A prova técnica pericial na conformidade e em litígios envolvendo a LGPD e a violação à dados pessoais

Diante da possibilidade da inversão do ônus da prova em favor do titular de dados, como agentes de tratamento poderão fazer prova de conformidade, ou mesmo de que não deram causa a eventos ou incidentes ligados à dados pessoais, evitando-se responsabilizações e penalidades?

José Antonio Milagre*

A multas e sanções da Lei Geral de Proteção de Dados (LGPD) já poderão ser aplicadas a partir de agosto de 2021. A LGPD estabelece que o Juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa. De fato, a produção da prova envolvendo tratamento irregular de dados pessoais, no ambiente tecnológico, possui uma série de peculiaridades.

É inegável que atribuir ao titular de dados o ônus técnico de provar o tratamento indevido de dados pessoais ou a insegurança da informação de controladores e operadores é tarefa deveras custosa, considerando sua hipossuficiência, bem como assimetria informacional existente, razão pela qual quis o legislador prever a possibilidade da denominada "inversão do ônus da prova", já consagrada no Código de Defesa do Consumidor. É cediço que a demonstração de falha no sistema cabe a quem tem melhores condições **[1]**.

Além disso, quando versamos da hipótese de tratamento com base

no “consentimento” (uma das premissas para tratamento de dados pessoais) é previsão legal que cabe ao controlador o ônus de provar que o consentimento foi obtido em conformidade com o disposto na lei, ou seja, se o titular nega ter consentido, caberá àquele a responsabilidade de apresentar evidências desta conduta.

Muitos agentes de tratamento indagam qual a melhor forma de demonstrar que as atividades de tratamento de dados pessoais na empresa adotam, de fato, controles e medidas de segurança da informação para proteção dos dados pessoais. Como provar que as ações técnicas e organizativas estão ativas e não passam de autodeclarações? Como ir além de uma “autodeclaração” e gerar evidências independentes, provas da adoção de um Sistema de Gestão da Privacidade da Informação? Ou como avaliar robustez de controles para assegurar que eram efetivos, considerando o estado da técnica atual?

É notório que a Segurança da Informação tem sua atuação na proteção dos atributos de segurança, confidencialidade, disponibilidade e integridade a informação. Não se pode cogitar em privacidade sem segurança da informação. Tanto é verdade que um dos princípios ligados às atividades de tratamento de dados pessoais, trazidos na LGPD, é o princípio da segurança, pelo qual, devem os agentes de tratamento utilizar 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. A declaração de aplicabilidade, principal ligação entre avaliação de riscos e implementação da segurança da informação, prática que revela os controles eleitos como necessários para organização e como serão implementados, é uma importante atividade no processo de adequação e deve ser conduzida com muita cautela, para se evitar, em um futuro, seja considerado que a empresa não adotou controles que seriam evidentemente necessários, de acordo com suas atividades desenvolvidas.

A legislação pátria de proteção de dados é clara ao prever que o tratamento irregular de dados pessoais não é só aquele que não observa a legislação (aspecto jurídico), mas também aquele que não "fornece a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, dentre elas, o modo pelo qual é realizado, o resultado e os riscos que razoavelmente dele se esperam, bem como as técnicas de tratamento de dados pessoais disponíveis à época em que foram realizados" (aspecto técnico).

Algumas inferências são possíveis: a) É preciso alinhar o modo pelo qual os dados pessoais são tratados, com o uso de melhores e reconhecidas práticas de segurança da informação disponíveis; b) É preciso identificar e analisar os riscos que determinadas atividades de tratamento de dados possuem; c) É preciso certificar que as técnicas usadas para tratamento de dados pessoais estão *paripassu* com técnicas seguras e disponíveis à época do tratamento.

A exemplo, tem-se tornado comum, judicialmente, processos movidos por pessoas contra plataformas, por invasões feitas a partir do acesso ligado a um único fator de autenticação. As teses, são as que disponibilizar um serviço onde se autentica com apenas um fator, em teoria, não é postura alinhada com técnicas já disponíveis e mais seguras, como por exemplo, o uso de uma biometria ou validação adicional por um token ou dispositivo, autenticação duplo fator.

Neste sentido, já se decidiu que a não comprovação de instruções enviadas ao usuário do sistema, sobre utilização certificação digital ou duplo fator de autenticação, para conferir maior segurança nas operações, evidenciam falha interna de segurança na empresa **[2].**

Conquanto não existam critérios rígidos para se avaliar o que é "melhor técnica", é neste ambiente que a perícia forense digital poderá ter atuação fundamental, tanto em processos judiciais e até mesmo em processos administrativos da

Autoridade Nacional de Proteção de Dados (ANPD) e outros órgãos. A prova pode ser a pericial, ligada a um exame, ou até mesmo a prova técnica simplificada, envolvendo casos de menor complexidade, onde o especialista, analisando o contexto, profere seu parecer, sendo ouvido na própria audiência de instrução, com a garantia da participação dos assistentes técnicos, dispensando-se, nesta hipótese, um laudo.

