REVISTA DA ESCOLA SUPERIOR DA ADVOCACIA DE RONDÔNIA – ESA/RO
DESTEMIDOS PIONEIROS - ISSN 2594-9306

REPARAÇÃO CIVIL E LGPD: O VAZAMENTO DE DADOS PESSOAIS SIGILOSOS E O CASO KLARA CASTANHO

CÉSAR AUGUSTO WANDERLEY OLIVEIRA
cesarwanderley@gmail.com
Mestre em Geografia. Pós-graduado em Direito Processual Civil

RESUMO: O presente artigo tem como objetivo a análise do recente caso vivido por uma atriz brasileira que teve dados pessoais sensíveis expostos sob o ponto de vista do Direito Civil e os pressupostos para a reparação do dano sofrido junto da abordagem do caso em relação às normas da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) além do papel da Autoridade Nacional de Proteção de Dados - ANPD, quanto a fiscalização de incidentes desta natureza.

PALAVRAS-CHAVE: Dados pessoais, LGPD, indenização, incidente de segurança.

1 INTRODUÇÃO

A atriz Klara Forkas Gonçalez Castanho revelou, em junho de 2022, ter engravidado após abuso sexual, só descobrindo a gestação no fim, optando mediante processo judicial a entrega da criança à doação, baseada no artigo 19-A do Estatuto da Criança e do Adolescente (BRASIL, 1990). O parto ocorreu no Hospital Brasil, da Rede D'or, ocorre que as informações sigilosas de seu prontuário foram “vazadas” e por cerca de duas horas ficaram disponíveis expondo um *print* com a data do parto, sexo do bebê, o nome do hospital e da atriz. Depois da repercussão negativa, o site retirou o conteúdo do ar.

Dessa forma, o presente artigo tem como objetivo a análise deste recente caso, sob o ponto de vista do Direito Civil e os pressupostos para a reparação do dano sofrido junto da abordagem do caso em relação às normas da Lei 13.709/2018 denominada Lei Geral de Proteção de Dados Pessoais – LGPD (BRASIL, 2018) além do papel da Autoridade Nacional de Proteção de Dados - ANPD, quanto a fiscalização de incidentes desta natureza.

Antes de adentrar o tema são necessárias duas observações.

A primeira é minha manifestação de apoio à atriz. É inegável que a lei assiste à gestante o direito de não exercer a maternidade e, tendo sido ou não vítima de estupro, o sigilo do processo é medida não só assegurada, mas também imprescindível para a

proteção dos envolvidos nesse rito tão traumático. Não há espaço em uma sociedade democrática de Direito para a estigmação da mulher, ainda quando a concepção ocorreu de maneira consentida, quem dirá quando foi fruto de uma violência. Ainda que o objeto do presente artigo seja a análise jurídica objetiva do caso exposto, é impossível deixar de externar minha solidariedade e meu desejo que, dentro das proporções possíveis, esse evento possa ser superado e utilizado como referência para que todos os envolvidos que falharam na proteção da paciente vulnerável possam adotar medidas rígidas para evitar, ou ao menos mitigar, a repetição desses eventos.

A segunda é a temporalidade dos fatos. As considerações tomaram como referência apenas as informações disponíveis até 25 de junho do ano vigente, momento da última revisão, portanto, dependendo da época da leitura, várias questões aqui tratadas podem ter sofrido mudanças.

2 DA PROTEÇÃO DOS DADOS PESSOAIS

Muito antes do Brasil positivar em lei específica a necessidade preeminente da proteção de dados pessoais o artigo 5º, inciso X, da CRFB, já asseverava: “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” (BRASIL, 1988). A importância do tema requeria há muito tempo a elevação dessa proteção que recentemente foi incorporada à nossa lei maior por ocasião da Emenda Constitucional nº 115, de 10 de fevereiro de 2022, que alterou a CF/88 para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais, modificação mais relevante consistiu na inserção no art. 5º o inciso LXXIX, que expõe ser “assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”.

A modificação constitucional harmoniza-se com a tardia regulamentação da proteção de dados no território nacional que vem sendo construída desde 2010, quando se iniciou a consulta pública do Ministério da Justiça sobre o anteprojeto de lei de proteção de dados pessoais, passou pela sanção em 2011 da Lei nº 12.527/2011 de Acesso à Informação (BRASIL, 2011), em 2012 com a Lei nº 12.737/ 2012, Carolina Dieckmann (BRASIL, 2012) que trouxe a tipificação de crimes cibernéticos como

compartilhar dados pessoais sem autorização, em 2014 com a entrada em vigor do Marco Civil da Internet, Lei nº 12.965/2014 (BRASIL, 2014), em 2016 com a aprovação do Regulamento Geral sobre Proteção de Dados (GDPR, na sigla em inglês) para só em 2018 ocorrer, efetivamente, a promulgação da Lei n. 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais – LGPD (BRASIL, 2018) com *vacacio* de 2 (dois) anos, entrando em vigor grande parte apenas em 18 de setembro de 2020 por força da MP 959/2020 (PLV 34/2020).

Ressaltando que a promulgação ocorreu em 2018 com um ambiente ainda aquecido pelo escândalo do Facebook e a *Cambridde Analytica* ocorrido em março e a entrada em vigor em maio do GDPR na Europa.

