ReGeo
ISSN: 2177-3246

O ÔNUS DA PROVA EM AÇÕES DE VAZAMENTO DE DADOS: DISCUSSÃO SOBRE A POSSIBILIDADE DE INVERSÃO DO ÔNUS DA PROVA EM FAVOR DO TITULAR DOS DADOS, CONSIDERANDO SUA HIPOSSUFICIÊNCIA TÉCNICA E INFORMACIONAL

THE BURDEN OF PROOF IN DATA BREACH LAWSUITS: A DISCUSSION ON THE POSSIBILITY OF REVERSING THE BURDEN OF PROOF IN FAVOR OF THE DATA SUBJECT, CONSIDERING THEIR TECHNICAL AND INFORMATIONAL VULNERABILITY

LA CARGA DE LA PRUEBA EN LOS LITIGIOS POR VIOLACIÓN DE DATOS: UN ANÁLISIS SOBRE LA POSIBILIDAD DE INVERTIR LA CARGA DE LA PRUEBA A FAVOR DEL TITULAR DE LOS DATOS, TENIENDO EN CUENTA SU VULNERABILIDAD TÉCNICA E INFORMATIVA

https://doi.org/10.56238/revgeov17n7-011

Data de submissão: 18/05/2026 **Data de publicação:** 02/07/2026

Beatriz Jacinto Xavier
Bacharel em Direito
Instituição: Faculdade UNISAPIENS
E-mail: drabeatrizxavier@gmail.com

Pedro Henrique Moreira Simões
Doutorando em Direito
Instituição: Faculdade FADISP
E-mail: pedrohmsimoes@yahoo.com.br

RESUMO

O presente artigo científico discute a complexa questão do ônus da prova em ações judiciais decorrentes de vazamentos de dados pessoais. Analisa-se a inadequação da regra geral do Código de Processo Civil, que atribui ao autor a prova dos fatos constitutivos de seu direito, frente à notória hipossuficiência técnica e informacional do titular dos dados. Propõe-se, a partir dos princípios da Lei Geral de Proteção de Dados Pessoais (LGPD) e da analogia com o Código de Defesa do Consumidor (CDC), a inversão do ônus da prova como mecanismo de equilíbrio processual. Argumenta-se que a responsabilidade do controlador de dados, em virtude de sua posição privilegiada e de seu dever de segurança, justifica a readequação da carga probatória em favor da vítima. O artigo analisa o dilema processual decorrente do vazamento de dados na sociedade moderna, que tem a informação como seu principal ativo. Diante da centralização massiva de dados em grandes empresas, os incidentes de segurança se tornaram um risco inerente, expondo indivíduos a sérios prejuízos. O principal obstáculo para a vítima buscar reparação é a regra geral do ônus da prova, que a obriga a demonstrar a culpa ou negligência da empresa controladora. O texto argumenta que essa regra é desproporcional e injusta, pois o titular dos dados se encontra em uma posição de hipossuficiência técnica e informacional. Ele não tem acesso aos registros internos, logs de sistema ou relatórios de auditoria, ou seja, as únicas evidências capazes de provar a causa do incidente. Para resolver essa assimetria, o artigo defende a inversão do ônus da prova como um mecanismo essencial para garantir o acesso à justiça. Essa solução encontra respaldo em duas importantes frentes do direito brasileiro onde A Analogia com o Código de Defesa do Consumidor (CDC) no texto compara a vulnerabilidade do titular de dados à do consumidor, justificando a aplicação do princípio de inversão do ônus da prova já consagrado no CDC. A Dinâmica da Prova no Código de Processo Civil (CPC): O artigo ressalta que o próprio CPC permite ao juiz

redistribuir a prova quando ela se torna “excessivamente difícil” para uma das partes, o que é o caso em ações de vazamento de dados. Exigir que a vítima prove a falha do sistema seria uma “prova diabólica”. Em conclusão, o artigo defende que a interpretação judicial deve reconhecer a inversão do ônus da prova como a regra em casos de vazamento de dados. Essa medida não apenas iguala a relação processual, mas também fortalece a Lei Geral de Proteção de Dados (LGPD), incentivando as empresas a admedidas de segurança mais robustas e garantindo que o direito à proteção de dados seja efetivo na prática.

Palavras-chave: Ônus da Prova. Vazamento de Dados. Proteção de Dados. LGPD. Inversão do Ônus da Prova. Hipossuficiência.

