As faces da proteção de dados

PINHÃO E KOIFFMAN ADVOGADOS

PINHÃO E KOIFFMAN ADVOGADOS
Direito que viabiliza tecnologia e inovação

ÍNDICE

Há mais de 20 anos como sócio do PK Advogados, atuando na advocacia empresarial especializada em direito e tecnologia, sempre foi um grande desafio esclarecer às empresas o tema da proteção de dados, em face das parcas e esparsas previsões anteriormente existentes em nossa legislação.

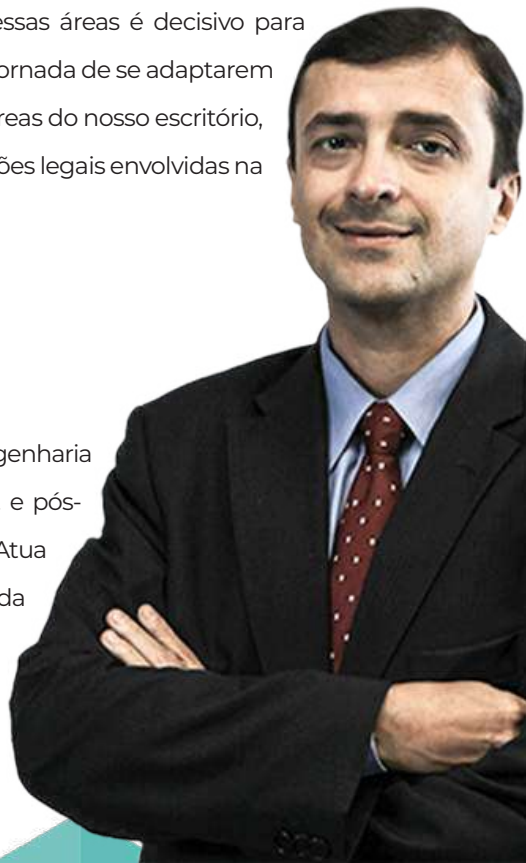
Felizmente, na última década o cenário mudou bastante, inicialmente com a aprovação do Marcio Civil da Internet em 2014, como uma das leis mais modernas mundialmente para regular as aplicações de internet. Posteriormente, a nossa Lei Geral de Proteção de Dados (LGPD) em 2018, como uma lei bastante avançada e alinhada aos padrões europeus, além de colocar o Brasil em um novo patamar internacional, como um país com um framework abrangente em proteção de dados.

O Brasil seguiu a tendência global dos governos que buscam aprimorar a proteção de dados e fomentar negócios com maior segurança jurídica. A compreensão adequada do cenário regulatório brasileiro do ponto de vista do uso dos dados e suas consequências é um dos objetivos deste material, abrangendo aspectos relacionados não apenas às normas de proteção de dados em si, mas também seus reflexos nas operações de M&A, indenizações por vazamentos de dados, impactos trabalhistas e tributários, monitoramento dos programas de governança, gestão de terceiros, prevenção e mitigação de incidentes e inovações de legal design aplicados no relacionamento com os titulares.

O PK Advogados possui profissionais especializados em proteção de dados, em todas as suas áreas, já tendo entregado diversos projetos de adequação à LGPD em variados setores como financeiro, seguradoras, saúde, concessionárias, shopping centers, redes de fast food, big data, bebidas, construção civil, desenvolvimento de software, fintechs, indústria automotiva, mineradoras, editoras de música, agronegócio, dentre outros. Continua assessorando o monitoramento dos programas de governança em privacidade, assim como apoiando o DPO nos diversos desafios de moldarem as suas empresas a esse novo sistema no país.

Um escritório especializado na questão da proteção de dados em todas essas áreas é decisivo para estabelecer e gerenciar com sucesso empresas de qualquer tamanho nessa jornada de se adaptarem ao novo sistema. Nosso objetivo com esse título, desenvolvido por todas as aéreas do nosso escritório, foi fornecer as empresas um manual para que elas possam entender as questões legais envolvidas na proteção de dados no Brasil em todas as suas vertentes de negócios.

Dr. Hélio Ferreira Moraes _hfmoraes@pk.adv.br
_https://www.linkedin.com/in/heliomoraes/ +55 (11) 3054-1020



Advogado, graduado da Universidade de São Paulo - USP. Licenciado em Engenharia Elétrica, da Escola Politécnica da Universidade de São Paulo (USP) em 1990, e pós-graduação em Automação e Controle também na Escola Politécnica (USP-SP). Atua na área de Comunicação que presta consultoria em legislação de Tecnologia da Informação e Telecomunicações e é sócio PK - Pinhão & Koiffman Advogados.

GESTÃO DE INCIDENTES EM PRIVACIDADE
Como agir para evitar ou mitigar danos

Falamos em incidente de segurança quando nos referimos a qualquer evento, confirmado ou sob suspeita que possa acarretar, acidentalmente ou não, a destruição, perda, alteração ou qualquer outra forma inadequada de tratamento, que afete a confidencialidade, integridade ou disponibilidade dos dados pessoais.

É comum que ao pensarmos em incidente de segurança, relacionemos o assunto ao meio digital ou online como ataques hackers, sequestros de bancos de dados, infecção por malwares, perda de documentos salvos nos computadores, dentre tantos outros exemplos. Na realidade, o conceito é muito mais abrangente e comum do que se imagina, é tão corriqueiro, que pode até passar desapercebido o fato de se tratar de um incidente de segurança, como por exemplo quando realizamos o descarte inadequado de documentos, armazenamos impressões em gavetas e armários sem segurança adequada, compartilhamos informações internamente ou até mesmo terceiros, sem nos certificarmos sobre a restrição do acesso àquelas informações, dentre outros.

Antes de adentrarmos nas medidas que podem ser adotadas para evitar incidentes, é importante ressaltar que a LGPD é norteada por diversos princípios, dentre os quais, falando em incidente de segurança, cabe ressaltar o princípio da segurança, que traz aos agentes de tratamento a obrigatoriedade de aplicação de medidas técnicas e administrativas aptas à proteger os dados pessoais de incidentes, bem como o princípio da prevenção, que igualmente trata da necessidade de adoção de medidas que previnam a ocorrência de danos.

Ainda com relação à responsabilidade de prevenir incidentes, o artigo 46 reforça o conceito, deixando a salvo no §1º a possibilidade de que a ANPD disponha sobre padrões técnicos mínimos para tal. Enquanto isso não ocorre, e, considerando a crescente economia digital, reforçada atualmente pelas adaptações necessárias devido ao cenário de pandemia, é altamente recomendado que sejam aplicados elevados padrões em termos de segurança da informação, implementação e monitoramento de medidas organizacionais.