O vazamento de dados não é novidade, no mês de novembro de 2020, o Superior Tribunal de Justiça foi vítima de um enorme ataque cibernético considerado o maior já ocorrido no Brasil. A invasão interrompeu o acesso aos seus sistemas, implicou o cancelamento dos julgamentos e a Corte se viu sob o risco de uma inestimável perda de dados[1].

Na área da saúde não é diferente, o Hospital Albert Einstein em novembro de 2020, de acordo com notícias divulgadas, foi responsável pela exposição de dados sensíveis de cerca 16 milhões de pessoas por 1 (um) mês[2], supostamente por um funcionário do hospital que trabalhava em um projeto com o Ministério da Saúde que divulgou na internet uma lista de senhas do sistema do Ministério da Saúde que dava acesso aos bancos de dados dos pacientes, aproximadamente 8% (oito por cento) dos brasileiros foram atingidos.

Essas considerações são necessárias para entender que, de uma maneira geral, nem os órgãos públicos do mais alto escalão nem as mais imponentes entidades privadas estão realmente seguras em relação à guarda dos dados pessoais em seu poder. O ocorrido no Hospital Brasil, da Rede D'or, embora não seja até a presente data ligado a qualquer ataque cibernético, guarda causa comum com os exemplos anteriores. O cuidado com os dados não se restringe apenas aos armazenados em servidores, mas também os arquivos físicos, não se limita aos que estão de acesso ao público, mas também à forma de tratamento e acesso dos funcionários e quais serão os usos a partir da coleta até a sua destruição.

Esse cuidado compõe dois pressupostos muito caros para a proteção de dados. O primeiro, “Privacy by Design”, criado pela canadense Ann Cavoukian (disposto no artigo 25 do GDPR) previsto no artigo 46 da LGPD (UNIÃO EUROPEIA, 2016), que assevera que “Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”.

O segundo pressuposto, denominado “Privacy by Default” ou “privacidade por padrão”, que decorre do primeiro pressuposto e consiste na ideia de que empresas garantam o processamento de dados pessoais apenas na medida do estritamente necessário para atingir uma finalidade específica; e a proteção da privacidade de forma automática no momento da coleta de dados pessoais por algum sistema de tecnologia ou prática de negócio, sem que seja necessária qualquer manifestação da vontade ou intervenção do indivíduo.

Em regras gerais, os dados pessoais dos clientes somente poderão ser coletados, exibidos, utilizados e armazenados em sistemas da empresa mediante prévia autorização, ademais nos casos em que os dados já estejam constando no sistema, será necessário obter o consentimento destes para que essas informações continuem sendo mantidas no registro. Contudo, naturalmente, no contexto da LGPD na saúde, tem um tratamento peculiar.

Inegável que no atendimento aos pacientes, os médicos têm base legal para quase todos os dados coletados. Por exemplo, no cadastro dos indivíduos, a lei obriga que constem nome, CPF, entre outros dados dessa natureza, as exceções da LGPD na saúde ainda se estendem a casos de proteção à vida, tutela da saúde, estudos feitos por órgãos de pesquisas, processos judiciais, obrigações legais ou regulatórias do controlador e processos judiciais (Art. 7º da LGPD). Contudo é necessário ressaltar que o incidente não ocorreu pela coleta irregular do dado, mas sim por sua utilização totalmente divergente da finalidade.

Não é difícil imaginar que nos hospitais os dados circulem tanto internamente quanto externamente, já que existem muitos agentes envolvidos. Esse acesso pode ocorrer desde casos em que familiares consultam se alguém deu entrada no hospital, até

a troca de informações entre outros especialistas para aprimorar o tratamento, o ponto fundamental não é a coleta ou o tratamento, porque no caso não foram trazidos dados além dos legalmente necessários aos procedimentos, mas sim a malversação de sua utilização.

Não é necessário um conhecimento profundo da legislação para dar conta que muito desses pressupostos foram frontalmente desrespeitados pelo Hospital. Feitos esses apontamentos iremos analisar o incidente nos termos da legislação civil e apontar a possibilidade de indenização por parte da consumidora além de traçar em linhas gerais a organização dos argumentos jurídicos destinados a essa reparação e o papel da agência nacional na apuração desse incidente.

3 DA ANÁLISE DO INCIDENTE NOS TERMOS DO LEGISLAÇÃO CIVIL E DO ACESSO A DADOS SENSÍVEIS DO CONSUMIDOR

A Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) dispõe sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (LGPD, artigo 1º).

A LGPD, como a constituição antes citada, tem por fundamentos, entre outros, o respeito à privacidade, à inviolabilidade da intimidade, da honra e da imagem, além da defesa do consumidor.

Nesse sentido, a LGPD diz ser dado pessoal “ informação relacionada a pessoa natural identificada ou identificável ” (LGPD, artigo 5º, inciso I), especificando que dado pessoal sensível é o “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural ” (LGPD, artigo 5º, inciso II). Portanto o prontuário médico naturalmente é considerável dado pessoal sensível, pois relatam as informações sobre o estado de saúde do paciente e todos os dados atrelados ao prontuário médico devem ser considerados confidenciais, conforme prevê o artigo 2º da Lei nº 13.787/18.

Ademais, a Resolução do Conselho Federal de Medicina nº 1605/2000 proíbe o médico de revelar o conteúdo do prontuário sem o consentimento do paciente e o Código de Ética proíbe que médicos permitam o manuseio e o conhecimento de prontuários por pessoas não obrigadas ao sigilo profissional (CONSELHO FEDERAL DE MEDICINA, 2014).