ABSTRACT

This scientific article discusses the complex issue of the burden of proof in lawsuits arising from personal data breaches. It analyzes the inadequacy of the general rule of the Civil Procedure Code—which attributes the burden of proving constitutive facts to the plaintiff—given the notorious technical and informational vulnerability of the data subject. Based on the principles of the General Data Protection Law (LGPD) and by analogy with the Consumer Defense Code (CDC), this study proposes the reversal of the burden of proof as a mechanism for procedural balance. It argues that the data controller's liability, due to their privileged position and duty of security, justifies the reallocation of the evidentiary burden in favor of the victim. The article examines the procedural dilemma resulting from data breaches in modern society, where information is the primary asset. Given the massive centralization of data by large corporations, security incidents have become an inherent risk, exposing individuals to serious harm. The main obstacle for victims seeking redress is the general rule of the burden of proof, which requires them to demonstrate the controller's fault or negligence. This text argues that such a rule is disproportionate and unjust, as data subjects face technical and informational hipossufficiency; they lack access to internal records, system logs, or audit reports—the only evidence capable of proving the cause of the incident. To resolve this asymmetry, the article advocates for the reversal of the burden of proof as an essential mechanism to ensure access to justice. This solution is supported by two major pillars of Brazilian law: the analogy with the CDC, comparing the data subject's vulnerability to that of a consumer, and the dynamic distribution of the burden of proof in the Civil Procedure Code (CPC), which allows judges to redistribute the burden when it becomes “excessively difficult” for one party. Requiring the victim to prove a system failure would constitute “diabolical proof” (probatio diabolica). In conclusion, the article maintains that judicial interpretation must recognize the reversal of the burden of proof as the standard in data breach cases. This measure not only balances the procedural relationship but also strengthens the LGPD, incentivizing more robust security measures and ensuring that data protection rights are effective in practice.

Keywords: Burden of Proof. Data Breach. Data Protection. LGPD. Reversal of the Burden of Proof. Hipossufficiency.

RESUMEN

Este artículo científico aborda la compleja cuestión de la carga de la prueba en los litigios derivados de filtraciones de datos personales. Analiza la insuficiencia de la regla general del Código de Procedimiento Civil, que asigna la carga de la prueba de los hechos que constituyen un derecho al demandante, dada la notoria desventaja técnica e informativa del titular de los datos. Con base en los principios del Reglamento General de Protección de Datos (RGPD) y por analogía con el Código de Protección del Consumidor (CDC), propone la inversión de la carga de la prueba como mecanismo de equilibrio procesal. Argumenta que la responsabilidad del responsable del tratamiento, debido a su posición privilegiada y su deber de seguridad, justifica el reajuste de la carga de la prueba a favor de la víctima. El artículo analiza el dilema procesal que surge de las filtraciones de datos en la sociedad actual, que considera la información su principal activo. Dada la masiva centralización de datos en las

grandes empresas, los incidentes de seguridad se han convertido en un riesgo inherente, exponiendo a las personas a graves daños. El principal obstáculo para una víctima que busca reparación es la regla general de la carga de la prueba, que la obliga a demostrar la culpa o negligencia de la empresa controladora. El texto argumenta que esta regla es desproporcionada e injusta, ya que el titular de los datos se encuentra en una posición de desventaja técnica e informativa. No tiene acceso a registros internos, registros del sistema ni informes de auditoría, es decir, la única evidencia capaz de probar la causa del incidente. Para resolver esta asimetría, el artículo aboga por la inversión de la carga de la prueba como mecanismo esencial para garantizar el acceso a la justicia. Esta solución encuentra respaldo en dos áreas importantes del derecho brasileño: la analogía con el Código de Protección al Consumidor (CPC), que compara la vulnerabilidad del titular de los datos con la del consumidor, justificando la aplicación del principio de inversión de la carga de la prueba ya consagrado en el CPC. La dinámica de la prueba en el Código de Procedimiento Civil (CPC): Este artículo destaca que el propio CPC permite al juez redistribuir la carga de la prueba cuando esta se vuelve excesivamente difícil para una de las partes, como ocurre en los litigios por filtración de datos. Exigir a la víctima que demuestre el fallo del sistema constituiría una prueba excesivamente difícil. En conclusión, el artículo argumenta que la interpretación judicial debería reconocer la inversión de la carga de la prueba como norma en los casos de filtración de datos. Esta medida no solo iguala la relación procesal, sino que también fortalece la Ley General de Protección de Datos (LGPD), incentivando a las empresas a adoptar medidas de seguridad más robustas y garantizando la efectividad del derecho a la protección de datos en la práctica.

Palabras clave: Carga de la Prueba. Filtración de Datos. Protección de Datos. LGPD. Inversión de la Carga de la Prueba. Falta de Suficiencia de la Prueba.

1 INTRODUÇÃO

A sociedade contemporânea, profundamente imersa na economia da informação, têm na coleta e no tratamento de dados pessoais um de seus pilares. No entanto, o avanço tecnológico e a massificação do uso de plataformas digitais trouxeram consigo um risco inerente e crescente: o vazamento de dados. Incidentes de segurança, sejam eles causados por falhas técnicas, ataques cibernéticos ou negligência humana, expõem a privacidade e a segurança dos titulares de dados a graves prejuízos patrimoniais e extrapatrimoniais.