Portanto, primeiramente por se tratar de uma exigência legal, a adoção dessas medidas não são pontuais ou passageiras, deverão ser inseridas na cultura das empresas. Além disso, de forma geral a responsabilidade sobre seguir tais medidas recairá naquele que faz uso e se beneficia dos dados, assim, em uma empresa, por exemplo, ainda que um funcionário aja inadequadamente, será ela a responsável, justifica-se desse modo então, que a primeira medida a ser tratada aqui seja a conscientização da alta gestão e dos colaboradores.

Uma organização, independentemente do seu porte, tem seu sustento em alguma medida relacionado a dados, logo, a alta gestão e os colaboradores compreenderem essa característica, da mesma forma que dominam todas as outras áreas do seu negócio, é reconhecer que a proteção de dados é indispensável para o prosseguimento das suas atividades.

Percebe-se que não é eficiente elaborar um projeto pontual que existirá apenas por algum período e logo cairá no esquecimento. A organização que verdadeiramente se preparar, instituirá um programa que será verificado e atualizado, demonstrando ao longo da sua jornada decisões consistentes, elaboradas e pensadas para cada caso.

Para o sucesso da incorporação da proteção de dados à cultura da organização, é essencial que todos sejam treinados para conscientização e conhecimento tanto do tema, quanto das práticas adotadas pela empresa, mas, sem a participação da alta gestão todo o conhecimento será em vão e se perderá, pois os colaboradores não encontrarão nas figuras de liderança a motivação, o incentivo e o exemplo. Ademais, por vezes será necessário o olhar e autorização para compreender quais são os pontos sensíveis de cada área, bem como o gasto com a aquisição de programas, produtos e serviços que auxiliarão na proteção de dados.

Não cabe mais no mercado uma empresa que não adote uma nova postura, pois é uma questão estratégica para se manter competitivo, o que refletirá em mais oportunidades de crescimento econômico. Desta forma, além de tornar as operações mais confiáveis, a proteção de dados como estratégia comercial mostra-se um ativo eficaz.

Algumas formas incentivar esse comprometimento:

• Reuniões sobre os impactos da LGPD nos negócios;
• Pronunciamentos da alta gestão;
• Incentivo na participação de cada etapa do processo de adequação;
• Inclusão dos colaboradores nas tomadas de decisão;
• Incentivo à participação nos treinamentos.

A conscientização será um processo vertical, sendo o segundo passo o envolvimento dos colaboradores. Ao contrário das lideranças que muitas vezes possuem atividades estratégicas, a maioria dos colaboradores possui contato direto e ativo com os dados pessoais no dia a dia, tornando-os peças fundamentais para garantir que incidentes não ocorram e, uma vez ocorrendo, sejam um dos primeiros "mecanismos" de alerta. Logo, uma forma muito interessante de incentivar a participação é frisar a importância deles como elementos essenciais.

O comportamento da alta gestão e a participação ativa dos colaboradores na identificação das atividades com dados pessoais já contribuirá com o processo de conscientização. Contudo, para intensificar e já colocar em prática novos comportamentos os colaboradores devem ter ciência e aplicar os princípios trazidos pela LGPD e as boas práticas, as quais destacamos algumas:

• Bloquear o computador todas as vezes que sair da mesa de trabalho;
• Salvar todos os arquivos no local adequado orientado pela área de TI: evitar salvar no computador ou usar rede compartilhada, dando preferência para armazenagem em nuvem, se disponível;
• Evitar compartilhamento de arquivos ou informações sensíveis via WhatsApp e outros aplicativos não oficializados pelo TI como adequados para uso na empresa;
• Adotar senhas complexas e mantê-las em lugar seguro.

Seguir essas ações simples já podem garantir que incidentes incialmente pequenos ocorram e eventualmente tragam consequências maiores.

A conscientização será um dos meios para trazer esses personagens para o caminho de identificar falhas e vulnerabilidades que possam acarretar a exposição de dados pessoais, sendo imprescindível para a aplicação de medidas apropriadas. Falando em medidas, e considerando que o tema proteção de dados está diretamente relacionado com segurança da informação, é importante ressaltarmos o assunto, e esclarecer que as ameaças sempre exploram uma vulnerabilidade.

Para melhor compreensão deste tópico, é importante reforçarmos alguns conceitos: i) vulnerabilidade é a fragilidade de um ativo. Trata-se de um ponto fraco, uma falha, que pode ser explorada por agentes internos ou externos; ii) Ameaça é a situação em que o agente interno ou externo explora a vulnerabilidade, de forma acidental ou não; iii) risco refere-se ao potencial, associado à exploração de vulnerabilidades. É a combinação da probabilidade de ocorrência de um evento e de qual seria seu impacto se ocorresse.

Podemos concluir que se uma ameaça consegue explorar uma vulnerabilidade, o nível do risco é consideravelmente aumentado, e, se bem-sucedida, os dados pessoais são expostos. Infelizmente, os riscos não podem ser completamente eliminados, no entanto, é possível aplicar controles e medidas de segurança, de forma que o risco seja modificado a níveis aceitáveis, aí é que está então, o diferencial da empresa que previne risco, evidenciar a correta aplicação de controles. Quando falamos em controles, podemos dividir em controles de segurança física e medidas técnicas.

• Controles de segurança física referem-se ao perímetro e estrutura física da empresa, são exemplos i) recepção e controle de pessoas autorizadas a acessar a área da empresa; ii) vigilância especializada; iii) câmeras ou serviços auxiliares; iv) existência de espaços restritos quando necessário para armazenamento de equipamentos, como datacenter por exemplo; v) energia e iluminação de emergência; vi) armários trancados para armazenamento de documentos físicos; v) segregação de áreas utilizadas pessoas da organização, de áreas utilizadas por terceiros, dentre outros.
• Quanto às medidas técnicas, são aplicadas para prevenir riscos em formato eletrônico, são exemplos i) firewall; ii) DLP; iii) antivírus; iv) criptografia; v) segmentação de dados; vi) atualizações de segurança; vii) controles de acesso; viii) testes de intrusão; ix) backups; x) classificação da informação, dentre outras.

Compreendido que essas medidas que visam a proteção de dados serão parte integrante do novo modelo de negócios será preciso elaborar um Programa de Governança em Privacidade, que será estruturado para dar, àqueles que tratarão os dados pessoais, direcionamento e segurança no sentido de atender não só a legislação, mas contribuir com um sistema mais bem organizado. Sendo um programa de governança entende-se que a privacidade será parte da visão da empresa, desta forma as atividades, serviços e produtos deverão considerar a privacidade em sua concepção ou em na adequação de projetos já existentes.