O prontuário médico trata-se de documento do paciente, cabendo ao médico ou à instituição hospitalar promover a sua guarda e manter os seus dados pelo prazo mínimo de 20 anos. Conforme a legislação já existente, os hospitais deverão zelar pela privacidade e a proteção dos dados dos prontuários independentemente do seu formato, seja físico ou digital. O mesmo tratamento deve ser direcionado aos prontuários digitais, existem normas administrativas do Conselho Federal de Medicina (CFM) que obrigam que sistemas de registro eletrônico em saúde ("S-RES") tenham uma certificação específica (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005), além de preverem o Manual de Certificação para Sistemas de Registro Eletrônico em Saúde, que estabelece padrões mínimos de segurança da informação aplicáveis a sistemas que tratam dados tão relevantes como os dados de saúde.

Além dos sistemas eficientes de segurança da informação, os estabelecimentos de saúde também devem observar a postura de seus profissionais.

Pois bem, o regramento de dados em seu artigo 6º, fixa que o tratamento de dados pessoais deverá observar a boa-fé, bem como segurança, com a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (LGPD, artigo 6º,VII) , além do dever de prevenção, com a "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais" (LGPD, artigo 6º, inciso VIII). Apenas revisitando os pressupostos de Privacy by Design e Privacy by Default, antes mencionados.

Finalmente, o artigo 42 da LGPD, diz que o controlador (hospital) ou operador (servidores) dos dados pessoais será responsabilizado quando "causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo" (LGDP, artigo 42), havendo inclusive a responsabilidade solidária entre ambas as operadoras (LGDP, artigo 42, §1º). A

denominação de controlador e operado não é tão binária, contudo, para fins da análise do caso partiremos desse cenário.

In casu, vê-se que o funcionário teve acesso aos dados pessoais, inclusive de natureza sensível, fazendo uma verdadeira devassa, a fim de obter alguma vantagem indevida. Com efeito, a vulnerabilidade da coleta e/ou armazenamento dos dados foi essencial para que o funcionário tivesse acesso a tais elementos, pois não foi possível aferir, em sendo realmente um profissional da enfermagem, se aquele ator realmente participaria daquela atividade específica ou estaria se aproveitando do acesso para obter a informação.

3.1 Dos danos materiais e os estéticos

O Código Civil, em seu artigo 944 (BRASIL, 2002), diz que a indenização mede-se pela extensão do dano, seja ela patrimonial, seja ela extrapatrimonial. Nota-se, assim, que a regra é a de que quem estiver obrigado a reparar um dano deve recompor a situação pessoal e patrimonial do lesado ao estado anterior (*statu quo ante*), para torná-la como era se o evento maléfico não tivesse se verificado, evento esse que impõe ao responsável pelo dano a obrigação de repará-lo.

No caso em apreço, utilizando como pressuposto o desvio da função do funcionário, a vulnerabilidade do armazenamento dos dados restou verificada na medida em que esse funcionário obteve todas as informações do consumidor e, com isso, enviou essas informações para terceiros.

Identificar com clareza o dano não material sofrido pela vítima e pleitear a consequente reparação é tarefa das mais difíceis, muito embora o cálculo dos danos materiais, utilizando como referência erro médico, seja mais fácil de dimensionar se houver a necessidade, por exemplo, de outras cirurgias reparadoras. O mesmo não pode se dizer do dano estético.

O dano estético é toda alteração morfológica do indivíduo, que, além do aleijão, abrange as deformidades ou deformações, marcas e defeitos, ainda que mínimos, e que impliquem sob qualquer aspecto um afeiamento da vítima, consistindo numa simples lesão desgostante ou num permanente motivo de exposição ao ridículo ou de complexo

de inferioridade, exercendo ou não influência sobre sua capacidade laborativa (DINIZ, 2005).

Ainda segundo a autora, o dano estético possui diversas terminologias, como, por exemplo, dano corporal (pretium corporis), dano físico, dano deformidade, dano fisiológico, dano à saúde, dano biológico, não importando qual terminologia será utilizada para a proteção da integridade física da vítima.

Portanto, não existe nesse sentido uma absorção automática de qualquer dano não material no âmbito dos danos morais que abordaremos a seguir.

Assim, o que caracteriza o dano estético não é a concepção subjetiva de enfeiamento, mas sim o conceito objetivo – aferível através de perícia médica – de ofensa à integridade física que torna diferente do estado anterior (BITTAR, 2008). Tal situação poderia se consolidar caso a paciente, por exemplo, desenvolvesse depressão após a exposição dos dados. Esses fatos, uma vez comprovados, devem ser utilizados como pressupostos para o desenvolvimento do raciocínio indenizatório material.

Ademais, a objetividade da responsabilidade do hospital foi estabelecida para ressalvar a posição jurídica do consumidor, ao qual não podem ser atribuídos os problemas e inadequações eventualmente existentes nos serviços que encerram a atividade empresarial do fornecedor.

Essa é a lição de Zelmo Denari (2004), que esclarece que o caput *do* dispositivo dispõe que a responsabilidade do fornecedor de serviços independe da extensão da culpa, acolhendo, também nesta sede, os postulados da responsabilidade objetiva. As causas excludentes de responsabilidade do prestador de serviços são as mesmas previstas na hipótese do fornecimento de bens, a saber: que tendo prestado o serviço, o defeito inexiste, ou que a culpa é exclusiva do usuário ou de terceiro. Pela teoria do risco do negócio, albergada no mencionado art. 14 da Lei n. 8.078/90, o fornecedor responde objetivamente pelas adversidades que envolvam a prestação de serviços inerentes à atividade lucrativa que desempenha no mercado de consumo. Assim, os fornecedores não podem se furtar aos riscos da sua atividade econômica, tampouco transferi-los ao consumidor.

