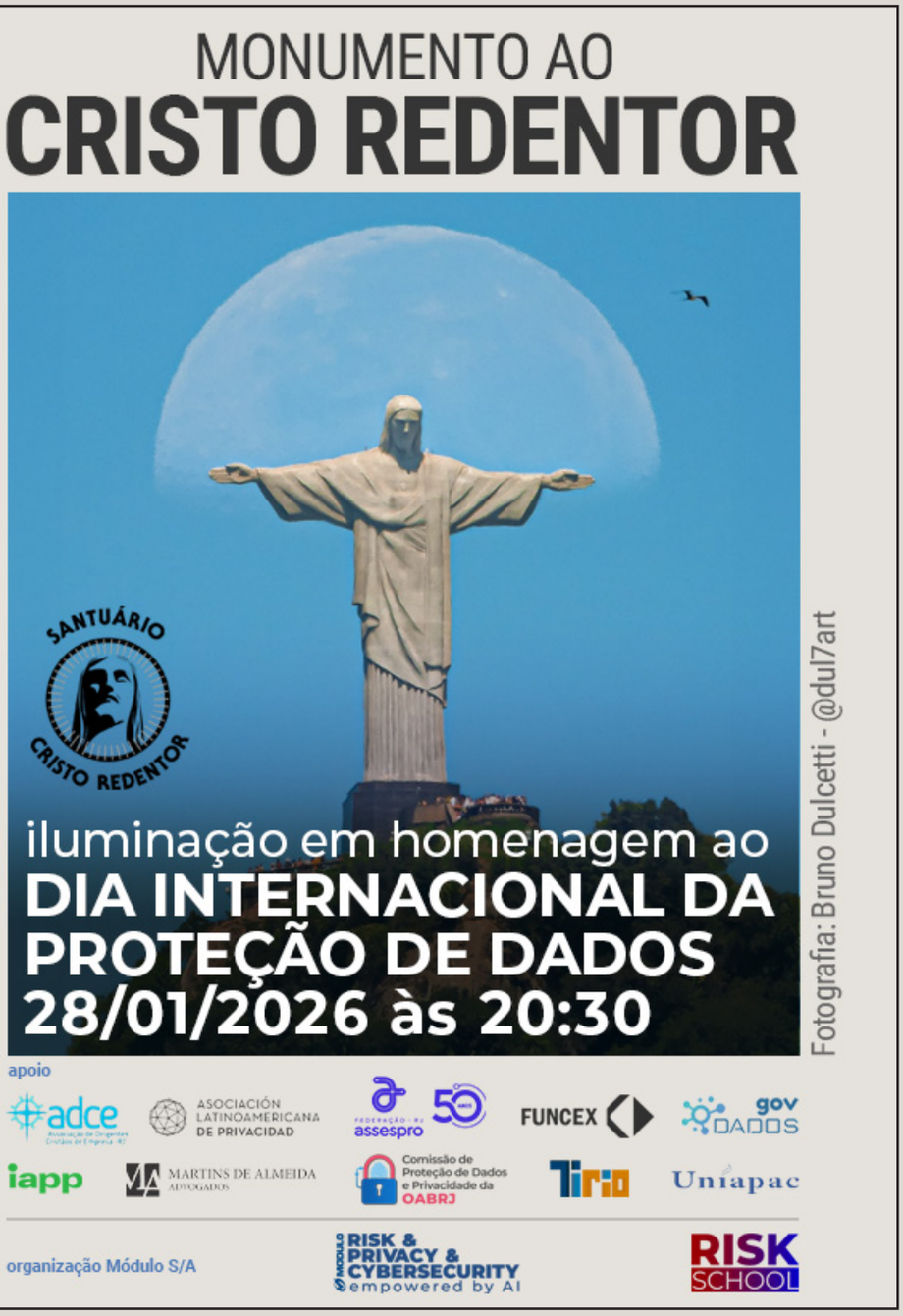
LGPD em Ação

artigos em comemoração ao
dia internacional da proteção de dados



Evento no Cristo Redentor reforça o Dia Internacional da Proteção de Dados com lançamento de eBook

No próximo dia 28 de janeiro, o Santuário Arquidiocesano Cristo Redentor realiza mais uma edição do evento em celebração ao Dia Internacional da Proteção de Dados, em parceria com o Núcleo de Segurança e Proteção de Dados e a Módulo Security. A iniciativa reforça o compromisso com a conscientização sobre a proteção de dados pessoais e a aplicação da Lei Geral de Proteção de Dados (LGPD) no Brasil.