Oportuno mencionar que, de acordo com a LGPD, responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que deixa de adotar as 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. A Autoridade Nacional de Proteção de Dados Pessoais, inclusive, já recebeu contribuições para regulamentar o processo de notificação de incidentes envolvendo dados pessoais.

A resposta a incidentes adequada necessariamente passa pela perícia técnica. Explica-se. Como provar, em um processo administrativo ou judicial relativo a suposto tratamento irregular, que a empresa efetivamente adotava as medidas de segurança e satisfazia, a exemplo, o disposto na LGPD ou no futuro regulamento de "padrões técnicos mínimos de segurança"? Como demonstrar, por exemplo, as medidas que foram adotadas para reter ou mitigar os efeitos do prejuízo ligado a incidentes de segurança envolvendo dados pessoais, para fins de atenuar a aplicação de sanções e multas?

Não é demais destacar que no juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos dos serviços, para terceiros não autorizados a acessá-los. Além disso, poderá a própria ANPD determinar medidas para reverter ou mitigar os riscos e os efeitos do incidente, como, por exemplo, determinar a condução de uma perícia ou auditoria,

para que se possa levantar elementos e evidências sobre o ocorrido, gerando, inclusive, maior transparência aos titulares envolvidos.

Neste contexto, a perícia técnica em processos, litígios e autuações ligadas a vazamento de dados pessoais ou supostos tratamentos irregulares revela-se fundamental, como garantia independente de que o agente de tratamento cumpriu suas obrigações, quer preventiva, quer reativamente. A perícia digital pode ser útil em inúmeras fases ou acontecimentos ligados à temática, incluindo, mas não se limitando a:

1. *a) Divergências sobre a coleta do consentimento:* Demonstrar que os registros do sistema informático que gravam o consentimento não foram alterados e que os dados correspondem a uma atividade de aceitação, íntegra, perfazendo os requisitos do consentimento;
2. *b) Comprovação de deveres ligados a proteção de dados:* A exemplo, documentar processos de exclusão definitiva de dados, transferência de dados, ou acompanhar procedimentos desta natureza, ressalvados os segredos do negócio;
3. *c) Identificar a robustez de controles e a validade das técnicas de segurança utilizadas:* Avaliação da integridade de logs, controles de acesso, práticas de backup, criptografia e procedimentos de anonimização, dentre outros; Importante destacar que a perícia pode auxiliar a empresa a comprovar que os controles estavam ativos, evitando-se responsabilização judicial por controles falhos ou irregulares. A exemplo, já se decidiu que a utilização de criminosos, por *"logins inativos há mais de um ano"* (Falha no controle de acesso) para acesso a site e roubo de dados, é considerada violação dos protocolos de segurança do site, sendo cabível dano moral e material **[3]**. Por outro lado, a vítima que demora cinco dias para comunicar o incidente de furto de aparelho de celular com realização

de transações bancárias, a partir dos dados e informações obtidas, não faz jus à restituição de valores e indenização por danos **[4].**

4. *d) Identificar quem deu causa a um incidente e o modus operandi:* Nem sempre os incidentes serão causados pelo controlador, mas poderemos ter responsabilidade exclusiva do titular o ou mesmo falha ou exploração de vulnerabilidades em controladores conjuntos, operadores, dentre outros; A perícia pode ajudar a esclarecer como foi explorado o sistema comprometido e se algum agente de tratamento violou instruções lícitas do controlador ou obrigações contratuais e legais. De outra ordem, pode ainda esclarecer a culpa exclusiva do titular de dados ou de terceiros;
5. *e) Investigação cibernética:* Contribuir com o controlador ou demais agentes no apoio a titulares que tiveram dados vazados e na investigação da materialidade e autoria de delitos cibernéticos, possibilitando a estes as medidas jurídicas cabíveis, demonstrando ainda evidencias que a empresa adotou medidas para minimizar os prejuízos, identificar e responsabilizar os ofensores, evitando responsabilizações, inclusive, judiciais. Neste cenário, a justiça já entendeu que serviço online que não checa a ocorrência comunicada e adota medidas rápidas para bloquear o uso indevido e reduzir o prejuízo tem falha no sistema de segurança **[5].**
6. *f) Prova técnica simplificada*: Atuar em nomeações por autoridades de controle e judiciais, no esclarecimento técnico de questões controvertidas ligadas a privacidade e dados pessoais, que não demandem um exame em si, mas um parecer técnico.