Esse, inclusive, é o escólio de Sérgio Cavalieri Filho (2018), para quem “todo aquele que se disponha a exercer alguma atividade no mercado de consumo tem o dever

de responder pelos eventuais vícios ou defeitos dos bens e serviços fornecidos, independentemente de culpa”

No mesmo sentido é o entendimento do C. Superior Tribunal de Justiça, segundo o qual “a responsabilidade do fornecedor é interpretada de forma objetiva” em especial quando restar “configurado que ele não se cercou das cautelas necessárias para diminuir o risco do seu negócio” (BRASIL, 2012).

No caso, espera-se que o hospital tente se escusar da responsabilidade, sob o argumento de que não divulgou os dados, portanto, teria controle efetivo do incidente. Todavia, evidencia-se falha na prestação de serviço quanto à inobservância ao dever de segurança e preservação dos dados pessoais dos clientes e de informações de seu sistema interno, tendo em vista o vazamento de informações pessoais da consumidora, o que possibilitou a conduta danosa perpetrada por terceiro, devendo o controlador (hospital) também responder pelos danos causados, porquanto inerente ao risco da atividade econômica. Logo, ainda que exista essa tese, não há como imputar a culpa exclusiva de outrem, a fim de elidir a responsabilidade quanto aos danos, sobretudo porque é dever da fornecedora de serviços fornecer segurança aos seus clientes quanto aos dados pessoais disponibilizados à ocasião das contratações para prestação de serviços, de forma a adotar mecanismos de salvaguarda contra vazamento de dados ou utilização indevida dos mesmos.

Nessa linha, entendemos ficar demonstrado o nexo causal entre a falha dos serviços e os danos causados à consumidora, concluindo que o prejuízo material sofrido, relativo à exposição de seus dados pessoais sensíveis, deve ser reparado.

3.2 Dos danos morais

O dano moral encontra-se previsto na CRFB, artigo 5º, incisos V e X, e independe de qualquer vinculação com prejuízo material. Sabe-se que o dever de indenizar por danos morais deriva da violação dos direitos da personalidade, caracterizada pela afetação da honra, da integridade psíquica, do bem-estar íntimo, de suas virtudes, enfim, causando um mal-estar ou uma indisposição de natureza espiritual.

Sem dúvida, o Direito não repara qualquer padecimento, dor ou aflição, mas aqueles que forem decorrentes da privação de um bem jurídico sobre o qual a vítima teria interesse reconhecido juridicamente. Dito de outro modo, o dano moral consiste na lesão de direitos, com conteúdo não pecuniário, isto é, não avaliáveis comercialmente, lesionando a esfera personalíssima da pessoa humana.

No particular do mercado de consumo, o CDC identificou o consumidor como sujeito de direitos especiais, construindo um sistema normativo e principiológico, objetivando proteger e efetivar os direitos desse sujeito vulnerável. Trata-se de verdadeira realização de um direito fundamental de proteção do Estado para o consumidor (CRFB, artigo 5º, inciso XXXII).

De um lado, sabe-se que "o descumprimento de contrato pode gerar dano moral quando envolver valor fundamental protegido pela Constituição Federal de 1988" (CONSELHO DA JUSTIÇA FEDERAL, 2012). Cuida-se daquilo que a doutrina se refere como dano moral relativo, ou seja, aquele em que há lesão específica a um bem ou interesse patrimonial, mas que também implica um prejuízo extrapatrimonial, como ocorre no caso em análise, em que a dignidade da consumidora e de sua família vem sendo violada, reiteradamente, em razão da fragilidade do sistema de tratamento/armazenamento dos dados do hospital, com acesso a dados sensíveis.

De outro lado, a obtenção de dados pessoais e sensíveis do consumidor pode implicar danos futuros, pelo difícil, ou impossível determinação do "esquecimento" dos fatos veiculados.

A propósito, o Superior Tribunal de Justiça já tem assente em sua jurisprudência que a ofensa injusta à dignidade da pessoa humana, que é um dos fundamentos da República Brasileira, implicará "dano moral, não sendo necessária a comprovação de dor e sofrimento. Trata-se de dano moral *in re ipsa* (dano moral presumido) " (BRASIL, 2012-a).

Nesse sentido, a própria LGPD, em seu artigo 42, diz ser reparável o dano extrapatrimonial causado em razão da violação à legislação de proteção de dados pessoais. Cuida-se de responsabilidade objetiva, na medida em que não menciona a necessidade de comprovação de culpa, com base na teoria do risco, segundo a qual toda

pessoa que exerça alguma atividade que possa gerar danos a terceiros deverá repará-los, caso os elementos constituintes da responsabilidade aconteçam.

Sabe-se, ademais, que a Lei 12.965/2014 (Marco Civil da Internet), em seu artigo 7º, incisos I a III, tutela a inviolabilidade da intimidade e da vida privada do usuário, com o respectivo dever de reparar o dano moral ou material decorrente de sua violação, além da "inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei" , bem como a "inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial " (BRASIL, 2014).