A programação deste ano inclui o lançamento do eBook LGPD em ação, publicação digital que reúne contribuições de apoiadores, sobre como a proteção de dados pessoais e a LGPD são vividas em diferentes contextos organizacionais, setoriais e profissionais. O material busca aproximar o tema da prática cotidiana, com foco em aprendizados, desafios e pontos de atenção, e ficará disponível para divulgação ao longo de 2026.

A cerimônia terá início às 20h30, com a presença de representantes de instituições e especialistas ligados à agenda de proteção de dados no país. Ao final do evento, o monumento ao Cristo Redentor será novamente iluminado em azul, gesto simbólico que destaca a relevância da privacidade e do uso responsável de dados pessoais.
Ao associar um símbolo reconhecido mundialmente a uma agenda contemporânea de interesse público, o Santuário Cristo Redentor reafirma seu papel como espaço de reflexão, diálogo e mobilização sobre temas que impactam diretamente a sociedade.

SERVIÇO:

Evento e Iluminação do Cristo Redentor pelo Dia Internacional da Proteção de Dados
Data: 28 de janeiro de 2026
Horário: 20h30

apoio

ÍNDICE

Cândida Diana Terra

Advogada e Presidente da Comissão de
Proteção de Dados e Privacidade da OAB-RJ

Iluminar a privacidade: um dever coletivo com o presente e com o futuro

Durante muito tempo, a privacidade foi tratada como um tema secundário, quase um luxo reservado a quem tinha algo a esconder. No imaginário coletivo, falar em proteção de dados parecia distante da vida real, restrito a especialistas em tecnologia, grandes empresas ou debates acadêmicos. Esse tempo acabou. A privacidade deixou de ser uma abstração e passou a ocupar o centro das relações sociais, econômicas e institucionais.

Vivemos em uma sociedade profundamente orientada por dados. Cada ação cotidiana — uma compra online, um cadastro em um aplicativo, uma consulta médica, um acesso a serviço público, uma simples navegação na internet — gera rastros, perfis e inferências. Dados pessoais tornaram-se ativos valiosos, capazes de definir oportunidades, limitar direitos, influenciar decisões e, em situações extremas, produzir exclusões silenciosas. Iluminar a privacidade, portanto, é uma exigência democrática.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) representou um marco civilizatório ao reconhecer que o tratamento de dados deve respeitar direitos fundamentais, como a liberdade, a dignidade e o livre desenvolvimento da personalidade. Mais recentemente, a proteção de dados foi alçada à condição de direito fundamental pela Constituição. Ainda assim, o desafio permanece: normas existem, mas a cultura da privacidade ainda não se consolidou.

É aqui que o papel da sociedade se torna decisivo. Não basta que empresas estejam “em conformidade” formal com a lei, nem que o poder público publique regulamentos. A proteção de dados só se sustenta quando os titulares — cidadãos, consumidores, trabalhadores,

estudantes — compreendem seus direitos e sabem reconhecê-los no dia a dia. Transparência, consentimento, finalidade, segurança e responsabilização não são conceitos técnicos: são instrumentos de cidadania.

A ausência de informação cria um ambiente propício a abusos normalizados. Vazamentos são tratados como fatalidades. Coletas excessivas de dados passam despercebidas. Perfis automatizados decidem sem explicação. A sociedade se acostuma a entregar seus dados em troca de conveniência, sem questionar quem coleta, por que coleta, por quanto tempo armazena e com quem compartilha. Iluminar a questão da privacidade é romper com essa naturalização.

Nesse contexto, as instituições e a advocacia exercem papel estratégico. A Ordem dos Advogados do Brasil sempre esteve na linha de frente da defesa do Estado Democrático de Direito, dos direitos fundamentais e das liberdades civis. A agenda da privacidade se insere, de forma inequívoca, nessa tradição histórica.

A Ordem dos Advogados do Brasil – Seção Rio de Janeiro, por meio da Comissão de Proteção de Dados e Privacidade da OAB-RJ, tem atuado justamente para iluminar esse debate, aproximando o tema da realidade social, institucional e econômica do Estado do Rio de Janeiro. O objetivo não é apenas discutir a LGPD sob o viés normativo, mas promover uma verdadeira mudança cultural.