Falando primeiramente sobre os projetos que já existem na empresa, a LGPD em seu art. 37 dispõe sobre a obrigatoriedade de elaborar um registro das operações de tratamento de dados pessoais. Neste registro ocorrerá o mapeamento das atividades que usam dados, identificando pontos como a finalidade, a localização, a fonte, os tipos de dados e a quantidade, o interessante é que além de atender uma exigência legal esse mapeamento servirá como base para identificar o nível de adequação com o programa de privacidade e possibilitará uma análise dos riscos que estão expostos, dando direcionamento para as medidas necessárias.

Outra característica relevante do registro de operações é a identificação de terceiros. É comum que as atividades sejam compartilhadas ou dependam da atuação de outras organizações, dentro da lei existem diversos pontos sobre a responsabilidade que cada parte possui, sendo importante garantir que as relações sejam estabelecidas e mantidas com aqueles que também estão dispostos a se adequarem. Para isso, são criadas cláusulas contratuais, aditivos, por vezes verificações documentais ou presenciais para garantir o cumprimento da lei.

Podemos concluir com relação às medidas de prevenção, que a empresa deve, minimamente, possuir um programa de governança em proteção de dados em harmonia com o programa de segurança da informação, que trará boas práticas e atitudes para o dia a dia da empresa, além de realizar gestão de risco para prever vulnerabilidades e minimizar riscos, defender o ambiente com elevados padrões de segurança cibernética e promover conscientização para educar os colaboradores e outros envolvidos.

Enfim, é importante ressaltar que o artigo 48, § 1º, inciso III, estabelece que, em ocorrido o incidente, caso haja a necessidade de comunicar a ANPD e os titulares, em razão de risco ou dano relevante, a comunicação deverá contar, inclusive com a descrição das medidas técnicas e de segurança que foram utilizadas para a proteção dos dados. Dessa forma, todas as medidas aplicadas, devem ser também evidenciadas, para eventual necessidade de comprovação a autoridades ou ao próprio titular.

Aplicadas todas as medidas mencionadas, o ambiente estará consideravelmente seguro, mas não livre de riscos. Nesse sentido, é imprescindível que a empresa esteja preparada para a ocorrência de um incidente de segurança, ou seja, deve haver uma estruturação interna para respostas, caso ocorra. A estruturação interna deverá ser balizada por um Plano de Resposta a Incidentes, que deverá estabelecer diretrizes para o monitoramento, gestão e resposta a incidentes.

O Plano de Resposta a Incidentes deve identificar previamente quem serão os envolvidos na resposta, ou seja, quem será responsável por determinadas ações diante de um incidente. O time de resposta será organizado por funções, deve contar com a participação do Encarregado pela proteção de dados, juntamente com outros participantes definidos de acordo com a estrutura da empresa, e deve estar previamente treinado para o acionamento e execução do Plano, bem como para a coleta de evidências relacionadas ao evento.

Nesta fase de preparação, é importante também que a empresa realize periodicamente simulações de incidente. Essa medida é necessária para que se possa avaliar a eficácia do Plano, como a velocidade da resposta, o envolvimento do time e ações tomadas, a fim de corrigir eventuais vulnerabilidades identificadas no Plano.

Se, ainda que aplicadas todas as medidas expostas, houver notícias da ocorrência de um incidente, o primeiro passo é a análise minuciosa da situação, que deve ser feita pelo Encarregado, em conjunto com a área de tecnologia e, havendo indícios razoáveis de que o incidente de fato ocorreu ou está andamento, o Plano de Respostas deve ser de fato acionado. O primeiro passo após a confirmação da ocorrência do incidente de segurança e acionamento do Plano, é a avaliação para classificar a criticidade do incidente, considerando o volume de dados e indivíduos envolvidos e os tipos de dados (sensíveis, de crianças etc.).

Imediatamente, devem ser aplicadas medidas de contenção técnica do evento, incluindo a contratação de um parceiro especializado em segurança cibernética, para atuar ou apoiar a área de tecnologia que atuará nesta contenção e isolamento, remoção ou preservação dos sistemas afetados e, em fase posterior, entendido que há risco ou dano relevante aos titulares, será necessário notificá-los, além da ANPD, ocasião em que será imprescindível a apresentação de todas as evidências coletadas, tanto das medidas preventivas adotados, quanto com relação ao que foi feito para contenção do evento.

A ANPD poderá, então, de acordo com o previsto na LGPD aplicar sanções administrativas que vão desde uma simples advertência até de multas que podem chegar a 2% do faturamento limitadas a cinquenta milhões de reais. Uma das sanções que merece destaque é a publicização do incidente de segurança, ou seja, caso a Autoridade entenda como necessário a empresa deverá divulgar o ocorrido, caso isso ocorra a imagem da empresa sofrerá danos em relação a confiabilidade do mercado, o que poderá gerar o fim de contratos e de tratativas comerciais, gerando por vezes um prejuízo muito mais do que uma sanção econômica.

Contudo, antes que ocorra a aplicação de todas essas medidas, será realizado um procedimento administrativo que dará a possibilidade de defesa a empresa. Neste procedimento, deverão considerar alguns critérios, e trazemos como destaque a boa-fé do infrator, a cooperação e a adoção de mecanismos e procedimentos aplicados que podem minimizar os danos, além de possuírem uma política de boas práticas e governança. Veja, todas as formas de prevenção e mitigação que foram abordadas aqui servirão para atender as necessidades anteriores para não ocorrer um incidente, para atender quando um incidente ocorrer e para a defesa em relação as possíveis consequências.

A IMPORTÂNCIA DO MONITORAMENTO DO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

A cultura de proteção de dados pessoais ganhou grande importância no cenário nacional com a edição da Lei Geral de Proteção de Dados (Lei nº 13.709/18). Isso fez com que diversas empresas e organizações buscassem orientação profissional para se adequarem à Lei e, consequentemente, evitarem as graves penalidades previstas àqueles que não atingirem os requisitos mínimos para o tratamento de dados pessoais.

A fim de facilitar o processo de adequação, as empresas poderão formular regras de boas práticas e de governança que estabeleçam aspectos como, por exemplo, as suas condições de organização, o seu regime de funcionamento, seus procedimentos e normas de segurança para mitigação de riscos, assim como as obrigações específicas para os diversos entes envolvidos no tratamento de dados.

De acordo com o artigo 50, I, da LGPD, a implementação de um programa de governança deve, no mínimo:a) demonstrar o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) ser aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
c) ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) ter o objetivo de estabelecer relação de confiança com o titular de dados, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) estar integrado à estrutura geral de governança da instituição, além de estabelecer e aplicar mecanismos de supervisão internos e externos; g) contar com planos de resposta a incidentes e remediação; h) ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

No entanto, é importante destacar que um programa de governança em privacidade não é algo estático e imutável. Para amadurecimento do programa, é importante que os novos processos sejam aperfeiçoados e monitorados, sempre acompanhando as novas mudanças regulatórias, as alterações estruturais da instituição e eventuais novos projetos que envolvam atividades de tratamento de dados. Para isso, é importante que o monitoramento do programa de governança em privacidade seja conduzido por uma equipe especializada em proteção de dados pessoais, que poderá identificar lacunas e pontos de melhoria para auxiliar no aperfeiçoamento constante do programa.