Deste modo, a centralidade dos dados na economia moderna que outrora era vista como informação secundária, hoje é o ativo mais valioso de muitas corporações. Na chamada economia da informação, os dados pessoais deixaram de ser meros registros para se tornarem a matéria-prima de um vasto ecossistema de negócios. Empresas de tecnologia, varejo, finanças e até saúde se baseiam na coleta, análise e monetização de dados para personalizar serviços, direcionar publicidade e tomar decisões estratégicas. Assim, esse modelo, impulsionado por dispositivos conectados e plataformas digitais onipresentes, criou uma espiral de coleta de dados sem precedentes, onde cada interação online, cada compra e até cada movimento físico se traduz em valiosos pontos de dados.

Portanto, a vulnerabilidade e os riscos de segurança aos dados são a grande preocupação hodierna, devido a massificação da coleta, com o advento da inevitável concentração de dados pessoais em grandes repositórios digitais. Essa concentração, porém, transformou as empresas em alvos atrativos para ataques cibernéticos e incidentes de segurança. A vulnerabilidade não reside apenas na má-fé de criminosos digitais. Muitas vezes, o vazamento de dados é resultado de falhas técnicas complexas, de processos de segurança inadequados ou de erro humano, como um funcionário que cai em um golpe de phishing.

Em síntese, as consequências desses incidentes são múltiplas e de longo alcance. Para o indivíduo, a exposição de informações pode levar a prejuízos patrimoniais, tais como: roubo de identidade, fraudes financeiras, uso indevido de cartões de crédito. Assim como, danos extrapatrimoniais, como por exemplo, a exposição de intimidade, constrangimento, ansiedade, perda de controle sobre a própria vida digital e, em casos extremos, perseguição e violência. E por fim, o titular dos dados, confiando sua privacidade a uma entidade pública ou privada, encontra-se em uma posição de profunda vulnerabilidade, sem meios para evitar o incidente e, muitas vezes, sem conhecimento técnico para compreender sua causa ou extensão.

Diante do exposto, o imperativo da proteção e da regulação da escala e da gravidade dos riscos, tornou-se peremptório que a sociedade respondesse com a criação de marcos regulatórios robustos. Leis como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de

Dados (GDPR) na Europa representam a tentativa de equilibrar o avanço tecnológico com o direito à privacidade e à autodeterminação informativa. Tais legislações impõem deveres rigorosos de segurança e transparência às empresas, exigindo que elas protejam os dados que coletam e responsabilizando-as por incidentes. Assim, buscam reverter a lógica da vulnerabilidade, colocando o ônus da segurança e da prova sobre as entidades que detêm e lucram com os dados, e não sobre o indivíduo que os cede. Assim, o desafio do vazamento de dados deixa de ser apenas uma questão de tecnologia, tornando-se um tema central do direito, da ética e da governança na era digital.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), a LGPD, estabeleceu um marco legal protetivo, elevando a proteção de dados a um direito fundamental e atribuindo deveres rigorosos aos agentes de tratamento. Contudo, quando um incidente de segurança se concretiza e o titular dos dados busca a reparação judicial, depara-se com um desafio processual significativo: a prova.

Nessa conjuntura, de um lado, marca um avanço legal, mas, de outro, revela uma complexa barreira processual que pode comprometer a efetividade da lei. Para entender essa tensão, é fundamental detalhar o papel da LGPD e a dificuldade prática da sua aplicação judicial.

Preliminarmente à LGPD, a proteção de dados pessoais era tratada de forma fragmentada, muitas vezes com base em leis esparsas ou, por analogia, no Código de Defesa do Consumidor. Com a sua entrada em vigor, a LGPD promoveu uma mudança de paradigma: a proteção de dados tornou-se um direito autônomo, intimamente ligado à dignidade da pessoa humana e ao direito fundamental à privacidade.

Com efeito, no intuito de garantir essa proteção, a lei impôs deveres claros e rigorosos aos "agentes de tratamento" — ou seja, às empresas e organizações que coletam e processam dados. Eles são obrigados a adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados de acessos não autorizados e de incidentes. Além disso, a LGPD exige que esses agentes notifiquem a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares dos dados afetados sobre a ocorrência de um incidente de segurança que possa gerar risco ou dano relevante. A lei, portanto, criou o arcabouço necessário para atribuir responsabilidade e exigir conformidade.

No entanto, apesar dos avanços, a efetividade da LGPD nas cortes depende de um princípio fundamental do direito processual: o ônus da prova. A regra geral, conforme o Código de Processo Civil, determina que o autor de uma ação deve provar os fatos que constituem seu direito. Consequentemente, para um possível vazamento de dados, essa regra se torna um obstáculo quase intransponível para o titular dos dados. A informação sobre o que causou o incidente — se foi uma falha técnica, uma configuração inadequada, a ausência de um sistema de defesa ou a omissão em uma

atualização de software — está sob a custódia exclusiva do réu, a empresa controladora dos dados. A vítima, por sua vez, é um elo vulnerável na cadeia. Assim sendo, não existe acesso aos logs do sistema, aos relatórios de auditoria interna ou a qualquer outra evidência técnica que demonstre a negligência da empresa. Essa assimetria de informações e conhecimento técnico é conhecida no meio jurídico como hipossuficiência técnica e informacional. A vítima tem acesso apenas ao resultado do incidente — a exposição de seus dados —, mas não à sua causa.