A Comissão atua como espaço plural de diálogo entre advocacia, setor público, iniciativa privada, academia e sociedade civil. Promove eventos, cursos, debates e publicações voltados à disseminação do conhecimento, à qualificação técnica dos profissionais e à conscientização da população. Ao fazer isso, contribui para reduzir assimetrias de informação e fortalecer a noção de que privacidade não é obstáculo à inovação, mas condição para um desenvolvimento tecnológico ético e sustentável.

Outro eixo fundamental da atuação da Comissão é o estímulo à governança responsável. Empresas e instituições públicas precisam compreender que proteger dados não é apenas cumprir uma obrigação

legal, mas assumir um compromisso com a confiança social. A Comissão contribui ao orientar boas práticas, fomentar o debate sobre riscos, incentivar a prevenção de incidentes e reforçar a importância da responsabilização.

Iluminar a questão da privacidade é, em última análise, reconhecer que dados pessoais dizem respeito a pessoas reais, com histórias, vulnerabilidades e direitos.

É compreender que a proteção de dados não se resume a documentos ou políticas, mas se manifesta nas escolhas diárias de organizações e indivíduos.

Iluminar a privacidade é um dever coletivo. É um compromisso com o presente e, sobretudo, com o futuro.

Alberto Blois

Presidente do TI Rio

LGPD: Governança, pessoas e maturidade no ecossistema de TI do Rio de Janeiro

Falar de proteção de dados no setor de tecnologia não é falar de exceção, é falar de regra. No ecossistema de TI do Estado do Rio de Janeiro, a Lei Geral de Proteção de Dados deixou de ser apenas um requisito legal e passou a se consolidar como um elemento estruturante da gestão, da governança e da relação entre empresas, profissionais, clientes e a sociedade.

Do ponto de vista do TI Rio, que representa um ecossistema diverso, formado majoritariamente por pequenas e médias empresas, a LGPD se materializa no cotidiano muito mais como um processo contínuo de amadurecimento do que como um projeto com começo, meio e fim. Não se trata apenas de adequação documental, mas de uma mudança cultural, de um compromisso que atravessa decisões técnicas, práticas de RH, modelos de negócio e a forma como a tecnologia é concebida e entregue.

Na prática, um dos primeiros aprendizados do setor foi compreender que proteção de dados não é um tema exclusivo da área jurídica ou de compliance. Ela começa no desenho dos sistemas, passa pela arquitetura da informação, pela segurança, pela governança de dados e chega até ao relacionamento com colaboradores e clientes. Para empresas de TI, isso significa assumir que cada solução desenvolvida, cada contrato firmado e cada integração realizada carrega também responsabilidades sobre dados pessoais.

Um desafio recorrente no ecossistema é equilibrar a necessidade de agilidade, típica de empresas enxutas e inovadoras, com a disciplina exigida pela LGPD. Muitas organizações operam com equipes pequenas, múltiplos projetos simultâneos e recursos limitados. Nesse contexto, a

tentação de tratar a proteção de dados como algo secundário é real. No entanto, a experiência mostra que, quando a LGPD é incorporada desde o início dos processos, ela deixa de ser um custo adicional e passa a funcionar como um fator de redução de riscos e aumento de previsibilidade.

Outro ponto central é a relação entre LGPD e pessoas. A proteção de dados não diz respeito apenas a clientes e usuários finais, mas também aos próprios colaboradores. Informações de RH, dados sensíveis, processos de recrutamento, avaliação e desenvolvimento exigem cuidado redobrado. No ecossistema de TI do Rio, onde a disputa por talentos é intensa e a rotatividade existe, tratar dados pessoais com transparência e responsabilidade fortalece a confiança interna e contribui para ambientes de trabalho mais saudáveis e maduros.

A experiência coletiva do setor também evidencia que a LGPD funciona como um catalisador de boas práticas. Empresas que avançaram na organização de seus dados passaram a ter mais clareza sobre seus processos, maior controle sobre fluxos de informação e melhores condições para escalar operações. Governança de dados, segurança da informação e conformidade regulatória deixam de ser ilhas e passam a integrar uma visão mais ampla de gestão.

Há ainda um aspecto estratégico relevante: a LGPD como elemento de competitividade. Cada vez mais, clientes públicos e privados exigem comprovações mínimas de maturidade em proteção de dados. Para as empresas de TI do Rio de Janeiro, estar preparado não é apenas cumprir a lei, mas viabilizar negócios, participar de cadeias mais complexas e acessar mercados mais exigentes. Nesse cenário, passamos a dispor de um diagnóstico que permite às empresas compreender melhor seu estágio de maturidade e engajamento em proteção de dados.