Da leitura do artigo mencionado acima, podemos destacar alguns pontos que indicam expressamente essa necessidade, a exemplo do que dispõe o item b que aponta que o programa deve ser aplicado a todo o conjunto de dados pessoal, o que demanda um processo de conhecimento e atualização do registro de operações de tratamento de dados pessoais. Além disso, o item "h" aponta que o programa precisa ser atualizado constantemente, o que demanda atuação contínua e coleta de métricas para conhecimento de vulnerabilidades para aplicação dos ajustes necessários.

Importante advertir o leitor nesse ponto que o processo de monitoramento é algo complexo que deve estar entrosado entre equipe de governança em privacidade e equipe de segurança da informação. Isso porque, por vezes as vulnerabilidades são estruturais/tecnológicas ou até mesmo realizadas por profissionais utilizando-se de equipamentos da empresa, de forma que a equipe de segurança da informação precisa também participar desse monitoramento, para conseguir enxergar comportamentos desviados ou equipamentos que não oferecem a segurança necessária.

Necessário destacar o papel do gerenciamento de risco através do uso de auditorias especializadas. Em regra, as auditorias têm a capacidade de fornecer evidências sobre se determinado programa de governança em privacidade cumpre seu objetivo, assim como se os controles nele estabelecidos são gerenciados de forma correta.

O escopo da auditoria deve incluir todas as unidades organizacionais que tratam dados pessoais, assim como eventuais terceiros que integrem as atividades da instituição. Ademais, ela pode ser realizada de forma interna, em empresas que atuam como operadoras de dados pessoais ou por terceiros independentes.

No caso das auditorias internas, elas são realizadas com o intuito de obter auto avaliações do programa de governança de privacidade, ajudando, assim, a verificar em que estado este se encontra e quais deficiências devem ser corrigidas. Por sua vez, as auditorias em empresas que atuam como operadoras de dados ocorrem nos casos em que a instituição, enquanto controladora de dados, deseja verificar se as entidades contratadas como operadoras de dados estão cumprindo suas obrigações frente às legislações referentes à privacidade e proteção de dados pessoais.

Já as auditorias por terceiros independentes podem ser realizadas tanto por empresas de consultoria especializadas ou, ainda, por autoridades de fiscalização, como a Agência Nacional de Proteção de Dados (ANPD). Nesses casos, a depender de quem realizar a auditoria, certificações

podem ser emitidas ou sanções administrativas podem ser aplicadas, especificamente no caso da ANPD.

Sem prejuízo da realização de auditorias, outras medidas de manutenção podem ser tomadas, a fim de auxiliar o processo de monitoramento do programa de governança em privacidade e, com o intuito de demonstrar uma estrutura que possa ser viável – não obstante possa sofrer algum tipo de alteração a depender do porte da empresa e de suas necessidades – indicamos alguns pontos que são primordiais no processo de monitoramento:

a) Atualização do registro de operações: Necessário que haja procedimento formalizado internamente que indique as diretrizes para a atualização e que haja o apontamento de responsáveis para essa atividade, sendo que sua aplicabilidade deve ocorrer tanto para novas atividades quanto para atividades que serão modificadas e extintas;

b) Análise de vulnerabilidades: A partir das atualizações e até observando a metodologia "Privacy by design", deve ser feita análise para entender as vulnerabilidades das atividades novas/modificadas, inclusive a fim de entender se há um "padrão" de vulnerabilidades que indique a necessidade de trabalho mais focado.

c) Relatórios de performance e atualização dos documentos de governança: Considerando que a LGPD determina que o tratamento de dados deve se pautar, inclusive, pelo princípio da prestação de contas, e que o programa de governança deve estar sempre atualizado, é recomendável que a empresa realiza periodicamente um relatório de performance formalizando as vulnerabilidades encontradas e os planos de ação necessários, atualizando os documentos do programa de governança quando se mostrarem obsoletos ou desatualizados.

d) Treinamentos: Os treinamentos são importantes pois tendem a evitar equívocos, como é o caso do treinamento de integração de novos funcionários, bem como serve para corrigir atitudes equivocadas que já tenham sido adotadas. Assim, é importante que mensalmente os novos funcionários sejam reunidos para que conheçam a estrutura de governança da empresa e o que se espera deles quando lidarem com dados pessoais, bem como, a partir das vulnerabilidades encontradas no processo de atualização do registro de operações ou qualquer outra encontrada no processo de monitoramento, seja feito treinamento específico para evitar que a vulnerabilidade torne a acontecer.

e) Acompanhamento regulatório: Importante primeiramente que o DPO consiga dominar o ambiente regulatório ao qual a empresa esteja alocada. Além disso, independente de ambiente regulatório, é importante que esteja antenado com as atualizações legislativas que possam afetar o programa de governança em privacidade.

f) Simulações: Não é necessário aguardar que um titular reclame ou um incidente aconteça

para que nos demos conta de que os procedimentos para gestão dos direitos dos titulares e gestão de incidente estão desatualizados ou que a equipe responsável não está preparada. Para isso, é importante que a empresa realize simulações e formalize o desempenho e desfecho dessas simulações;

g) Gestão de terceiros: Considerando que muitas vezes há o compartilhamento de dados com parceiros comerciais entre outras empresas, necessário que o Encarregado tenha conhecimento sobre os processos em que há o compartilhamento, quem recebe ou nos repassa as informações e qual a maturidade desses agentes em relação à proteção de dados pois, considerando o risco da atividade, será necessário adotar diversas medidas, sobretudo contratuais e de auditoria ao longo da relação contratual ou, até mesmo deixar de contratar com determinado agente.

Como dito anteriormente, a intenção não é exaurir o assunto, sobretudo porque as medidas podem ser variáveis a depender do porte e atividade exercida pelo agente de tratamento, contudo, entendemos que as medidas acima são extremamente recomendáveis e devem estar entrosadas com as medidas que seja adotadas pela equipe de governança em segurança da informação para que o processo seja o mais completo possível.

Serviços de apoio ao Encarregado (DPO) podem ser fundamentais para auxiliar este com respostas à consultas, análises contratuais, análises de novos procedimentos e opiniões legais. Ademais, a realização de treinamentos personalizados pode auxiliar no processo de conscientização dos colaboradores das empresas, conforme as necessidades identificadas.