Com o objetivo de solucionar essa situação de profundo desequilíbrio, a solução jurídica para garantir a justiça reside na inversão do ônus da prova. Esse mecanismo processual, já consagrado no direito do consumidor, permite que o juiz atribua ao réu o dever de provar que não foi negligente. A inversão do ônus da prova pode ser aplicada em ações de vazamento de dados por dois caminhos, conforme explicitado: analogia com o Código de Defesa do Consumidor onde a relação entre o titular dos dados e o controlador assemelha-se à relação de consumo, onde o consumidor é a parte mais vulnerável. E também a dinamicidade do Código de Processo Civil que permite ao juiz redistribuir o ônus da prova quando for "excessivamente difícil" para uma das partes cumprir o encargo. E ao transferir a obrigação de provar a inexistência de culpa para a empresa, que detém todos os meios e o dever legal de segurança, o Poder Judiciário garante que o propósito protetivo da LGPD não seja frustrado. A inversão do ônus da prova é a ferramenta essencial para que o direito à proteção de dados saia do papel e se torne uma realidade efetiva para os cidadãos brasileiros.

Por isso, a regra geral do ônus da prova, conforme o Código de Processo Civil (CPC), impõe ao autor a obrigação de provar os fatos constitutivos de seu direito (Brasil, 2015). Em casos de vazamento de dados, essa regra se mostra desproporcional. A informação sobre o que causou o incidente — se foi uma falha na segurança, uma invasão, uma omissão na adoção de medidas preventivas — está sob a custódia exclusiva do controlador dos dados, que detém todo o conhecimento técnico e informacional sobre seus sistemas. O titular, por sua vez, é um elo vulnerável na cadeia, carecendo de acesso às evidências necessárias para demonstrar a culpa ou a negligência do controlador.

Em verdade, a premissa "A Hipossuficiência do Titular e o Desequilíbrio Probatório" delineia o principal obstáculo que um indivíduo enfrenta ao buscar reparação por um vazamento de dados: o notório desequilíbrio entre as partes. Conforme, a regra processual brasileira, consagrada no Art. 373 do CPC, estabelece que "o ônus da prova incumbe: I - ao autor, quanto ao fato constitutivo de seu direito..." (BRASIL, 2015). Embora essa seja uma regra fundamental, sua aplicação literal em ações de proteção de dados desconsidera a hipossuficiência técnica e informacional do titular.

Por isso, o titular de dados não é um perito em segurança da informação, nem tem acesso aos logs de sistemas, relatórios de vulnerabilidade, registros de acesso ou qualquer outro documento

interno da empresa controladora. Exigir que ele prove a falha na segurança ou a negligência da empresa seria impor uma "prova diabólica" — uma prova virtualmente impossível de ser produzida. A informação crucial para a elucidação do caso é retida pela parte ré, que é a única com acesso a ela.

Diante desse quadro de profunda assimetria, a doutrina e a jurisprudência têm se inclinado para a inversão do ônus da prova como a solução mais justa e eficaz. Tal medida encontra amparo em dois importantes pilares do ordenamento jurídico brasileiro: Analogia com o Direito do Consumidor: A relação entre o titular de dados e o controlador assemelha-se, em muitos aspectos, à relação de consumo. O titular é a parte vulnerável, que confia seus dados a um fornecedor que os detém e lucra com eles. O Código de Defesa do Consumidor (CDC), em seu Art. 6º, inciso VIII, já prevê essa inversão:

> "São direitos básicos do consumidor: (...) a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências" (BRASIL, 1990).

Conforme argumenta Doneda (2019), o titular de dados encontra-se em uma posição de vulnerabilidade análoga à do consumidor, o que justifica plenamente a aplicação desse princípio protetivo.

E ainda, a versão moderna do CPC, em seu Art. 373, §1º, trouxe um importante avanço ao permitir a readequação da carga probatória pelo juiz, "quando, por peculiaridades da causa, a distribuição do ônus da prova se tornar excessivamente difícil para uma das partes". Para juristas como Pinheiro (2020), essa previsão legal se encaixa perfeitamente em casos de vazamento de dados, nos quais a dificuldade de prova para a vítima não é apenas uma peculiaridade, mas uma característica intrínseca do próprio incidente. O juiz, portanto, pode e deve inverter o ônus, exigindo que o controlador demonstre que adotou todas as medidas de segurança exigidas pela Lei Geral de Proteção de Dados (LGPD).