É importante destacar que o aprendizado é contínuo. Novas tecnologias, como inteligência artificial, análise avançada de dados e automação, ampliam exponencialmente os desafios. No setor de TI, onde a inovação é permanente, a LGPD funciona como um marco de responsabilidade, lembrando que nem tudo o que é tecnicamente possível é socialmente aceitável.

Acreditamos que o principal ponto de atenção para os próximos anos é evitar que a LGPD seja tratada como um tema resolvido. A lei não é estática, assim como não são estáticos os modelos de negócio, as tecnologias e as relações de trabalho. Manter a proteção de dados como pauta viva, integrada à estratégia e à cultura organizacional, é um desafio coletivo.

No ecossistema de TI do Rio de Janeiro, a LGPD já está em ação. Como aprendizado, como prática e como parte do processo de amadurecimento de um setor que entende que tecnologia e responsabilidade caminham juntas.

Dr. Gilberto Martins de Almeida

Sócio-fundador na Martins de Almeida Advogados

Como simplificar a convivência com a LGPD?

Simplicidade: sinônimo de economia, agilidade, boa comunicação e imagem.

LGPD: sinônimo de tamanha novidade e complexidade, que fez as instituições criarem política corporativa e equipe interna específicas, formando grande “ilha”.

Esse isolamento faz que hoje as organizações se perguntem: em questões da LGPD sobre segurança, se deve aplicar a PSI (Política de Segurança da Informação), ou incluir regras de segurança na PPDP (Política de Proteção de Dados Pessoais)?

Multiplique-se isso pelo número de itens que a LGPD também cobre (propriedade intelectual, contratos, compliance, governança, etc.), e aí temos o atual panorama de redundâncias e inconsistências. Como então sair desse “imbróglio” paralisante?

Resposta: focando em um denominador comum, para assegurar consolidação, integração, racionalização e coerência. Qual? Gestão de Riscos, que a LGPD prestigia expressamente, além de ser uma técnica e pauta comum a vários temas.

Então, se incluirmos a LGPD na matriz de riscos da organização, teremos norteador e passo inicial “nativo” e prático para consolidar, simplificando em geral.

Chegou a hora de investirmos na “arquitetura”, mais do que seguir empilhando tijolos. A consolidação simplificadora (da matriz de riscos e das políticas internas) torna a LGPD parceira catalisadora em vez de um complexo corpo estranho.

Por Federação Assespro-RJ

Tradição e Futuro: A Jornada da Federação Assespro-RJ na Cultura de Proteção de Dados

Em 2026, a Federação Assespro-RJ alcançará um marco histórico: completaremos meio século de atuação com o pioneirismo de ser a primeira e mais antiga associação de empresas de tecnologia do Brasil. Nossa missão sempre foi atuar como a voz legítima do setor, fomentando negócios e prosperidade por meio de articulação política robusta, eventos estratégicos de alto nível e um apoio constante às demandas dos nossos associados.

Diferente de organizações que já nasceram na era da nuvem, gerir uma entidade com décadas de história significa lidar com um lastro de informações e processos consolidados muito antes da internet se tornar onipresente. Sabíamos que ajustar 50 anos de cultura organizacional a um novo cenário regulatório, onde a privacidade deixa de ser um acessório para se tornar um pilar estratégico, não seria um mero detalhe operacional. Era necessário uma mudança de mindset.

Essa adaptação, que já estava em nosso radar, ganhou contornos de urgência crítica com o advento da pandemia, entre 2020 e 2022. Enquanto o lockdown limitou portas físicas, ele propulsionou uma migração maciça e imediata para o ambiente online. Reuniões, eventos, tratativas políticas e a própria gestão da entidade passaram a ocorrer em bits e bytes da noite para o dia. Nesse cenário, a conformidade deixou de ser uma meta de médio prazo para se tornar um imperativo de sobrevivência e reputação.

A Federação Assespro-RJ contou com a expertise da Módulo Security para fazer uma transição, adequação e revisão de nossos processos estruturais e assegurar a conformidade total com a LGPD em um período de grande incerteza global. Tivemos que vencer a resistência natural à mudança e provar que a segurança não é um freio para a inovação, mas sim o asfalto que permite que ela corra mais rápido. Esse foi o nosso grande divisor de águas.

