“A Intimação do DPO que Nunca Existiu: o surto coletivo dos ‘especialistas’ em LGPD”

O Brasil inteiro falou da “intimação do DPO”. O problema é que poucos leram o processo.

Em questão de horas, o que era um ato regulatório virou narrativa. O que exigia análise virou opinião. E o que deveria ser tratado com rigor técnico acabou se transformando em mais um episódio de reprodução em massa onde muitos comentam, poucos verificam e quase ninguém aprofunda. E se dizem *Especialistas*

Criou-se, assim, um verdadeiro caso: **a intimação que virou um surto nacional na LGPD**.

Não foi um erro isolado. Foi coletivo.

O mercado, mais uma vez, reagiu antes de compreender. Especialistas se apressaram em explicar aquilo que ainda não haviam lido por completo. E, nesse movimento, consolidou-se uma interpretação que não encontra sustentação no próprio processo.

Não foi a ANPD que errou. Foi o mercado que não leu.

E talvez seja exatamente por isso que esse episódio se torna tão emblemático. Porque ele não expôs apenas uma possível não conformidade regulatória **ele expôs o próprio mercado**.

Expôs o quanto ainda se comenta sem análise, se conclui sem evidência e se constrói autoridade sobre percepções frágeis. Expôs um nível de despreparo que não está necessariamente na ausência de conhecimento, mas na superficialidade com que ele é aplicado.

No fim, o que temos não é apenas uma intimação mal interpretada. Temos um retrato claro de um ecossistema que, diante da complexidade, ainda prefere simplificar mesmo que isso custe a própria precisão.

E é justamente sobre isso que precisamos falar.

Nos últimos dias, o mercado de privacidade e proteção de dados foi tomado por uma enxurrada de opiniões apressadas sobre o Edital de Intimação nº 1, de 23 de março de 2026. O que poderia ser uma discussão técnica relevante acabou se transformando em um verdadeiro exercício coletivo de suposições, onde muitos preferiram comentar antes de compreender.

A narrativa que rapidamente ganhou força a de que a Autoridade teria intimado entidades por ausência ou dificuldade de contato com o DPO é, no mínimo, conveniente. Simples, direta e fácil de replicar. Mas completamente desconectada da realidade dos fatos.

A intimação não é pontual. Não é isolada. E, principalmente, não tem como causa a ausência de DPO.

Ela foi encaminhada de forma abrangente. **Todos os clubes foram intimados.**

Isso, por si só, já desmonta a tese amplamente divulgada. Não estamos diante de uma falha individual, mas de uma atuação coordenada da autoridade, com foco claro: **o tratamento de dados pessoais e sua conformidade prática**.

O problema é que, enquanto a autoridade olha para evidência, parte do mercado segue presa à narrativa.

E é justamente nessa desconexão que surgem os maiores absurdos.

Ao analisar algumas das respostas apresentadas, o que se observa não é apenas fragilidade técnica, mas uma tentativa reiterada de contornar a realidade dos fatos por meio de construções argumentativas que não se sustentam. Em alguns casos, chega-se a um nível de contradição que beira o insustentável.

Veja-se, por exemplo, a seguinte linha de defesa: a alegação de que, ***"em decorrência da ausência de previsão legal", não haveria tratamento de dados pessoais de crianças e adolescentes menores de 16 anos.*** A afirmação, por si só, já seria questionável. Mas, quando confrontada com a realidade a presença física desses menores nos estádios, o acesso a sistemas, o vínculo com responsáveis, o registro de informações ela simplesmente colapsa.

A provocação é inevitável: afinal, estamos falando de pessoas ou de "*entidades invisíveis*"? Porque, se não há tratamento de dados, então, por lógica, teríamos que admitir a existência de verdadeiros ***"espíritos torcendo nos estádios".***

A ironia escancara o problema: negar o tratamento não elimina o fato. Apenas evidencia a ausência de compreensão sobre ele.

E esse não é um caso isolado. Em outra frente, observa-se a tentativa de sustentar a conformidade por meio de cláusulas contratuais com terceiros, especialmente no que diz respeito a indenizações por eventuais falhas. A lógica parece simples: se houver erro, alguém paga por ele. Mas essa visão revela uma distorção perigosa sobre o próprio objetivo da regulação.

Indenizações contratuais podem até proteger o caixa do controlador. Mas não protegem o titular.

Partir do pressuposto de que operadores terão capacidade financeira equivalente para absorver riscos ignora uma realidade básica do mercado: **nem todos os operadores possuem a mesma estrutura, a mesma receita ou a mesma capacidade de resposta**. E mais do que isso, ignora o ponto central da LGPD que nunca foi garantir ressarcimento financeiro, mas sim assegurar direitos.

Contratos com terceiros, por mais robustos que sejam, não garantem tratamento adequado de dados. Não garantem governança. E, definitivamente, não substituem a responsabilidade do controlador.

A atuação da autoridade, inclusive, deixa isso ainda mais evidente ao trazer esses terceiros para dentro da análise, sem, em momento algum, retirar do controlador o protagonismo da responsabilidade e, ao mesmo tempo, acendendo um alerta silencioso para o mercado: **há uma quantidade relevante de operadores atuando sem qualquer nível real de adequação**.