Em suma, a inversão do ônus da prova é a ferramenta essencial para que o direito à proteção de dados saia do campo teórico e se torne uma realidade efetiva nas cortes. Ela garante a paridade de armas processuais e assegura que a responsabilidade por incidentes de segurança recaia sobre quem detém os meios e o dever legal de prevenção.

Diante desse panorama, o presente trabalho visa a analisar a possibilidade de inversão do ônus da prova em ações de reparação de danos decorrentes de vazamentos de dados, considerando-se a notória hipossuficiência técnica e informacional do titular dos dados. A partir da premissa de que a sociedade se ergue sobre o pilar dos dados, o cenário se desdobra para revelar os desafios e as

vulnerabilidades inerentes a essa nova realidade. O desenvolvimento do tema passa, inevitavelmente, pela análise da centralidade dos dados na economia moderna, dos riscos a que essa centralidade expõe os indivíduos e da resposta regulatória necessária para mitigar esses perigos.

Neste ínterim, observa-se que os dados pessoais não são apenas informações, eles são um dos motores da economia moderna. Empresas usam nossos dados para personalizar anúncios, otimizar serviços e tomar decisões estratégicas. Esse modelo, impulsionado por tecnologias como smartphones e redes sociais, leva à coleta e ao armazenamento massivo de informações sobre os indivíduos. Essa centralização de dados, no entanto, cria vulnerabilidades inevitáveis. Como todo sistema, aqueles que armazenam dados estão sujeitos a falhas técnicas, ataques cibernéticos e erros humanos. Quando ocorre um vazamento de dados, a segurança e a privacidade dos indivíduos são expostas a riscos sérios e concretos.

E ainda, o principal obstáculo que a vítima de um vazamento enfrenta na justiça conforme regra geral da lei brasileira exige que quem entra com uma ação judicial (o autor) prove os fatos que sustentam seu pedido. Em um caso de vazamento de dados, isso significa que a vítima teria que provar a falha ou a negligência da empresa que detinha seus dados.

Essa regra se torna desproporcional porque as evidências estão todas com a empresa. O indivíduo não tem como acessar os registros de segurança, os logs de servidor, os relatórios de auditoria ou as análises técnicas que mostram o que deu errado. Essa falta de acesso e de conhecimento é o que o texto chama de hipossuficiência técnica e informacional. A vítima é a parte mais fraca e não tem as ferramentas necessárias para cumprir a exigência legal de prova.

Por fim, a análise da inversão do ônus da prova impõe ao mecanismo jurídico que não retira a necessidade de prova, mas a transfere para a parte que tem o controle das evidências — ou seja, a empresa que sofreu o vazamento. Com a inversão do ônus, a empresa seria obrigada a provar que não foi negligente e que adotou todas as medidas de segurança adequadas para proteger os dados. Em vez de a vítima ter que provar a culpa da empresa, a empresa tem que provar sua inocência. Essa mudança busca criar um processo mais justo e, ao mesmo tempo, incentivar as empresas a levarem a segurança de dados mais a sério, sabendo que terão que provar sua diligência em caso de um incidente.

2 O CONTEXTO JURÍDICO DO VAZAMENTO DE DADOS E A LGPD

A LGPD, inspirada por legislações internacionais como o GDPR europeu, estabelece um ecossistema legal que visa a garantir a proteção dos dados pessoais. A lei fixa princípios como a segurança, a prevenção e a não discriminação, e impõe aos agentes de tratamento, em especial ao

controlador, a adoção de medidas técnicas e administrativas aptas a proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas (Brasil, 2018).

A responsabilidade civil em caso de dano é tratada no art. 42 da LGPD, que dispõe: "O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo" (Brasil, 2018). Embora a redação do dispositivo não seja explícita sobre a natureza da responsabilidade, se objetiva ou subjetiva, a doutrina tem ponderado sobre a aplicação da responsabilidade objetiva em casos de vazamento, haja vista que a própria LGPD estabelece um dever de segurança para o controlador, independentemente de culpa (Pinheiro, 2020).

Ademais, a LGPD é um diploma legal que deve ser interpretado em harmonia com outros ramos do direito, especialmente o direito processual e o direito do consumidor. A proteção do titular de dados, nesse sentido, se alinha à proteção do consumidor, um sujeito igualmente vulnerável na relação jurídica (Doneda, 2019).

A LGPD, inspirada por legislações internacionais como o GDPR europeu, estabelece um ecossistema legal que visa a garantir a proteção dos dados pessoais. A lei fixa princípios como a segurança, a prevenção e a não discriminação, e impõe aos agentes de tratamento, em especial ao controlador, a adoção de medidas técnicas e administrativas aptas a proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas (Brasil, 2018).

A responsabilidade civil em caso de dano é tratada no art. 42 da LGPD, que dispõe: "O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo" (Brasil, 2018). Embora a redação do dispositivo não seja explícita sobre a natureza da responsabilidade, se objetiva ou subjetiva, a doutrina tem ponderado sobre a aplicação da responsabilidade objetiva em casos de vazamento, haja vista que a própria LGPD estabelece um dever de segurança para o controlador, independentemente de culpa (Pinheiro, 2020).