O que à primeira vista poderia parecer um excesso de burocracia, na verdade, trouxe benefícios tangíveis e inesperados. O processo de adequação forçou uma organização interna (“arrumar a casa”) que, ironicamente, facilitou o acesso ao nosso próprio histórico. Ao catalogar e proteger os dados para cumprir a lei, ganhamos agilidade na busca por informações estratégicas.

Mas o maior ganho foi imaterial: fortalecemos a confiança. O associado sabe que, ao interagir com a Federação, seus dados são tratados com o respeito e a segurança que a nossa posição de liderança exige.

Olhando para o futuro, a Federação Assespro-RJ mantém o foco nas tendências que unem Inteligência Artificial e Segurança da Informação. Vivemos um momento onde a IA pode ser usada tanto para criar ameaças cibernéticas mais sofisticadas quanto para blindar sistemas de forma preditiva.

Nessa convergência digital entre IA e Cyber, reconhecemos uma verdade fundamental: a tecnologia mais avançada ainda depende de quem a opera ou configura. O “elo mais fraco” continua sendo — e sempre será — o humano.

Por isso, insistimos que a cultura corporativa e a educação contínua são as verdadeiras barreiras de proteção. Firewalls e criptografia são essenciais, mas é a consciência de cada colaborador e parceiro que define a integridade dos dados.

Este é um processo contínuo e que evolui rapidamente. E ninguém faz isso sozinho. Acreditamos que unir forças, somar experiências e compartilhar aprendizados práticos é o único caminho para construir um ambiente de inovação que seja, ao mesmo tempo, próspero e seguro para todos.

Por Uniapac Adce'Rio

O apoio na tradição da comemoração do Dia Mundial da Proteção de Dados e Privacidade no Cristo Redentor

A UNIAPAC- International Christian Union of Business Executives (União Cristã Internacional de Dirigentes de Empresas) é uma organização ecumênica com sede em Paris, presidida pela alemã Sigrid Marz, tendo como Secretário Geral, o chileno Rodrigo Whitelaw.

Nascida na Bélgica em 1931, a UNIAPAC reúne hoje associações de líderes empresariais cristãos de 40 países na Europa, América Latina, África e Ásia, defendendo uma economia baseada no respeito pela dignidade da pessoa humana e no sentido do bem comum, bem como a promoção dos negócios como uma nobre vocação.

Impulsiona ao redor do mundo, um universo de aproximadamente cinquenta mil empresários e empreendedores com o propósito de unir, orientar e inspirar líderes empresariais para que, à luz do Pensamento Social Cristão, se comprometam com a transformação de suas empresas e do ambiente de seus negócios, contribuam para a construção de uma sociedade mais justa e humana.

A Uniapac Adce' Brasil está estabelecida em treze estados, sob a presidência do empresário Sergio Cavalieri, filho de um dos fundadores do movimento brasileiro da evangelização no ambiente do trabalho.

No Rio de Janeiro, Elmair Neto, preside a Uniapac Adce'Rio, que em 2025, completou 63 anos, tendo o dia da sua fundação, em 03 de agosto, incluída no Calendário Oficial da cidade do Rio de Janeiro, por iniciativa do Presidente da Câmara Municipal, Vereador Carlo Caiado, sancionada pelo Prefeito Eduardo Paes, também recebendo Menção de Reconhecimento e Aplauso da Assembleia Legislativa do Estado do Rio de Janeiro, por iniciativa do Deputado Estadual Claudio Caiado.

O Dia Internacional da Proteção de Dados é uma importante data para lembrarmos da relevância da privacidade e a segurança dos nossos dados pessoais. Pelo terceiro ano consecutivo, a Uniapac Adce' Rio apoia a comemoração dessa data, uma tradição que se estabelece desde 1981, quando assinada a Convenção 108 do Conselho da Europa, o primeiro tratado internacional sobre proteção de dados, que elenca as diretrizes para a proteção dos dados pessoais, assim garantindo a privacidade dos cidadãos.

Essa iniciativa influenciou legislações globalmente, permitindo a criação no Brasil, da Lei Geral de Proteção de Dados.

Com o aumento dos vazamentos de dados e ataques cibernéticos, é essencial adotar medidas de segurança eficazes e os empresários e empreendedores, cada vez mais em suas empresas, procuram fortalecer políticas de governança de dados, investimentos em criptografia e autenticações reforçadas e gradativa capacitação dos seus colaboradores nesse olhar.

