dez. 1994).

Revela consignar que o dano moral coletivo não representa uma mera soma de danos morais individuais, visto que o dano moral individual é eminentemente subjetivo, exigindo para sua configuração, a constatação do dano, lesão, angústia, dor, humilhação ou sofrimento pessoal do lesado, enquanto, o dano moral coletivo, conforme já fixou o Superior Tribunal de Justiça: "(...) é aferível in re ipsa, ou seja, sua configuração decorre da mera constatação da prática de conduta ilícita que, de maneira injusta e intolerável, viole direitos de conteúdo extrapatrimonial da coletividade, revelando-se despicienda a demonstração de prejuízos concretos ou de efetivo abalo moral. Precedentes. Independentemente do número de pessoas concretamente atingidas pela lesão em certo período, o dano moral coletivo deve ser ignóbil e significativo, afetando de forma inescusável e intolerável os valores e interesses coletivos fundamentais". (STJ - REsp: 1610821 RJ 2014/0019900-5, Relator: Ministro LUIS FELIPE SALOMÃO, Data de Julgamento: 15/12/2020, T4 - QUARTA TURMA, Data de Publicação: DJe 26/02/2021).

Neste contexto, no intuito de demonstrar o dano moral a uma coletividade, é importante que se aponte apenas a ocorrência de uma conduta empresarial violadora do ordenamento jurídico e, bem assim que o fato transgressor seja de razoável significância e ultrapasse os limites da tolerabilidade, causando sensação de frustração e impotência, ou mesmo revolta, no universo de indivíduos expostos às consequências da conduta antijurídica praticada.

No caso vertente, entendo que restou demonstrado o dano coletivo, conforme já pontuado acima, atento aos inúmeros transtornos causados à coletividade diante do defeito de prestação de serviço representado pelo vazamento de dados pessoais de usuários brasileiros, configurada infração à confiança usuários do serviço.

Afora isso, registro que, em virtude de tais eventos, o réu sofreu punição no âmbito administrativo momento em que o SENACON – Secretaria Nacional do Ministério da Justiça e Segurança Pública - aplicou multa à empresa em questão no importe de R\$ 6.6000.000,00 (seis milhões de reais) – Id 9671129425 -.

Por fim, atento à circunstância de que o requerido representa um conglomerado estadunidense de tecnologia, considerada uma das cinco grandes da tecnologia e uma das empresas mais valiosas do mundo, alcançando capitalização de mercado de mais de USD 450 (quatrocentos e cinquenta) bilhões de dólares, conforme informações obtidas no endereço eletrônico: <https://www.google.com/finance/quote/M1TA34:BVMF> (<https://www.google.com/finance/quote/M1TA34:BVMF>), entendo como razoável a quantificação do valor do dano moral coletivo no importe de R\$ 10.000.000,00 (dez milhões de reais), o qual deverá ser atualizado com base na tabela da Corregedoria de Justiça do Poder Judiciário deste Estado, a partir da data desta sentença, acrescida de juros de mora de 1,0% ao mês desde a citação, ficando consignado que a referida quantia será revertida ao Fundo Estadual de Proteção e Defesa do Consumido – FEPDC/MG -, nos termos do artigo 13 da Lei n.º 7.347/85.

No que pertine aos danos morais individuais relativos aos usuários diretamente atingidos pelo vazamento de dados, atento ao exame dos fundamentos acima, bem como a situação fática analisada nos autos, entendo que deve ser fixado em R\$ 5.000,00 (cinco mil reais), o qual deverá ser atualizado com base na tabela da Corregedoria de Justiça deste Estado a partir da data desta sentença, acrescida de juros de mora de 1,0% desde a data da citação.

Saliento que o cumprimento individual da sentença em relação aos danos morais, deverá ocorrer na residência de cada consumidor afetado, o qual deverá demonstrar que se adequava à condição de usuário do serviço (Facebook) à época dos fatos com vazamento dos seus dados.

Em relação ao pedido cominatório para que o requerido seja compelido a desenvolver um mecanismo de reinstalação automática do aplicativo WhatsApp para todos os usuários, não merece prosperar, visto que é necessária a anuência dos consumidores/usuários do serviço, já que estes têm o direito de optar por outro aplicativo e versão, devendo ser preservado o princípio da autodeterminação informativa do consumidor, previsto no artigo 2º, inciso II, da Lei n.º 13.709/2018.