Ademais, a LGPD é um diploma legal que deve ser interpretado em harmonia com outros ramos do direito, especialmente o direito processual e o direito do consumidor. A proteção do titular de dados, nesse sentido, se alinha à proteção do consumidor, um sujeito igualmente vulnerável na relação jurídica (Doneda, 2019).

A proteção de dados pessoais, elevada pela LGPD ao patamar de direito fundamental, se concretiza através da atribuição de deveres e, consequentemente, da responsabilidade civil dos agentes de tratamento. O cerne do debate sobre a natureza da responsabilidade em casos de vazamento de dados reside na interpretação do art. 42 da LGPD. Embora o dispositivo não use a expressão

"responsabilidade objetiva", a doutrina tem argumentado que a conjunção de outros artigos da lei aponta para essa direção (Pinheiro, 2020).

A LGPD impõe um dever de segurança, previsto no art. 46, segundo o qual "os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais". Ao vincular o dever de reparação do dano à violação desse dever de segurança, a lei afasta a necessidade de o titular de dados comprovar a culpa do controlador. A responsabilização, portanto, se baseia na simples existência do dano e na violação de uma obrigação legal, o que configura a responsabilidade objetiva. Essa interpretação fortalece a posição do titular, que não precisa se aprofundar nas complexidades técnicas do incidente, bastando demonstrar o dano sofrido em razão do vazamento.

A LGPD não é um sistema legal isolado, mas sim um diploma que dialoga com o ordenamento jurídico brasileiro, sendo o Código de Defesa do Consumidor (CDC) um de seus principais interlocutores. A analogia entre a relação entre controlador e titular de dados e a relação de consumo é amplamente aceita, dada a notória hipossuficiência do titular.

Conforme sustenta Doneda (2019), a vulnerabilidade do titular não se limita apenas à falta de poder econômico, mas se estende à sua hipossuficiência técnica e informacional. O indivíduo, que não possui conhecimento especializado sobre sistemas de segurança, nem acesso aos registros internos de uma empresa, não pode ser obrigado a provar a falha que levou ao vazamento. Essa assimetria de informações e conhecimento justifica a aplicação dos princípios do CDC. Por exemplo, o art. 6º, inciso VIII, do CDC prevê a inversão do ônus da prova em favor do consumidor quando ele é hipossuficiente ou sua alegação é verossímil. A aplicação desse princípio às ações de vazamento de dados é um instrumento crucial para reequilibrar a balança processual e garantir que o direito à reparação seja efetivo.

Ao interpretar a LGPD em harmonia com o CDC, o sistema jurídico brasileiro confere maior proteção aos titulares de dados, reconhecendo que a responsabilização dos agentes de tratamento é um pilar essencial para a construção de um ambiente digital mais seguro e confiável.

3 A INVERSÃO DO ÔNUS DA PROVA COMO MECANISMO DE EQUILÍBRIO

A regra geral do ônus da prova, consagrada no art. 373 do CPC, determina que "o ônus da prova incumbe: I - ao autor, quanto ao fato constitutivo de seu direito; II - ao réu, quanto à existência de fato impeditivo, modificativo ou extintivo do direito do autor" (Brasil, 2015). A aplicação literal dessa norma em ações de vazamento de dados resulta em um cenário de profundo desequilíbrio.

O titular dos dados, na condição de autor da ação, tem a incumbência de provar que o controlador não adotou as medidas de segurança adequadas ou que agiu com negligência. Ocorre que tal prova é praticamente impossível. Os mecanismos de segurança, os registros de acesso, os logs de auditoria e a análise da causa-raiz do incidente são informações que se encontram exclusivamente sob o domínio do réu, o controlador. A parte lesada, por sua vez, tem acesso apenas ao resultado: o vazamento de seus dados.

Nesse contexto, a inversão do ônus da prova surge como um instrumento jurídico indispensável para reestabelecer o equilíbrio processual e garantir o acesso à justiça. Tal possibilidade encontra respaldo em duas importantes vertentes do ordenamento jurídico brasileiro: o Código de Defesa do Consumidor (CDC) e o próprio Código de Processo Civil.

O CDC, em seu art. 6º, VIII, prevê a inversão do ônus da prova em favor do consumidor "quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiência" (Brasil, 1990). A doutrina e a jurisprudência são unânimes em reconhecer a aplicabilidade de tal princípio nas relações de consumo. A relação entre o titular dos dados e o controlador assemelha-se, em muitos aspectos, à relação de consumo, dada a vulnerabilidade e a assimetria informacional da parte mais fraca.