Dentre os nossos associados na Associação de Dirigentes Cristãos de Empresa do Rio de Janeiro, há vários especialistas no tema da LGPD, que em unidade, colaboram para o estabelecimento de diretrizes para o bom uso e proteção das informações pessoais e a segurança da informação, que de forma ampla, é um compromisso contínuo para empresas, indivíduos e governanças.

A Uniapac Adce' Rio parabeniza a Módulo e Risk School pela tradição dessa iniciativa!

Fabrício da Mota Alves

Presidente - GovDADOS

Léo Farias

Encarregado pelo Tratamento de Dados Pessoais - GovDADOS

Da origem do Dia da Proteção de Dados ao desafio contemporâneo da biometria

O Dia Internacional da Proteção de Dados, celebrado em 28 de janeiro, não nasceu como uma data simbólica ou comemorativa no sentido superficial do termo. Ele marca a abertura, em 1981, da Convenção 108 do Conselho da Europa, o primeiro tratado internacional juridicamente vinculante voltado à proteção de dados pessoais. À época, o debate ainda era incipiente, mas já havia uma percepção clara: a informatização crescente da sociedade alteraria de forma profunda a relação entre indivíduos, Estado e mercado. O risco não estava apenas no uso indevido de dados, mas na transformação estrutural do próprio poder informacional.

Naquele contexto histórico, o debate concentrava-se sobretudo em grandes bases administrativas e censos populacionais ainda limitados em escala e capacidade analítica. Ainda assim, já se afirmava um entendimento essencial: proteger dados pessoais significava proteger pessoas, e não apenas regular fluxos de informação. A preocupação central não era criar barreiras artificiais à inovação tecnológica, mas reconhecer que a informatização poderia, de forma gradual, corroer direitos fundamentais, caso não fosse acompanhada de limites jurídicos adequados.

Desde então, o cenário mudou radicalmente. A digitalização tornou-se ubíqua e a inteligência artificial passou a desempenhar papel central na tomada de decisões. É nesse ponto que o debate sobre biometria ganha centralidade, representando uma inflexão qualitativa na história da proteção de dados. Diferentemente de identificadores tradicionais, a biometria se ancora em características físicas intrinsecamente ligadas

ao corpo humano, funcionando como extensões diretas da identidade da pessoa.

Essa natureza sensível da biometria encontra um ponto de ajuste necessário quando confrontada com as vulnerabilidades sistêmicas do ambiente digital contemporâneo. No cenário brasileiro, a proteção de dados dialoga diretamente com uma necessidade imperativa de segurança. A fragilidade estrutural da segurança cibernética no país é um dado estatístico alarmante: o Brasil registrou 314,8 bilhões de tentativas de ataques cibernéticos em 2024, liderando o ranking de atividades maliciosas na América Latina. Além disso, o país consolidou-se como o segundo que mais sofre com crimes cibernéticos no mundo, com aproximadamente 700 milhões de ocorrências anuais.

Essa realidade de vulnerabilidade extrema impõe uma ponderação contextual de riscos, na qual a biometria deixa de ser uma escolha meramente tecnológica para se tornar uma salvaguarda essencial. Diante da obsolescência de senhas e métodos tradicionais de autenticação frente ao aumento exponencial nas fraudes com deepfakes e identidades sintéticas entre 2024 e 2025, a biometria emerge como o mecanismo prioritário para garantir a fidedignidade das interações. Ela atua como a resposta técnica a uma falha estrutural de segurança, viabilizando a confiança necessária para o exercício da cidadania digital e o acesso a serviços essenciais.

Essa transição da teoria para o pragmatismo regulatório encontra um paralelo histórico e consolidado no ordenamento nacional, notadamente na Justiça do Trabalho. O Tribunal Superior do Trabalho (TST), por meio da Súmula 338, estabeleceu que o ônus da prova da jornada de trabalho é do empregador, o que impulsionou a adoção de tecnologias de registro fidedignas. Recentemente, no Tema Repetitivo 136, o Tribunal reforçou que a validade do registro de ponto eletrônico - incluindo o biométrico - prescinde da assinatura do empregado, dada a presunção de veracidade e a integridade técnica do sistema. Nesse contexto, o Judiciário realizou uma ponderação de valores: em nome de uma proteção maior aos direitos do trabalhador e da integridade da prova, a fidedignidade do registro biométrico foi priorizada como mecanismo antifraude.