A consulta em caso de incidentes, com suporte no relacionamento entre os titulares envolvidos e a ANPD, assim como o apoio na construção e negociação de cláusulas contratuais com parceiros estratégicos, são outros exemplos de serviços essenciais no processo de monitoramento do programa de governança.

Portanto, considerando a extensa agenda regulatória disponibilizada pela ANPD, que estabeleceu um dinâmico cronograma com as ações planejadas para os próximos meses, é de suma importante que as empresas priorizem medidas focadas no acompanhamento regulatório relacionado à proteção de dados pessoais. Com isso, será possível garantir a constante atualização e adequação das políticas e procedimentos implantados, bem como o efetivo monitoramento do programa de governança em privacidade.

A INFLUÊNCIA DA LGPD EM OPERAÇÕES DE M&A

A entrada em vigor da Lei Geral de Proteção de Dados (Lei nº 13.709/18, "LGPD"), que visa a coibir o uso abusivo e desnecessário de dados pessoais por empresas, instituições e até pelo poder público, prevendo multas e sanções em caso de seu descumprimento, gerou a necessidade de rápida adaptação, nas empresas dos mais diversos ramos e portes, para adequação de suas estruturas e procedimentos, em conformidade com as regras estabelecidas pela nova legislação. Nesse cenário, assim como nos diversos âmbitos de gerenciamento e operação de um negócio, não poderia ser diferente em relação a ocasiões em que há a transferência, entre empresas, de parte ou a totalidade de seus ativos, ou mesmo em situações em que a própria titularidade da empresa é transferida, por meio da venda de ações ou quotas: são as operações comumente chamadas de M&A (sigla do inglês Mergers and Acquisitions, ou Fusões e Aquisições).

Embora a preocupação com proteção de dados em uma operação de M&A seja mais acentuada e sensível quando são envolvidas startups e empresas de tecnologia (em razão do risco que uma má estrutura de proteção de dados pode acarretar, em empresas cujos ativos preponderantes são bases de dados), o cumprimento das regras trazidas pela LGPD deve ser objeto de atenção em negócios e operações envolvendo qualquer tipo de empresa, uma vez que, em maior ou menor grau, a operacionalização e gerenciamento de uma empresa é inviável, ou, no limiar, impossível, sem a utilização de dados pessoais de colaboradores, consumidores, gerentes, fornecedores, entre outros.

Assim, buscaremos, abaixo, traçar um panorama geral das fases mais comuns a uma operação de M&A, apontando, em cada etapa, a importância do cumprimento das regras da LGPD e os riscos envolvidos na condução de um negócio sem uma governança de dados adequada.

Respeitada toda a diversidade e possibilidade de combinações e negociações existente, uma operação de M&A apresenta, em termos gerais, algumas fases comuns: (i) a negociação inicial e assinatura de acordos de confidencialidade (ou NDA's) e Memorandos de Entendimento (ou MOU); (ii) a auditoria legal na empresa-alvo (ou due diligence); (iii) a assinatura dos contratos definitivos (de compra e venda de ações/quotas ou de transferência de ativos); e (iv) o fechamento da operação.

Inicialmente, podemos destacar a importância da proteção de dados desde o interesse inicial da empresa compradora em sua empresa-alvo (aquela que deseja adquirir): a existência de um histórico de vazamentos de dados, ou de vinculação à sua marca a descaso com a proteção

de dados pessoais, por exemplo, pode gerar uma má reputação na empresa-alvo, deixando-a menos atraente em relação ao interesse de possíveis compradores. A baixa maturidade em relação a uma governança de dados também pode ser um motivo para a redução da faixa inicial do preço que o comprador está disposto a lançar mão para adquirir a empresa-alvo, já que, uma vez concretizada a operação, seria necessário um grande investimento para a adequação a uma boa estrutura de proteção de dados.

Encontrada a empresa-alvo e feitos os primeiros alinhamentos entre as partes, em razão da sensibilidade na abertura de informações estratégicas que serão trocadas pelas partes, assim como pelo caráter sigiloso normalmente atribuído às negociações de M&A, é comum que as partes envolvidas na negociação assinem um acordo de confidencialidade (ou, do inglês, NDA), que proíbe a divulgação de detalhes da operação e limita também o uso e divulgação de informações compartilhadas entre as partes durante toda a operação, o que inclui, certamente, dados pessoais.

Após a assinatura do acordo de confidencialidade e assentadas as bases iniciais da negociação, vendedor e comprador firmam um acordo, geralmente conhecido como Memorando de Entendimento (ou, do inglês, MOU), para estabelecer as regras que ordenarão toda a operação até a assinatura dos contratos definitivos. Nesse documento é de vital importância existirem cláusulas que regulem o compartilhamento de dados entre as partes (que costuma ser particularmente intenso durante a fase da auditoria) e preveja como serão conduzidos possíveis incidentes de vazamentos de dados compartilhados e as nuances da atribuição de responsabilidades em casos de descumprimentos da LGPD. Isso porque, a partir do momento em que há a utilização compartilhada de dados pessoais entre as partes, a empresa-alvo e o potencial adquirente configuram-se, para fins da LGPD, como controladores desses dados, podendo ser solidariamente responsáveis por eventuais danos causados, uso ilegal dos dados ou incidentes de segurança, nos termos do artigo 41, §1º, inciso II da LGPD. Assim, é recomendável que as cláusulas do MOU detalhem: (i) a finalidade e a hipótese legal que justificam o compartilhamento das bases de dados pessoais durante a operação, principalmente na fase de auditoria e (ii) as medidas técnicas a serem adotadas pelos envolvidos para preservar os direitos dos titulares e a segurança dos dados compartilhados.

Na etapa seguinte, é conduzido um processo de auditoria (ou due diligence) na empresa-alvo, por meio do qual o potencial adquirente realiza uma análise minuciosa de seus diversos aspectos, como sua situação contábil, financeira, a eventual existência de dívidas trabalhistas, tributárias, as multas que lhe foram aplicadas e os processos judiciais dos quais faz parte. Com isso, o comprador possui um conhecimento mais aprofundado da situação da empresa-alvo e pode fazer a precificação do negócio de maneira mais precisa. Nessa fase, a LGPD é essencial em dois aspectos distintos: o primeiro diz respeito à verificação do nível de maturidade e estrutura

de proteção de dados da empresa-alvo, o que influencia na verificação dos riscos a que o comprador pode estar sujeito caso a operação se concretize. Nesse ponto, devem ser analisados tanto os processos adotados pela empresa-alvo, como a forma de coleta e tratamentos de dados pessoais, a preocupação com a privacidade em documentos jurídicos (a existência de políticas de privacidade e cláusulas de proteção de dados em contratos vigentes, por exemplo), quanto a existência de uma robustez nos processos e programas de Segurança da Informação, que possam garantir uma menor exposição a riscos de ataques hacker e incidentes como sequestro (ramsonware) ou vazamento de dados.