Além disso, o art. 373, §1º, do CPC, permite ao juiz a redistribuição dinâmica do ônus da prova "quando, por peculiaridades da causa, a distribuição do ônus da prova se tornar excessivamente difícil para uma das partes, ou quando for o caso de responsabilidade pela prova do fato contrário". Essa regra é perfeitamente aplicável aos casos de vazamento de dados, nos quais a dificuldade de prova para o titular não é apenas uma "peculiaridade", mas uma característica intrínseca da própria relação jurídica (Tartuce; Neves, 2021) [1] . A demonstração do dano e do nexo de causalidade já se torna uma tarefa complexa; exigir que a vítima prove a falha do sistema do réu seria uma "prova diabólica", inviabilizando qualquer pretensão de reparação.

A regra geral do ônus da prova, consagrada no art. 373 do CPC, determina que "o ônus da prova incumbe: I - ao autor, quanto ao fato constitutivo de seu direito; II - ao réu, quanto à existência de fato impeditivo, modificativo ou extintivo do direito do autor" (Brasil, 2015). A aplicação literal dessa norma em ações de vazamento de dados resulta em um cenário de profundo desequilíbrio.

O titular dos dados, na condição de autor da ação, tem a incumbência de provar que o controlador não adotou as medidas de segurança adequadas ou que agiu com negligência. Ocorre que tal prova é praticamente impossível. Os mecanismos de segurança, os registros de acesso, os logs de auditoria e a análise da causa-raiz do incidente são informações que se encontram exclusivamente sob

[1] TARTUCE, Flávio; NEVES, Daniel Amorim Assumpção. Manual de direito do consumidor. 10. ed. Rio de Janeiro: Forense, 2021.

o domínio do réu, o controlador. A parte lesada, por sua vez, tem acesso apenas ao resultado: o vazamento de seus dados.

Nesse contexto, a inversão do ônus da prova surge como um instrumento jurídico indispensável para reestabelecer o equilíbrio processual e garantir o acesso à justiça. Tal possibilidade encontra respaldo em duas importantes vertentes do ordenamento jurídico brasileiro: o Código de Defesa do Consumidor (CDC) e o próprio Código de Processo Civil.

O CDC, em seu art. 6º, VIII, prevê a inversão do ônus da prova em favor do consumidor "quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiência" (Brasil, 1990). A doutrina e a jurisprudência são unânimes em reconhecer a aplicabilidade de tal princípio nas relações de consumo. A relação entre o titular dos dados e o controlador assemelha-se, em muitos aspectos, à relação de consumo, dada a vulnerabilidade e a assimetria informacional da parte mais fraca.

Além disso, o art. 373, §1º, do CPC, permite ao juiz a redistribuição dinâmica do ônus da prova "quando, por peculiaridades da causa, a distribuição do ônus da prova se tornar excessivamente difícil para uma das partes, ou quando for o caso de responsabilidade pela prova do fato contrário". Essa regra é perfeitamente aplicável aos casos de vazamento de dados, nos quais a dificuldade de prova para o titular não é apenas uma "peculiaridade", mas uma característica intrínseca da própria relação jurídica (Tartuce; Neves, 2021). A demonstração do dano e do nexo de causalidade já se torna uma tarefa complexa; exigir que a vítima prove a falha do sistema do réu seria uma "prova diabólica", inviabilizando qualquer pretensão de reparação.

O texto acima delineia o dilema central das ações judiciais de vazamento de dados. A aplicação literal da regra geral de ônus da prova cria um cenário de profundo desequilíbrio processual. O titular dos dados, embora seja a parte lesada, encontra-se em uma posição de notória hipossuficiência técnica e informacional. Ele não possui os meios, o conhecimento ou o acesso aos registros internos da empresa para demonstrar a falha que levou ao incidente.

Essa assimetria informacional faz com que a prova da culpa ou da negligência do controlador seja uma tarefa virtualmente impossível. Enquanto o controlador detém todos os logs de sistema, relatórios de auditoria e análise de vulnerabilidades, a vítima tem acesso apenas ao resultado do incidente: o dano. Para reverter essa lógica e garantir a efetividade da proteção de dados, o ordenamento jurídico brasileiro oferece as ferramentas necessárias.

A necessidade de inversão do ônus da prova não é apenas uma demanda de justiça, mas uma medida com sólido respaldo legal, ancorada em dois diplomas centrais do direito brasileiro.

O primeiro pilar para a inversão do ônus da prova em casos de vazamento de dados reside na analogia com o Direito do Consumidor. A relação entre o titular de dados e o controlador assemelha-se, em essência, à relação de consumo, em que o titular é o polo vulnerável. A Lei Geral de Proteção de Dados Pessoais (LGPD) e o CDC se complementam em seu propósito de proteger a parte mais fraca da relação jurídica.

Conforme a doutrina, a hipossuficiência do consumidor, que justifica a inversão probatória no CDC, é perfeitamente análoga à do titular de dados (Doneda, 2019). Não se trata de uma hipossuficiência meramente econômica, mas de uma falta de acesso a informações e de conhecimento técnico que impossibilitam a produção da prova.