O exemplo demonstra como o Direito se adapta às necessidades concretas de segurança, utilizando a tecnologia não para suprimir direitos, mas para preservar a justiça e a veracidade das relações laborais. Embora a citada construção jurisprudencial ainda precise ser plenamente harmonizada com o novo paradigma instituído pela Lei Geral de Proteção de Dados Pessoais (LGPD) e pela Emenda Constitucional nº 115, o exemplo permanece como um norte valioso, ilustrando que a proteção de dados não deve ser um obstáculo intransponível, mas um parâmetro para o uso responsável e necessário da tecnologia.

O desafio contemporâneo, portanto, não é o antagonismo entre privacidade e inovação, mas a implementação de uma governança rigorosa que permita o uso da biometria de forma proporcional, segura e fidedigna. O Dia da Proteção de Dados, portanto, permanece atual por sua função crítica. Ele nos lembra que esse direito fundamental também nos convoca a uma prática construtiva e realista.

Se há uma lição que atravessa as décadas desde 1981 até os desafios atuais, é esta: eficiência, segurança e inovação podem e devem coexistir com a autonomia individual.

A biometria possui usos legítimos e fundamentais para a estabilidade do mercado e a segurança do cidadão, desde que sua adoção seja pautada pela transparência e pela centralidade dos direitos fundamentais. Proteger dados, hoje como ontem, é proteger a dignidade da pessoa em um mundo cada vez mais orientado por sistemas automatizados. Esse continua sendo o verdadeiro sentido do Dia da Privacidade, agora reafirmado pela necessidade de um ambiente digital íntegro, seguro e fidedigno.

Fernando Nery

Sócio-fundador na Módulo Security Solutions

LGPD e o crescente apetite por dados pessoais

Há seis anos, o Santuário do Cristo Redentor homenageia o Dia Internacional da Proteção de Dados, iluminando o Monumento do Cristo Redentor com cores especiais. Este evento seria suficiente para mostrar a relevância do tema e sua evolução constante.

A evolução da tecnologia, em especial, o comércio eletrônico, as redes sociais e os smartphones, fizeram com que o dado pessoal passasse a ganhar valor no mercado. Há vinte anos, o matemático Clive Humby cunhou a frase “dados são o novo petróleo”, referindo-se não somente ao valor econômico mas também à necessidade de refiná-lo, uma vez que, em estado bruto, praticamente não tem utilidade. À época, o matemático também destacou questões como o lixo digital, e a necessidade do uso eficiente.

Em 2017, a revista The Economist e publicou a matéria “The world’s most valuable resource is no longer oil, but data”, que popularizou a frase.

Passados quase 20 anos, os dados ganharam ainda mais valor, e somente são comparados ao petróleo em frases nostálgicas. A evolução da tecnologia, as bandas de comunicação maiores, os equipamentos cada vez mais portáteis e poderosos, o armazenamento barato, os meios de pagamento mais ágeis, e a popularização da inteligência artificial, fizeram com que os dados crescessem significativamente de valor.

Não bastasse tudo isso, os dados pessoais passaram a ser cobiçados para a execução de fraudes e crimes tanto no mundo real como no digital.

Por outro lado, a regulamentação do uso de dados pessoais também está aumentando, e focada em proteger o titular dos dados, tanto a LGPD como o Projeto de Lei 2.308/23 destacam em seus artigos

primeiro que seu objetivo é defender os direitos fundamentais. Ou seja, a regulamentação visa defender as pessoas do avanço descontrolado da tecnologia.

Focando o cabo de guerra entre a proteção de dados pessoais, provido pela legislação e regulamentação, e o crescente valor de dados pessoais de todos os tipos (identificações, fotos, dados de saúde, consumo, financeiros, senhas, e muitos outros), o resultado é que no dia a dia, o apetite pelos dados pessoais está aumentando, e muitas vezes, paradoxalmente, a dita conformidade com a LGPD transforma-se em uma licença para coletar dados pessoais. Veja alguns exemplos:

Em boa parte de sistemas nas grandes cidades, para utilizar o transporte público, é necessário um cartão, cuja adesão corresponde a fornecer dados pessoais como nome, cpf, endereço, foto, e-mail, número do celular e cartão de crédito, além de autorizar a instalação de um app, que pede acesso ao GPS e à autenticação biométrica. Moderno. Não seriam dados demais?

Se o cidadão resolver não utilizar o transporte público por achar muito invasivo, e resolver andar a pé, ele será monitorado em seu caminho por centenas de câmeras de condomínios, comércios, órgãos públicos, circuitos de segurança, drones, transeuntes, e outros. A câmera não vem sozinha, uma vez a imagem capturada, a imagem é armazenada em algum lugar, e muitas vezes é avaliada com inteligência artificial.