De outro vértice, os transtornos ocasionados pela falta de segurança dos dados acarretaram um desvio produtivo das atividades da consumidora, na medida em que, em razão de um mau atendimento, ela desperdiçou seu tempo, desviando suas competências para tentar resolver um problema criado pelo fornecedor, a um custo de oportunidade indesejado, de natureza irrecuperável (DESSAUNE, 2011).

In casu, a personalidade da consumidora e de sua família tem sido violada cotidianamente, sem que o Hospital tenha tomado (até a presente data) qualquer providência idônea para fazer cessar o ilícito, a despeito de deterem todos os meios técnicos hábeis para tanto, seja a indicação de responsabilidade após processo de sindicância, seja o oferecimento dos fatos à autoridades competentes. Assim, considerando a devassa que foi feita por ocasião da divulgação dos dados, também deveria ser considerado o caráter pedagógico da medida, visando considerável aumento do valor pretendido.

3.3 Da redistribuição do ônus da prova (CDC, artigo 6º, inciso VIII, e CPC, artigo 373, § 1º)

Naturalmente estamos diante de uma relação de consumo. Sendo assim o artigo 6º, inciso VIII, do CDC, determina ser um direito básico do consumidor a facilitação de sua defesa em Juízo, inclusive com a possibilidade de inversão do ônus da prova. No mesmo sentido, o CPC, em seu artigo 373, § 1º, positiva ser viável, especialmente ante as peculiaridades do caso concreto, quando relacionadas "à impossibilidade ou à excessiva dificuldade de cumprir o encargo nos termos do caput ou à maior facilidade de

obtenção da prova do fato contrário, poderá o juiz atribuir o ônus da prova de modo diverso, desde que o faça por decisão fundamentada, caso em que deverá dar à parte a oportunidade de se desincumbir do ônus que lhe foi atribuído" (CPC, artigo 373,§1º, ob cit).

No contexto das relações jurídicas que envolvem acesso a dados pessoais e a dados sensíveis do consumidor, a LGPD, em seu artigo 42, § 2º, positivou a possibilidade de inversão do ônus da prova a favor do titular dos dados, quando for verossímil a alegação, houver hipossuficiência para a produção da prova ou quando a sua produção pelo titular resultar-lhe excessivamente onerosa.

In casu, viu-se que o servidor acessou o prontuário da consumidora, de modo que utilizou os dados do consumidor e de sua família para obter vantagens indevidas, citada eventual contraprestação pelo vazamento ou promoção pessoal mesmo que de natureza ideológica.

Dessa forma, se alguma prova técnica tiver de ser produzida em Juízo, que se inverta o ônus probatório, o qual deverá ser atribuído ao hospital, que é detentor de complexo aparato tecnológico que poderá dar conta dos cuidados tomados aos negligenciados para evitar vazamentos dessa natureza.

3.4 Da tutela para a remoção do ilícito

Não constitui qualquer novidade que, nas demandas nas quais se tenha por objeto a prestação de fazer ou não fazer, o magistrado poderá conceder a tutela específica ou determinar providências assecuratórias para a obtenção do resultado prático equivalente. Nesse sentido, a tutela específica voltada a inibir a prática, a reiteração ou a continuação de uma conduta ilícita, ou a sua remoção, prescinde da demonstração da ocorrência de dano ou da existência de culpa ou dolo (CPC, artigo 497, parágrafo único).

Nota-se, pois, que se trata de uma tutela com eficácia mandamental. Além disso, o CDC, em seus artigos 30, 35, inciso I e 84, fixa regime tutelar idêntico. Observa-se que a tutela inibitória tem por objetivo impedir, de forma direta, a violação do próprio direito material discutido em Juízo, vedando de forma definitiva a prática de ato contrário ao Direito ou, ainda, a sua continuação, isto é, seu objetivo é evitar que o ilícito ocorra,

prossiga ou se repita. Em suma, a atividade jurisdicional realiza o direito não apenas restaurando o que foi violado, como também evitando que essa violação ocorra.

No caso em apreço, o acesso ao prontuário continua disponível ainda que não esteja no endereço eletrônico do hospital, sendo assim, também será necessário a retirada desses documentos de vários locais na internet. Na situação concreta em tela, tem-se a probabilidade do direito pleiteado, consistente no dever de qualidade-segurança que todo prestador de serviços tem para com seus consumidores, vale dizer, que, *in casu*, o direito de o consumidor ter pleno acesso aos serviços hospitalar, sem qualquer interferência de terceiros ou exposição de dados pessoais sensíveis. De outra parte, tem-se o perigo de dano irreparável, a saber, a violação reiterada à privacidade do consumidor, que tem sido dia a dia sua tranquilidade e de sua família atordoada, justamente por um fato do serviço. Assim, no nosso sentir estão presentes todos os pressupostos para a concessão da tutela inibitória liminarmente, por força dos artigos 294 e seguintes, e 497, parágrafo único, todos os CPC, bem como dos artigos 84 e seguintes do CDC, sem prejuízo de atribuição de multa diária pelo descumprimento (artigo 500, do CPC, e artigo 84, §§, do CDC)

3.5 Da necessidade de sigilo do processo

Finalmente, cumpre registrar que o CPC, em seu artigo 189, inciso III, traz uma exceção ao regime de publicidade dos atos processuais, a saber, tramitará em segredo de justiça os casos que versarem sobre “os dados protegidos pelo direito constitucional à intimidade”.