O segundo e mais direto fundamento para a inversão está no próprio Código de Processo Civil. O art. 373, §1º, do CPC, permite que o juiz, de forma dinâmica, redistribua a carga probatória quando a sua distribuição original se tornar "excessivamente difícil" para uma das partes.

A dificuldade de provar a culpa do controlador em um vazamento de dados não é uma mera "peculiaridade", mas uma característica inerente à própria natureza do incidente. A prova da diligência ou da falha de segurança está sob o domínio exclusivo do réu. Exigir que a vítima realize essa prova seria impor-lhe uma "prova diabólica", algo que a jurisprudência moderna busca evitar para não inviabilizar o acesso à justiça.

Em suma, a inversão do ônus da prova não é uma exceção à regra, mas sim a aplicação de um princípio fundamental de equilíbrio processual que visa a corrigir uma assimetria inerente à economia da informação. É a ferramenta jurídica essencial para que a LGPD cumpra seu papel protetivo, garantindo que a responsabilidade por incidentes de segurança recaia sobre quem detém os meios e o dever de evitá-los.

4 CONCLUSÃO

A proteção de dados pessoais, por ser um direito fundamental, exige um reexame das regras processuais tradicionais quando estas se mostram insuficientes para garantir a efetividade da tutela jurisdicional. A atribuição do ônus da prova ao titular dos dados em ações de vazamento desconsidera sua inerente hipossuficiência técnica e informacional, criando uma barreira intransponível para a reparação de danos.

Em um cenário onde os dados pessoais se tornaram o novo motor da economia, o tradicional regime processual se mostra anacrônico para resolver os conflitos decorrentes de sua má gestão. A hipossuficiência técnica e informacional do titular dos dados é o princípio central que justifica a readequação da carga probatória. A vítima de um vazamento de dados, desprovida de acesso aos logs de

sistema, relatórios de auditoria e análises forenses, não pode ser obrigada a produzir uma prova diabólica, ou seja, uma prova cuja produção está além de sua capacidade fática e técnica. O direito à reparação, nesse contexto, seria meramente ilusório (Pinheiro, 2020).

Nesse sentido, a inversão do ônus da prova surge como a ferramenta jurídica indispensável para reestabelecer o equilíbrio processual. Conforme defende a doutrina (Doneda, 2019), a proteção do titular de dados se alinha à tutela do consumidor, um sujeito igualmente vulnerável na relação jurídica, o que justifica a aplicação do princípio previsto no art. 6º, VIII, do Código de Defesa do Consumidor. Além disso, o próprio Código de Processo Civil, em seu art. 373, §1º, confere ao magistrado a autoridade para aplicar a distribuição dinâmica do ônus da prova em situações onde a dificuldade de produção de prova é manifesta (Tartuce; Neves, 2021).

O reconhecimento judicial da inversão do ônus da prova, portanto, vai além da simples facilitação do acesso à justiça para a vítima. Ele consolida um novo paradigma de responsabilidade, transferindo o fardo da prova da diligência e da segurança para o agente de tratamento, que é quem de fato detém o controle dos riscos e dos meios para mitigá-los. Essa postura não apenas viabiliza a reparação dos danos, mas também fortalece a LGPD em sua função preventiva, incentivando a conformidade e a adoção de medidas de segurança robustas. Somente com essa interpretação progressiva e alinhada à realidade digital, a proteção de dados pessoais cumprirá sua missão de salvaguardar os direitos fundamentais do cidadão na sociedade contemporânea.

A inversão do ônus da prova, prevista no Código de Defesa do Consumidor e no próprio Código de Processo Civil, constitui-se como a solução mais adequada para equalizar a relação processual. Ela transfere o fardo probatório para quem detém as informações, os meios e o dever legal de segurança, que é o controlador de dados. Ao exigir que o controlador demonstre que adotou todas as medidas necessárias para evitar o incidente, o Judiciário não apenas facilita a reparação do dano, mas também incentiva a cultura da segurança e da prevenção, em perfeita consonância com os objetivos da LGPD.

Portanto, a interpretação judicial em casos de vazamento de dados deve caminhar no sentido de reconhecer a inversão do ônus da prova como regra, em virtude da impossibilidade técnica e da desigualdade entre as partes. Somente assim a LGPD cumprirá seu papel de instrumento efetivo de proteção dos direitos fundamentais dos cidadãos na era digital.

REFERÊNCIAS

BRASIL. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil. Diário Oficial da União, Brasília, DF, 2015.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 2018.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 1990.

DONEDA, Danilo. Da privacidade à proteção dos dados pessoais. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais. 4. ed. São Paulo: Saraiva Educação, 2020.

SARLET, Ingo Wolfgang. A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 12. ed. Porto Alegre: Livraria do Advogado Editora, 2017.

TARTUCE, Flávio; NEVES, Daniel Amorim Assumpção. Manual de direito do consumidor. 10. ed. Rio de Janeiro: Forense, 2021.