Os regulamentos de proteção de dados comumente estabelecem direitos e deveres e quais as medidas devem ser implementadas para a demonstração de aderência. Já o “como fazer” vem estampado em frameworks e melhores práticas, incluindo normas

internacionais, como a recém editada ISO 27701**[6]** que atualiza controles ligados a segurança da informação com a ótica de proteção de dados pessoais (ou privacidade da informação) e traz controles específicos para controladores e operadores de dados pessoais.

Trata-se de boas práticas reconhecidas internacionalmente e que auxiliam na aproximação entre o real estado técnico dos agentes de tratamento e dispositivos e deveres legais e de compliance. A norma aborda, inclusive, a relevância da perícia, especificamente, nos controles de resposta a incidentes, onde prevê a importância do processo de coleta de evidências. Acresça-se ainda a importância de se observar normas ligadas ao processo forense, como a ISO 27037**[7],** que estabelece diretrizes para identificação, coleta, aquisição e preservação de evidência digital.

De fato, compreender o que ocorreu com um sistema comprometido que tratava dados pessoais, *modus operandi* e possíveis responsáveis, além de elucidar a questão, cooperando para o esclarecimento e aprimoramento da segurança da informação e correção das vulnerabilidades encontradas, é tarefa essencial da perícia técnica, que certamente será demandada nos impasses ligados a dados pessoais.

Além disso, é importante notar o papel da perícia no processo administrativo, para fins de possível exclusão da responsabilidade dos agentes de tratamento, quando por meio dela, possa-se provar que os dados vazados não partiram da empresa, que a empresa não realizava o tratamento a ela atribuído ou ainda que o dano foi decorrente de culpa exclusiva do titular de dados e terceiros. Assim, agentes de tratamento envolvidos em processos judiciais ou administrativos de órgãos de defesa do consumidor e proteção de dados, precisam estar amparados por assistente técnico, para produção correta e adequada de provas relevantes para formação do seu contraditório, evitando-se, por intermédio do devido processo legal, penalidades onerosas e outras sanções

que possam até mesmo inviabilizar a atividade do agente de tratamento.

Por fim, impossível não notar o papel fundamental do assistente e da perícia forense digital também no contexto ligado à aplicação e gradação das penalidades, já que as sanções previstas na LGPD deverão considerar diversos critérios, dentre eles, uma importante atenuante pode ser a cooperação do infrator, onde por exemplo, apresenta informações claras no reporte do incidente, que podem se basear em uma investigação preliminar computacional, comprovando ainda a adoção de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, o que sem dúvida envolve o estabelecimento, em um processo resposta a incidentes com dados pessoais, de procedimentos para coleta, preservação e análise de evidências, com o devido reporte e parecer técnico, o que se dará, evidentemente, por meio da prova técnica pericial produzida pelo agente de tratamento envolvido.

Como visto, em um cenário de inversão de ônus de prova e severas sanções por tratamentos irregulares de dados, cabe às empresas e agentes de tratamento se precaverem, não só gerando evidências independentes de conformidade, aplicação de controles de segurança da informação e registros das manifestações de titulares de dados, mas também avaliando periodicamente seus sistemas por consultorias independentes e externas e principalmente, contando com a perícia e auditoria técnica no suporte e assistência em autuações, litígios, controvérsias, processos administrativos, indenizatórios, ou reparatórios, relacionados a possíveis incidentes ou usos irregulares dedados pessoais. Estabelecer, criar e gerir um sistema de gestão de proteção de dados com um processo de resposta a incidentes que contemple a perícia forense digital demonstra-se, pelos fundamentos apresentados, inegavelmente a melhor das práticas.

NOTAS

[1] TJRJ, 2018, Apl. 02417697420158190001

[2] TJSC, Apelação Cível 49235320168240038, Processo 00049235320168240038

[3] TJPR, 2018, Processo 00057547720158160194

[4] TJSE, 2019, Apelação Cível 36072120188250001

[5] TJSP, 2020, Recurso Inominado 10058267420208260006-sp-1005826-7420208260006

[6] https://www.iso.org/standard/71670.html

[7] https://www.abntcatalogo.com.br/norma.aspx?ID=307273

Sobre o Autor: **José Antonio Milagre** é Diretor da CyberExperts, Perito Forense em Informática. Pós-Graduado em Gestão de Tecnologia da Informação. Mestre e Doutor em Ciência da Informação pela UNESP. Diretor do Instituto de Defesa do Cidadão na Internet (IDCI Brasil), coautor de dois livros pela Editora Saraiva (Marco Civil da Internet: Comentários a Lei 12.975/2014 e Manual de Crimes Informáticos). consultor@josemilagre.com.br