No caso em referência, enquadram-se como dados protegidos pelo direito constitucional à intimidade as informações familiares e da vida pessoal do consumidor, bem como demais dados sensíveis que foram acessados pelo servidor indevidamente ou sem o devido cuidado, por meio de falha de segurança no tratamento ou no compartilhamento destes.

Sem dúvida, deve-se aplicar ao caso a teoria dos círculos concêntricos, de acordo com a qual a privacidade ou vida privada em sentido amplo contempla três círculos

concêntricos: a vida privada em sentido estrito, o círculo da intimidade e o círculo do segredo.

A vida privada em sentido restrito consiste no conjunto de relações entre o titular e os demais indivíduos, contendo informações de conteúdo material e também sentimentos, porém de caráter superficial e de menor impacto sobre a intimidade, como, por exemplo, as amizades comuns. Por sua vez, o círculo da intimidade é composto pelo conjunto de manifestações, só compartilhados com familiares e amigos próximos e, no máximo, com profissionais submetidos ao sigilo profissional, bem como a proteção do acesso indevido e publicização do conteúdo das comunicações pelos mais diversos meios, gerando o sigilo do conteúdo telemático, epistolar, telefônico, entre outros. Por fim, no círculo do segredo, há todas as manifestações e preferências íntimas que são componentes confidenciais da personalidade do titular, envolvendo suas opções e sentimentos que, por sua decisão, devem ficar a salvo da curiosidade de terceiros.

No caso em tela, não só a exposição do prontuário, como a juntada dos documentos aos autos, com conteúdos sensíveis e pertinentes à vida privada, à intimidade e a segredos dos consumidores, dão conta de que a decretação de sigilo do processo seria uma medida de rigor, com base no artigo 189, inciso III, do CPC.

4 DO PAPEL DA AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS

Autoridade Nacional de Proteção de Dados - ANPD, autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal, retratada pelo artigo Art. 52-A, foi elevada ao status de autarquia recentemente nos termos da Medida Provisória nº 1.124, de 13 de junho de 2022).

A LGPD é discutida em ações judiciais desde sua promulgação, contudo, somente em 1º de agosto de 2021 passaram a valer as sanções administrativas para empresas que não se enquadrarem nas novas regras. As punições previstas na legislação vão de advertência a multa no valor de até 2% do faturamento da empresa, limitada a R$ 50 milhões (Art. 52, Inciso II).

Natural o descolamento da esfera judiciária da administrativa, em uma análise objetiva a legislação no âmbito administrativo de fiscalização prevê a aplicando multa no

caso de mero vazamento de dados. Os termos de conduta da parte, se agiu de forma culposa, por exemplo, são mera situação atenuante ou agravante para a dosimetria da multa e/ou medida escolhida, que pode inclusive ser a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (Art. 52, Inciso XII).

Em que pese a possibilidade da multa, a postura da agência, do que se depreende de seus informativos e manuais, aponta para um aspecto mais responsivo, ou seja, tentar mostrar quais medidas as empresas devem adotar para remediar o problema e, se o agente não cooperar, vai estabelecer um procedimento administrativo, ou aplicar sanção.

Na verdade, até mesmo a comunicação do incidente à agência também será considerado como medida atenuante na medida que se amolda a um comportamento que demonstra “transparência e boa-fé”, nos termos do Inciso II, §2º, do Art. 52, sendo inclusive é princípio insculpido no Art. 6º.

No caso em exame a legislação assevera que o controlador (hospital) deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (Art. 48), contudo o tempo específico não foi regulamento, a menção se limita a retratar que a “comunicação será feita em prazo razoável” (§1º, Art. 48). Disso temos que ainda existe um espaço de discricionariedade para o prazo, sendo assim, ainda não é possível dizer que o hospital está descumprimento a LGPD, em que pese já tenham de passado mais que 48(quarenta e oito) horas do incidente e não foi possível verificar qualquer notícia nesse sentido no endereço eletrônica da autarquia.

Muito embora a imposição de multa seja eficiente em ambos os sentidos, coercitivos e pedagógicos, no caso em tela as determinações administrativas da agência talvez sejam muito mais importantes para a prevenção de situações similares do que o processo administrativo que poderá decidir pela multa, na medida que após a notícia do incidente a “autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como medidas para reverter ou mitigar os efeitos do incidente” (Inciso II, §2º, Art. 48).

Ademais, do ponto de vista de uma empresa privada existem outras sanções muito mais gravosas que a multa, cite-se a publicização da infração após devidamente apurada

e confirmada a sua ocorrência (Inciso IV, Art. 52) e a eliminação dos dados pessoais a que se refere a infração (Inciso VI, Art. 52), o que poderia significar a impossibilidade de funcionamento da empresa na prática. A publicização da infração pela autoridade, além de significar um juízo técnico da autarquia competente que facilmente embasaria milhares de ações judiciais buscando ressarcimento, certamente iria repercutir no valor das empresas de capital aberto, no último caso de eliminação dos dados, imaginemos o que iria significar para empresas do e-commerce. Não é demais lembrar que as sanções da LGPD são mais amenas que as previstas no GDPR indicando mais uma vez a expectativa de uma lenta adequação e o cuidado da agência em sopesar seus poderes na promoção da adequação e não em uma corrida pelo faturamento de multa milionárias.

Por fim, no caso de vazamento individual como foi o caso em análise também poderá ocorrer conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades (§7º, Art. 52). Salutar esclarecer que mesmo que a empresa não tenha feito notícia qualquer um poderá direcionar tal incidente à agência[12] e naturalmente a consumidora deverá fazê-lo na inércia do Hospital.