O segundo vetor de preocupação com a LGPD na fase de auditoria diz respeito à observância das regras de proteção de dados, por ambas as partes envolvidas, durante o próprio desenrolar dessa etapa.

O eventual compartilhamento de bases de dados referente a pessoas naturais da empresa-alvo configura um tratamento de dados que exigiria, segundo a LGPD, uma transparência aos titulares de dados (pessoas a quem os dados se referem), o que conflita com o caráter sigiloso dos documentos de confidencialidade assinados entre as partes, bem como da própria natureza da negociação. Essa transparência seria necessária uma vez que, pela LGPD, todo dado pessoal coletado por um agente de tratamento (empresas, instituições) deve servir para uma finalidade específica e ter uma justificação para ser utilizado (ex.: coleta de dados cadastrais para executar um contrato de compra e venda de produtos), não podendo ser utilizado para outra finalidade ou transferido para um terceiro, a menos que haja o consentimento do titular (o que representaria um problema tanto operacional quanto em relação à confidencialidade da negociação).

Dessa forma, a partir do momento em que as informações pessoais contidas em um banco de dados da empresa-alvo são compartilhadas com a empresa compradora, há a utilização de dados pessoais para finalidade diversa da qual ele foi coletado (uma vez que operações de M&A não são tão prováveis nem recorrentes no ciclo de vida de grande parte das empresas). Dada essa situação, visando a minimizar os risco e danos, recomenda-se que: (i) as políticas de privacidade da empresa-alvo, divulgadas aos titulares, bem como os termos de consentimento específicos firmados pelos titulares (quando o consentimento for a base de tratamento), devem prever a possibilidade de compartilhamento dos dados com terceiros para fins de avaliação do interesse na aquisição da empresa controladora (dos dados); e (ii) seja utilizada a justificação de interesse legítimo das empresas em negociação nesse uso de dados (artigo 10 da LGPD). Contudo, como essas alternativas representam um consentimento fraco ou inexistente do titular de dados, é preciso ter muita cautela com esse

compartilhamento, devendo ser tratados apenas os dados estritamente necessários para a realização dessa auditoria, (indicando, por exemplo, de maneira prévia quais dados são efetivamente necessários, o que minimiza o risco de compartilhamento desnecessário de dados). Em todo caso, o compartilhamento de dados pessoais sensíveis (ex.: origem racial ou étnica, convicção religiosa, opinião política) nessas situações é absolutamente desencorajado.

Ainda, é altamente recomendável nessas situações de compartilhamento de dados a utilização, sempre que possível, de técnicas como a anonimização de dados pessoais, que os desvincula de uma pessoa identificada, bem como a utilização de plataformas virtuais seguras (virtual data rooms), que limitam o acesso de pessoas às informações contidas nesses espaços, e, muitas vezes, também limitam as opções de manipulação pelos usuários das informações lá armazenadas.
Ocorrida a auditoria e não sendo identificados problemas e riscos capazes de inviabilizar o prosseguimento da negociação, são elaborados os contratos definitivos, que podem abordar tanto a venda de ações/quotas de uma sociedade (também conhecidos com SPA, em inglês), quanto a transferência de ativos do vendedor para o comprador. O contrato definitivo será de fundamental importância, pois definirá, com mais precisão todos os detalhes da negociação, regulando a relação entre as partes após a sua assinatura e após o fechamento, que é a fase final em que a operação é considerada concluída.

Tendo isso em vista, o contrato deverá prever diversas situações relacionadas à proteção de dados, tal qual a atribuição de responsabilidade, em decorrência de incidentes como vazamentos de dados, bem como de multas aplicadas por autoridades públicas ou ações judiciais relacionadas ao descumprimento da LGPD. Essas espécies de contrato geralmente possuem cláusulas robustas de "declarações e garantias", destinadas a atestar a suficiência e veracidade das informações disponibilizadas ao comprador ao longo do processo de auditoria. Nesse ponto, é importante que o contrato da operação preveja declarações específicas dos vendedores e/ou da empresa-alvo sobre a aderência às exigências da LGPD.

Além disso, é bem comum que os vendedores da empresa-alvo ou do ativo assumam a responsabilidade de indenizar o adquirente por contingências relacionadas a eventos ocorridos ou decisões tomadas antes da consumação da operação – não respondendo por eventos futuros, posteriores à venda da empresa ou do ativo. No entanto, especificamente no que diz respeito à proteção de dados, por mais que seja de se esperar a implementação das medidas de adequação a um bom nível de proteção de dados fique a cargo do adquirente, após o fechamento da operação, é possível, por exemplo, que vulnerabilidades em sistemas

de segurança permaneçam indetectadas e só venham a causar efetivos danos após a conclusão da negociação. Nesses casos, uma saída importante é a possibilidade de conciliação de interesses, que pode ser a previsão de um período de transição, posterior à operação, em que o vendedor permanece obrigado a indenizar eventuais contingências da empresa-alvo relativas à proteção deficiente de dados.

Assim, em um rápido percurso pelas fases de uma operação de M&A, é possível verificar que a proteção de dados é uma preocupação que deve tomar lugar de relevância para ambas as partes envolvidas, assim como para os profissionais que as assessoram, uma vez que a adequação à LGPD e suas diretrizes afeta em aspectos fundamentais do negócio, como a precificação da empresa-alvo, a análise de riscos para definir a viabilidade do negócio, sem esquecer da necessidade da observância constante das regras de proteção de dados na condução dos processos e etapas da operação

LEGAL DESIGN E LGPD: UMA UNIÃO QUE FUNCIONA

O direito é um ramo que não trabalha com resultados exatos. Como sabemos, é possível encontrar jurisprudências contra e a favor para quase todos os tipos de disputa.

No entanto, a Lei Geral de Proteção de Dados mudou significativamente essa dinâmica, na medida em que estipulou obrigações muito objetivas, cuja verificação pode ser comparada a uma ciência exata.

E é nesse ponto que o Legal Design oferece uma solução eficaz para os profissionais do direito, posto que se trata de uma abordagem baseada na consagrada forma de resolver problemas dos designers: o design thinking.

Esse caráter de maior objetividade da Lei Geral de Proteção de Dados se destaca quando analisamos as questões que tratam do direito das pessoas à informação sobre como seus dados pessoais serão tratados.

O consentimento, por exemplo, foi definido na lei como uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Repare na escolha de palavras do legislador. Inequívoca. Determinada.