Igualmente, no caso concreto, não merece abrigo o pleito de condenação do réu a veicular campanha de segurança sobre os mecanismos de proteção dos dados dos consumidores, uma vez que além envolver pedido genérico, as informações e configurações de segurança podem ser acessadas por todos os consumidores na própria rede social Facebook.

III - DISPOSITIVO

Isso posto, em relação a ação civil pública (PJE: 5064103-55.2019.8.13.0024), julgo *parcialmente procedentes os pedidos*, para:

1 – condenar o réu, a título de dano coletivo, a pagar o valor de R\$ 10.000.000,00 (dez milhões de reais), o qual deverá ser atualizado com base na tabela da Corregedoria de Justiça do Poder Judiciário deste Estado, a partir da data desta sentença, acrescida de juros de mora de 1,0% ao mês

desde a citação, ficando consignado que a referida quantia será revertida ao Fundo Estadual de Proteção e Defesa do Consumido – FEPDC/MG -, nos termos do artigo 13 da Lei n.º 7.347/85;

2 – condenar o réu, a título de danos individuais relativos aos usuários diretamente atingidos pelo vazamento de dados, a pagar o valor de R\$ 5.000,00 (cinco mil reais), o qual deverá ser atualizado com base na tabela da Corregedoria de Justiça deste Estado a partir da data desta sentença, acrescida de juros de mora de 1,0% desde a data da citação;

2.2 - saliento que o cumprimento individual da sentença em relação aos danos morais, deverá ocorrer na residência de cada consumidor afetado, o qual deverá demonstrar que se adequava à condição de usuário do serviço (Facebook) à época dos fatos com vazamento dos seus dados;

3 – julgar *improcedentes* os pedidos cominatórios contidos na alínea “E” e “G”.

Sem custas por força do disposto no artigo 87 do CDC e art. 18 da Lei da ACP, observando-se o princípio da simetria.

No que tange a ação civil pública (PJE: 5127283-45.2019.8.13.0024)_julgo *parcialmente procedentes os pedidos*, para:

1 - condenar o réu, a título de dano coletivo, a pagar o valor de R\$ 10.000.000,00 (dez milhões de reais), o qual deverá ser atualizado com base na tabela da Corregedoria de Justiça do Poder Judiciário deste Estado, a partir da data desta sentença, acrescida de juros de mora de 1,0% ao mês desde a citação, ficando consignado que a referida quantia será revertida ao Fundo Estadual de Proteção e Defesa do Consumido – FEPDC/MG -, nos termos do artigo 13 da Lei n.º 7.347/85;

2 - condenar o réu, a título de danos individuais relativos aos usuários diretamente atingidos pelo vazamento de dados em virtude da ação do *hackers*, a pagar o valor de R\$ 5.000,00 (cinco mil reais), o qual deverá ser atualizado com base na tabela da Corregedoria de Justiça deste Estado a partir da data desta sentença, acrescida de juros de mora de 1,0% desde a data da citação;

2.2 - saliento que o cumprimento individual da sentença em relação aos danos morais, deverá ocorrer na residência de cada consumidor afetado, o qual deverá demonstrar que se adequava à condição de usuário do serviço (Facebook) à época dos fatos com vazamento dos seus dados;

3 - julgar *improcedentes* os pedidos cominatórios contidos na alínea “F” e “G”.

Sem custas por força do disposto no artigo 87 do CDC e art. 18 da Lei da ACP, observando-se o princípio da simetria.

Publique-se.

Registre-se.

Intimem-se.

Belo Horizonte, data da assinatura eletrônica.

JOSE MAURICIO CANTARINO VILLELA

Juiz(íza) de Direito

29ª Vara Cível da Comarca de Belo Horizonte

Avenida Raja Gabaglia, 1753, Luxemburgo, Belo Horizonte - MG - CEP: 30380-900

Assinado eletronicamente por: JOSE MAURICIO CANTARINO VILLELA

24/07/2023 12:58:21

[https://pje-consulta-](https://pje-consulta-publica.tjmg.jus.br:443/pje/Processo/ConsultaDocumento/listView.seam)

[publica.tjmg.jus.br:443/pje/Processo/ConsultaDocumento/listView.seam](https://pje-consulta-publica.tjmg.jus.br:443/pje/Processo/ConsultaDocumento/listView.seam)

ID do documento: 9872707655



23072412582079900009868795824

IMPRIMIR

GERAR PDF