5 DAS CONCLUSÕES

Para analisar de maneira satisfatória o caso são necessárias duas conclusões. A primeira em relação à pretensão indenizatória da consumidora, entendemos que não importa se o incidente foi ato isolado de um funcionário do hospital, ou ainda, teve origem na fragilidade do guarda ou tratamento dos dados, ou mesmo, sistema operacional desenvolvido por um terceiro fabricante. Se o sistema ou a rotina atual não é suficiente para proteger o consumidor, mas está sendo usado para causar-lhe prejuízos, quem deve suportar os danos são os fornecedores. Afinal, tudo isso, como já dito, é elemento que integra a cadeia de fornecimento do serviço hospitalar, circunstância que atrai a responsabilidade solidária do hospital enquanto operadora contratada para prestar os serviços (art. 7º do CDC).

Sem dúvida, não se imputa ao hospital, dentro dos fatos disponíveis, uma conduta ilícita comissiva, mas sim uma conduta ilícita omissiva, consistente inércia ante a vulneração de seus sistemas de dados por parte de um colaborador, além da omissão

em solucionar o problema formalmente noticiado, contra o qual têm os meios para debelar, razão pela qual o ato antijurídico está no descumprimento do dever de segurança, inerente à prestação de. É que o CDC impõe ao fornecedor um dever de qualidade dos produtos e serviços, o qual, se descumprido, surgem efeitos previstos ao longo do CDC. Tal dever bifurca-se em uma dupla exigência, de qualidade-adequação (cuja regulação consta do CDC 18 e ss.) e de qualidade-segurança (cuja regulação consta do CDC 12 a 17). Tem-se aí a teoria da qualidade.

No caso concreto, o servidor demonstrou ter acesso a todos os dados pessoais sensíveis da consumidora, com o fim de obter vantagens diversas. Isso demonstra que, por sua vulnerabilidade, o empregado mal intencionado teve acesso, e a empresa não empregou controles efetivos na guarda dos dados, corroborando a vulnerabilidade e, em consequência, o acidente de consumo se consolidou.

Nesse contexto, para além das normas do CC e do CDC sobre o tema, a LGPD, em seu artigo 42, diz ser reparável o dano extrapatrimonial causado em razão da violação à legislação de proteção de dados pessoais. Cuida-se de responsabilidade objetiva. De outra parte, a Lei 12.965/2014 (Marco Civil da Internet), em seu artigo 7º, incisos I a III, tutela a inviolabilidade da intimidade e da vida privada do usuário, com o respectivo dever de reparar o dano moral ou material decorrente de sua violação, além da “inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei”, bem como a “inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial”. Observou-se que a conduta ilícita do hospital, para além dos prejuízos patrimoniais, implicou, sim, danos extrapatrimoniais à consumidora, que precisará ingressar em Juízo para ver restaurado o *status quo ante*. De modo que tais fatos jurídicos são idôneos a atingir os direitos da personalidade da parte consumidora, sobretudo no que diz respeito à integridade psíquica, à tranquilidade e à honra subjetiva.

No caso concreto, entendemos suficientemente demonstrada a grave violação dos direitos da personalidade. Como bem exposto, houve vazamento de dados pessoais sensíveis, consolidado em prontuário médico. A simples disponibilização indevida de tais dados já é suficiente para configurar o dano moral, situação que se agrava no caso concreto quando se leva em conta que isso foi utilizado para causar danos à parte autora.

Pela teoria do risco do negócio, albergada no art. 14 do CDC, o fornecedor responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação de serviços. Assim, os fornecedores não podem se furtar aos riscos da sua atividade econômica, tampouco transferi-los ao consumidor. Comprovada a falha na prestação de serviço quanto à inobservância ao dever de segurança e preservação dos dados pessoais dos clientes e de informações de seu sistema interno, tendo em vista o vazamento de informações pessoais, devem responder pelos danos causados, porquanto inerente ao risco da atividade econômica.

O aviltamento dos direitos inerentes à personalidade, sobretudo a intimidade, a vida privada e a integridade psíquica, visto que houve o vazamento dos dados pessoais e utilização indevida por terceiro para prática caluniosa, rende, ao nosso sentir, ensejo à pretensão indenizatória pelo dano moral experimentado.

Repisamos: evidencia-se que o vazamento de dados pessoais partiu no sistema do hospital, como comprova o *print* noticiado. O art. 14 do CDC estabelece, a propósito, que 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. Logo, o caráter objetivo da responsabilidade civil exclui a culpa e a torna indiferente para a solução de litígio lastreado na prestação defeituosa de serviços. Quer dizer, a objetividade da sua responsabilidade foi estabelecida na reportada legislação para ressalvar a posição jurídica do consumidor, ao qual não podem ser atribuídos os problemas e inadequações eventualmente existentes nos serviços que encerram a atividade empresarial do fornecedor.

A expectativa do controlador (hospital) em atribuir a culpa a terceiro, dentro do fatos apurados também não deve prosperar, pois foi evidenciada a falha na prestação de serviço quanto à inobservância ao dever de segurança e preservação dos dados pessoais dos clientes e de informações de seu sistema interno, tendo em vista que o vazamento de informações pessoais foi o que possibilitou a conduta danosa perpetrada por terceiro, devendo o controlador responder pelos danos causados, porquanto inerente ao risco da atividade econômica. Logo, não há como imputar a culpa exclusiva de outrem,

a fim de elidir a responsabilidade quanto aos danos, sobretudo porque é dever da fornecedora de serviços fornecer segurança aos seus clientes quanto aos dados pessoais disponibilizados à ocasião das contratações para prestação de serviços, de forma a adotar mecanismos de salvaguarda contra vazamento de dados ou utilização indevida dos mesmos.