Estes exemplos visíveis são superados em muito pelos tratamentos de nossos dados realizados em diferentes locais, e que ficamos sem saber. Há décadas, nossos dados são coletados, armazenados, integrados e correlacionados, e é incontável o número destas bases de dados.

Nesta situação, a legislação e a regulamentação são nossos protetores, as organizações precisam, além de estarem em conformidade com a LGPD, engajar seus colaboradores e educarem seus mercados, de forma a aumentar a cultura e a capacidade crítica dos cidadãos de maneira a, independentemente da evolução dos recursos tecnológicos, os dados pessoais de cada um estejam cada vez mais protegidos. Não é fácil resolver a equação que envolve a evolução tecnológica, o aumento das fraudes com dados pessoais, o crescente apetite por dados pessoais, e o aperto regulatório. Cada um deve fazer a sua parte.

Mauro Mallet

Coordenador do núcleo de segurança e proteção de dados do santuário Cristo Redentor

Proteção de dados como expressão de cuidado em espaços de fé e interesse público

A proteção de dados pessoais costuma ser tratada como um tema associado à tecnologia, ao mercado e às relações de consumo. No entanto, há contextos em que o tratamento de dados assume uma dimensão ainda mais sensível, por envolver confiança, valores simbólicos e aspectos profundos da experiência humana. Espaços de fé, cultura e relevância pública estão entre esses contextos.

O Santuário Arquidiocesano Cristo Redentor recebe, anualmente, cerca de dois milhões de visitantes de diferentes origens, culturas e realidades sociais. Além da visitação turística, o local é cenário de celebrações religiosas, eventos de cunho social, iniciativas de interesse cívico e atividades de utilidade pública. Em todos esses contextos, dados pessoais são tratados de forma legítima e necessária, seja por meio de formulários, comunicações institucionais, registros digitais, imagens ou informações que, muitas vezes, tocam dimensões sensíveis da identidade e da crença das pessoas.

Nesse ambiente, proteger dados pessoais não se resume ao atendimento formal às exigências da Lei Geral de Proteção de Dados. Trata-se de um dever de cuidado institucional. É reconhecer que cada dado tratado corresponde a uma pessoa real, que deposita confiança em uma instituição que simboliza acolhimento, espiritualidade e respeito à dignidade humana.

A atuação do Núcleo de Segurança e Proteção de Dados do Santuário parte desse entendimento. A proteção de dados não é tratada como um tema isolado ou meramente técnico, mas como parte integrante da governança institucional. Ela se reflete na organização dos ambientes digitais, na segurança dos sites institucionais, na gestão responsável das

contas e arquivos em nuvem, na definição criteriosa das bases legais para o tratamento de dados e na adoção de avisos de privacidade e termos adequados nos formulários utilizados pelo Santuário.

Essas escolhas não são orientadas por excesso de formalismo, mas por coerência entre valores e práticas. Em um espaço de alta visibilidade e simbolismo, cada decisão relacionada ao uso da tecnologia comunica, de forma direta ou indireta, o compromisso institucional com a confiança, a transparência e o respeito às pessoas.

Há também um aspecto pedagógico implícito nesse processo. Ao adotar práticas responsáveis de proteção de dados, o Santuário contribui para a consolidação de uma cultura de privacidade, demonstrando que esse direito fundamental não se limita a ambientes corporativos ou governamentais, mas está presente em todas as relações institucionais que envolvem pessoas.

O Dia Internacional da Proteção de Dados oferece uma oportunidade para reforçar essa reflexão. Mais do que uma data comemorativa, ele convida à reafirmação de compromissos contínuos com a dignidade da pessoa humana, com o uso responsável da tecnologia e com a construção de relações baseadas na confiança. Em um mundo cada vez mais orientado por dados, proteger informações pessoais é, em última instância, proteger pessoas.

Ao associar a iluminação do Cristo Redentor a essa agenda, o Santuário conecta um símbolo universal a um direito fundamental contemporâneo. A mensagem é clara: a proteção de dados é um valor coletivo, que atravessa instituições, culturas e gerações. É nesse espírito que o trabalho do Núcleo de Segurança e Proteção de Dados do Santuário se desenvolve, buscando garantir que fé, cultura, inovação e responsabilidade caminhem de forma integrada e coerente.