São palavras que deixam pouca margem à interpretação. Ou a manifestação é inequívoca, ou não é. Ao menor sinal de dúvida ou desconfiança, impossível utilizar o adjetivo “inequívoco”.

Em seguida, a LGPD elenca os princípios que devem ser observados por todos aqueles que executam atividades de tratamentos de dados pessoais e, entre eles, está o Princípio da Transparência.

Aqui, outra escolha sábia do legislador. Não existe meio transparente. Ou algo é transparente, ou não o é.

E o Princípio da Transparência foi definido como a garantia, aos titulares de dados pessoais, de que receberão informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.

Mais uma vez, se comprovada que a informação fornecida aos titulares não era clara, precisa e facilmente acessível, teremos uma violação legal transparente.

É fácil notar que a intenção do legislador foi: diga toda a verdade sobre o que você fará com os dados pessoais e então saberemos se o titular foi mal informado ou, possivelmente até enganado a depender da qualidade da informação que tenha sido ofertada ao titular dos dados, o que pode, inclusive, tornar nulo o consentimento.

E como fornecer uma informação assim, clara, precisa e inequívoca?

É aí que entra o Legal Design.

Se esse é o seu primeiro contato com o tema Legal Design, vou te explicar em poucas linhas o que ele é.

O Legal Design é uma abordagem que adaptou o Design Thinking para o mundo do direito, de forma a nos ajudar a projetar serviços e sistemas jurídicos mais humanos, úteis e satisfatórios.

Em outras palavras, é deixar de fazer o direito por fazer e colocar as pessoas no centro de toda solução jurídica para, com empatia, criatividade, prototipação e testes, alcançar a solução mais eficiente para o problema.

Quando a questão envolve o fornecimento de informações jurídicas, chamamos esse tipo de Design de Informação ou Visual Law.

Nele, o que se busca é a eficiência da entrega da informação jurídica e, por eficiência, se entende o ato de alcançar o objetivo de qualquer comunicação jurídica: (i) gerar interesse no leitor; (ii) capturar sua atenção para que lei até o final; (iii) garantir que ele compreenda tudo o que ler; e (iv) o leitor adotar o comportamento que dele se espera.

Para isso, aplicamos diversas técnicas como Plain Language, Storytelling e Comunicação Não Violenta (CNV).

Pela Plain Language, por exemplo utilizamos uma diretriz chamada “palavra conhecida”.
Embora o nome pareça lógico, muitos advogados cometem o erro de redigir o texto utilizando palavras que seriam conhecidas para ele, e não para o usuário final que terá que ler aquela política de privacidade, por exemplo.

Para evitar esse problema, o processo de Legal Design recomenda que o advogado faça um

estudo para entender qual é o perfil das pessoas que terão que ler o documento que ele está redigindo. Esse estudo pode envolver pesquisas, entrevistas e outras técnicas.

Já o Storytelling ajuda na retenção da atenção do leitor. Existem diversas estruturas narrativas que oferecem altos níveis de atração para o cérebro humano, não só para chamar e manter a sua atenção, mas também para conduzir o leitor por uma linha de raciocínio que achamos ser a ideal para que ele compreenda o assunto.

Ao contrário do que parece, não há uma previsão legal impondo uma forma determinada para redação de políticas de privacidade. No entanto, a maioria dos documentos seguem um formato engessado, um misto de copiar e colar combinado com falta de criatividade, que resulta no que já sabemos: ninguém lê. Ninguém entende. Ninguém sabe o que é feito com seus dados.

Já a função da Comunicação Não violenta é nos ajudar a escrever de uma forma mais humana Qual é o sentimento que você quer gerar na pessoa que lê o seu documento jurídico? Quais são as necessidades do leitor e como você pode ajudá-lo com seu documento jurídico? Para finalizar um projeto de Design de Informação completo, contamos ainda com a aplicação de recursos visuais, como gráficos e linhas do tempo, e de conceitos de design gráfico, como contraste e harmonia. Porém, explicar isso aqui transformaria nosso artigo em um livro.

A ideia é passar para você os conceitos básicos do Legal Design e mostrar como ele pode ser usado como uma ferramenta para te ajudar a cumprir a LGPD em seus requisitos mais objetivos, como o fornecimento de informação clara, precisa e facilmente acessível.

Em outras palavras, as políticas de privacidade tradicionais não são nada claras, precisas e muito menos facilmente acessíveis. Assim como muitos documentos jurídicos, elas são feitas de advogado para advogado e sua função principal era servir como prova em uma eventual ação judicial.

Porém, essa estratégia não funciona mais. Se você juntar uma política de privacidade tradicional em uma ação judicial que discute o cumprimento da LGPD, é bem possível que você sofra uma terrível condenação.

O Legal Design é esse novo sistema operacional que precisa ser instalado nos advogados para

que a antiga prática seja substituída por uma estratégia que seja deixar as partes confortáveis, facilitar os negócios, agilizar as transações e evitar os conflitos. Não só servir como prova.

Pode ser que você já tivesse ouvido falar sobre o Legal Design ou o Visual Law antes e eu quero aproveitar essa oportunidade para quebrar alguns erros conceituais que vejo com muita frequência.

Visual Law e Legal Design não são sinônimos. O Visual Law (ou design de informação) é um dos tipos de Legal Design. Temos também o Design de Produto, o Design de Serviço, o Design de Organização e o Design de Sistemas. São 5 os tipos de Legal Design.

O Legal Design não é a simplificação do direito. O ato de simplificar é uma das estratégias que usamos e nem sempre é recomendada. Para uma petição, por exemplo, cujo destinatário é um magistrado, não há qualquer problema em utilizar jargões e termos técnicos, pois ele os entende. Simplificamos apenas quando é necessário.

O Legal Design não é sobre estética ou beleza. Os recursos gráficos e conceitos de design são utilizados seguindo critérios técnicos. A busca é pela funcionalidade, não pela beleza. Quando nos preocupamos com o contraste, por exemplo, a preocupação é a legibilidade e a leiturabilidade. Não é estética.

A propósito, um dos conceitos de design que temos que seguir é a harmonia. E, pela harmonia, precisamos garantir que não há nada fora do lugar, sobrando ou inútil. Portanto, se um ícone foi colocado só por estética, sem uma função, isso constitui um erro técnico no Visual Law.

Em resumo, o Legal Design é sobre eficiência e funcionalidade. É sobre resolver os problemas jurídicos de uma forma melhor, posto que coloca o usuário no centro do processo. É sair do subjetivismo e entrar em uma zona mais objetiva. Um direito de resultados mais práticos, mais exatos, mais palpáveis.

E, por isso, ele é tão recomendado para projetos envolvendo a Lei Geral de Proteção de Dados.