Nessa linha, demonstra o nexo causal entre a falha dos serviços e os danos causados, concluindo-se que o prejuízo material sofrido, relativo aos dados pessoais sensíveis vazados, deve ser reparado. Quanto à indenização por dano moral, cediço que se configura o aludido dano quando há violação a algum dos direitos relativos à personalidade do indivíduo, ou seja, quando a pessoa sofre prejuízo em algum dos atributos como o seu nome, a sua honra, a sua liberdade, a sua integridade física ou psíquica, dentre outros, gerando o dever de indenizar.

Na hipótese, evidenciou-se aviltamento dos direitos inerentes à personalidade dos autores, sobretudo a intimidade, a vida privada e a integridade psíquica, visto que houve o vazamento dos dados pessoais e utilização indevida por terceiro para prática caluniosa, rendendo ensejo à pretensão indenizatória pelo dano moral experimentado.

Por conseguinte, a falha na prestação de serviços consubstanciada no vazamento de dados pessoais e utilização das informações para fins caluniosos e vexatórios, ultrapassa o mero aborrecimento e se mostra hábil a causar transtornos na rotina dos consumidores ante a privação frontal ofensa aos seus direitos fundamentais.

A segunda parte conclusão é no sentido das medidas administrativas a cargo da Autoridade Nacional de Proteção de Dados – ANPD, que deve empregar esforços para a mitigação de incidente desta natureza utilizando de seu poder regulatório e também do Conselho Federal de Enfermagem – Cofen, que deve apurar a conduta do profissional indicado como fonte do vazamento para rigorosa penalidade.

REFERÊNCIAS

[1] Comunicado. Em colaboração ao Superior Tribunal de Justiça, cujo sistema operacional está fora do ar em virtude de ataque cibernético, o Supremo Tribunal Federal dá publicidade à Nota Oficial do STJ. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=454634&ori=1 (acesso em jun/22)

[2] Procon notifica Hospital Albert Einstein por vazar dados de pacientes. Disponível em: https://exame.com/invest/minhas-financas/procon-notifica-hospital-albert-einstein-por-vazar-dados-de-pacientes/ (acesso em jun/22)

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, ISO/TR 20514 e ISO/TS18308, S-RES, 2005.

BITTAR, Carlos Alberto. **Reparação Civil por Danos Morais**. 2015, p. 270, citando Matos, Dano moral e dano estético, 2008, p. 168-169.

BRASIL, **Lei n.13.105, de março de 2015.** Institui o Código de processo civil. Diário Oficial da União: seção 1, Brasília, DF, Ano CLII No – 51, 17 mar 2015.

_____. Constituição: **República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988.

_____. **Lei 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União, Brasília, 16 jul. 1990.

_____. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002.

_____. **Lei nº 12.527, de 18 de novembro de 2011**. Lei e Acesso a informação (LAI). Brasília, DF: Senado Federal, 2011.

_____. **Lei nº 12.737, de 30 de novembro de 2012**. Lei dos Crimes Cibernéticos. Brasília, DF: Senado Federal, 2012.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. . Brasília, DF: Senado Federal, 2014.

_____. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Redação dada pela Lei nº 13.853, de 2019. Brasília, DF: Senado Federal, 2018.

_____. **Supremo Tribunal Federal REsp 1292141/SP**, Rel. Ministra Nancy Andrighi, Terceira Turma, julgado em 04/12/2012, DJe 12/12/2012

_____. **Supremo Tribunal Federal**, AgRg no AREsp 658.346/RS, Rel. Ministro Moura Ribeiro, Terceira Turma, julgado em 24/03/2015, DJe 07/04/2015.

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM nº 1.931**, de 17 de setembro de 2009. Artigo 77 e artigo 85. Disponível em: https://portal.cfm.org.br/images/stories/biblioteca/codigo%20de%20etica%20medica.pdf Acesso em jun/2022

CONSELHO DA JUSTIÇA FEDERAL. **Enunciado nº 411**. V Jornada de Direito Civil. Brasília,2012.

DENARI, Zelmo. Da qualidade de produtos e serviços, da prevenção e da reparação dos danos. In GRINOVER, Ada Pelegrini et al. **Código Brasileiro de Defesa do Consumidor Comentado Pelos autores do anteprojeto,** 8ª ed. São Paulo: Forense Universitária, 2004, Cap IV.

DESSAUNE, Marcos. **Desvio Produtivo do Consumidor** – O Prejuízo do Tempo Desperdiçado. São Paulo: RT, 2011

DINIZ, Maria Helena. **Curso de Direito Brasileiro**: Responsabilidade Civil. 8. ed. São Paulo: Saraiva, 2005

FILHO,Sérgio Cavalieri. **Programa de responsabilidade civil**. 9ª ed. Atlas. São Paulo, 2010. p. 484.

INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS E SUA AVALIAÇÃO PARA FINS DE COMUNICAÇÃO À ANPD. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca (acesso em jun/22)

UNIÃO EUROPEIA, Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation).Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em 25 de jun. de 2022.