E aqui está um ponto que muitos ainda não perceberam. Durante anos, consolidou-se a ideia de que o controlador deveria "cobrar" adequação do operador, enquanto muitos operadores se posicionaram como se estivessem à margem da obrigação regulatória, amparados na falsa premissa de que a responsabilidade seria sempre de quem contrata.

Essa atuação da autoridade muda o jogo.

Ela demonstra que o operador pode até sustentar um discurso de conformidade para o controlador pode, inclusive, omitir fragilidades, mas diante da autoridade, isso não se sustenta. **Você pode até tentar parecer adequado para o mercado. Para a autoridade, não.**

E mais: uma falha do controlador pode expor, em cadeia, toda a fragilidade do ecossistema de terceiros envolvido.

*O risco de hoje não é apenas contratar um fornecedor inadequado. É **ser** um fornecedor inadequado.*

Outro ponto que merece destaque é a insistência em tratar o Relatório de Impacto à Proteção de Dados como um *documento reativo*, algo a ser produzido apenas quando solicitado. Essa visão inverte completamente a lógica da proteção de dados.

O RIPD não é uma resposta à fiscalização. Ele é uma ferramenta de prevenção. Mas vai além: **ele é, na prática, uma declaração técnica de responsabilidade sobre o tratamento realizado**.

E aqui reside um dos maiores paradoxos da LGPD.

Ao **fazer** o RIPD, a organização se expõe porque documenta riscos, decisões e eventuais fragilidades. Ao *não fazer*, também se expõe porque evidencia que sequer avaliou o risco.

Ou seja: o RIPD sempre "entrega". Fazendo ou não fazendo.

A diferença é simples: quando feito corretamente, ele demonstra governança. quando inexistente ou improvisado, ele evidencia negligência.

Não por acaso, muitas das respostas apresentadas acabam reforçando a percepção de não conformidade. Há uma aparente crença de que uma *boa argumentação jurídica*, bem redigida e cuidadosamente estruturada, seja capaz de substituir a ausência de evidência técnica. Como se fosse possível convencer a autoridade pela forma, mesmo quando o conteúdo não se sustenta.

Na prática, ocorreu exatamente o oposto.

Cada argumento apresentado acabou expondo ainda mais a falha no tratamento. Cada tentativa de justificar revelou a ausência de algo que deveria já existir.

Porque há um ponto inegociável nesse cenário: não existe argumento capaz de substituir um documento que deveria ter sido produzido antes do tratamento de dados.

Não existe justificativa plausível para pedir prazo de algo que já deveria estar pronto. Não existe retórica que substitua evidência.

O que se esperava era simples: **entregar o que já deveria existir.**

Mas, ao invés disso, optou-se por explicar o que nunca foi feito.

E talvez seja justamente esse o ponto que ainda não foi plenamente compreendido por parte do mercado: **não existe "meia adequação" em proteção de dados**. Não há espaço para conformidade parcial, para ajustes futuros ou para justificativas baseadas em intenção.

Ou a organização conhece o seu tratamento de dados, ou não conhece. Ou reconhece os riscos, ou os ignora. Ou está adequada, ou está exposta.

No fim, o que esse episódio revela vai muito além da atuação da autoridade. Ele expõe um problema de maturidade no próprio ecossistema de privacidade e proteção de dados. A velocidade com que análises superficiais foram produzidas e disseminadas mostra que muitos ainda operam no campo da opinião, e não da análise técnica.

Não se trata de falta de informação. Trata-se de falta de profundidade.

E, em um ambiente regulado, essa diferença é tudo.

Porque, quando especialistas deixam de acompanhar os fatos para seguir a narrativa, o risco deixa de ser apenas jurídico ou regulatório. Ele passa a ser também reputacional e, sobretudo, intelectual.

E talvez o maior alerta desse caso seja exatamente esse: **o problema nunca foi a intimação. Foi a interpretação equivocada dela.**

Mas é igualmente necessário fazer um registro final, para que não haja qualquer distorção: **não se trata de diminuir a relevância dessa atuação muito pelo contrário**.

O que está em curso é um movimento claro de amadurecimento regulatório. A autoridade vem sinalizando, de forma cada vez mais incisiva, novas exigências, aprofundando o olhar sobre não conformidades, tratamento inadequado de dados e, principalmente, ampliando o alcance da responsabilização ao longo de toda a cadeia.

A inclusão efetiva de operadores no centro das análises, a exposição das fragilidades na relação com terceiros e a admissão de participação de terceiros interessados nos processos são elementos que, até pouco tempo atrás, não apareciam com esse nível de clareza e intensidade.

Isso não é detalhe. Isso muda o jogo.

E talvez o maior risco, neste momento, não seja a atuação da autoridade em si mas a incapacidade de parte do mercado de compreender, com a profundidade necessária, o que ela está realmente dizendo.

Wendel Babilon
Escritor, Auditor e Consultor Especializado em Privacidade e Proteção de Dados