O IMPACTO DA LGPD NAS RELAÇÕES DE TRABALHO

Com a digitalização das interações humanas e o uso de inteligência artificial na utilização de dados para as mais diversas finalidades, atualmente é praticamente impossível se imaginar uma relação jurídica que não enseje, ainda que indiretamente, o tratamento de dados pessoais. Nas relações de trabalho, esta também é uma realidade.

Analisando-se as relações de emprego, a coleta e uso de dados pessoais se dá desde o período pré-contratual até sua extinção e, assim, sob o ponto de vista trabalhista, a intimidade e vida privada do trabalhador sempre foram tidos como valores resguardados constitucionalmente (art. 5o, X, da CF), bem extrapatrimonial que, se violado, enseja indenização pecuniária, conforme expressamente previsto no artigo 223-G da Consolidação das Leis do Trabalhista aos trabalhadores da iniciativa privada.

Aos empregadores e servidores públicos este patrimônio imaterial é protegido pela Lei nº 12.527/11, que em seu artigo art. 31, permite a divulgação de informações pessoais, desde que com observância do respeito à intimidade, vida privada, honra e imagem das pessoas. Para tanto, estabelece que essas informações terão o acesso restrito pelo prazo máximo de 100 anos, durante os quais a sua divulgação depende de previsão legal ou consentimento expresso da pessoa a que elas se referirem (art. 31, § 1o).

Nesse sentido, no âmbito trabalhista, a Lei Geral de Proteção de Dados não criou direitos e obrigações, mas veio para ratificar a obrigatoriedade de preservação de informações pessoais dos trabalhadores como direito imaterial protegido, pois ainda que não haja previsão expressa e pela sua aplicação nas relações de emprego, o contrato de trabalho demanda o tratamento de dados pessoais e sensíveis pelo empregador, que neste contexto se configura como o controlador da informação, ressaltando-se que nos termos do artigo 3º a obrigação de preservação de dados se estabelece para qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, portanto, empregadores da iniciativa pública ou privada.

Partindo-se desta premissa, o empregador deverá adequar suas práticas para a coleta e manuseio das informações pessoais de seus empregados, se pautando nos parâmetros estabelecidos pela LGPD para fazê-lo, sob pena de responder judicialmente por prejuízo causados ao trabalhador na hipótese de divulgação ou utilização com a finalidade à qual se prestava.

Já há, de fato, precedentes na Justiça do Trabalho que se fundam na LGPD para estabelecer conduta antijurídica do empregador ensejadora de reparação pecuniária ao trabalhador lesado em virtude de vazamento de dados aos quais teve acesso em razão da relação de emprego, utilizados de forma equivocada ou tornados públicos indevidamente.

E esta é a razão pela qual as organizações devem rever seus conceitos, pois há pouco ainda se praticava a cultura da informação quantitativa, que é coletada e mantida sem qualquer avaliação de finalidade e adequação. O processo se aperfeiçoa sob a ótica da LGPD e a busca pela informação deve ser qualitativa, se verificando a necessidade de se ter e manter determinado dado ou documento.

A adequação das organizações aos parâmetros da LGPD ainda se mostra como um cenário desafiador, visto que algumas situações decorrentes da relação de emprego requerem maior atenção em razão da proteção exigida para cumprimento desta legislação, citando como primeiro exemplo, a atuação em regime de teletrabalho.

Em relação aos teletrabalhadores, profissionais que atuam sob modalidade contratual específica regulamentada pelo artigo 75 e seguintes da CLT, de forma preponderante fora do estabelecimento do empregador se utilizando de recursos tecnológicos na execução de suas atividades profissionais, a cautela há de ser redobrada, já que além da coleta de dados pessoais e sensíveis que decorrem da própria execução do contrato, especialmente se o trabalho é exercido da residência, o acesso a imagens do trabalhador, de terceiros com ele convivem no ambiente familiar e até mesmo informações partilhadas entre eles deve ser preservado.

Para tanto, é recomendado que o empregador adote uma política de etiqueta digital especialmente para esta modalidade contratual, consistente nas seguintes ações:

• Estabelecer horários para atendimento virtual da demanda pelo trabalhador, especialmente em se tratando de reuniões em vídeo;
• Adotar “backgrounds” corporativos como fundo de tela, a fim de impedir que a imagem da residência, de familiares e trabalhadores domésticos sejam partilhadas com colegas de trabalho, clientes e fornecedores;
• Orientar os gestores a agendar reuniões pontuais e em horários comuns para atuação profissional;
• Não requerer atendimento imediato de vídeo conferência sem prévio aviso;
• Informar previamente ao profissional que a reunião será gravada;
• Preferencialmente não permitir que as ferramentas de trabalho fornecidas pelo empregador (notebook e celular corporativo) sejam utilizados para finalidades distintas da execução do contrato de trabalho pelo empregado ou manuseadas por terceiros;
• Adotar políticas específicas para confidencialidade e segurança da informação, com fundamento na LGPD (Lei nº (Lei nº 13.709/2018);
• O teletrabalhador se enquadra nas hipóteses de exceção de controle de jornada, assim, a utilização de programas de rastreamento do tempo de atividade e de inatividade dos trabalhadores, registro de páginas de Internet acessadas, a localização em tempo real e captura

de imagem do ambiente de trabalho são incompatíveis com esta modalidade de trabalho, tanto sob o ponto de vista da legislação trabalhista em si, ensejando a desconfiguração desta modalidade contratual para fins de pagamento de horas extras pelo controle, bem como sob o prisma da proteção de dados, já que em desacordo com os princípios da finalidade e necessidade da coleta e utilização destes dados.

É recomendável que estas práticas sejam adotadas ao trabalho remoto em qualquer modalidade, ou seja, teletrabalho efetivo (artigo 75 da CLT), "home office" e no caso de adoção de "sistema híbrido".

Por outro lado, é importante também ressaltar que o teletrabalhador/ trabalhador remoto se equipara ao profissional que atual em regime presencial para todos os fins e efeitos e, portanto, é um preposto da empresa, ou seja, os atos do empregado enquanto na função de representação do empregador geram obrigação de responsabilidade civil deste na hipótese de prejuízo à terceiros. Desta forma, se o teletrabalhador no exercício de sua função é operador de dados, deve ser expressamente orientado quanto à responsabilidade de seu cargo sob a ótica da Lei Geral de Proteção de Dados, inclusive para fins de aplicação das penalidades legais cabíveis, até mesmo a rescisão contratual por justa causa.

Um outro reflexo importante que a LGPD trouxe para a seara trabalhista foi a obrigatoriedade de indicação de um encarregado pela supervisão da aplicação da lei, popularmente conhecido como "DPO" (data protection officer). Isto porque, comumente as empresas elegem para exercício desta função um membro do seu quadro de empregados, originalmente contratado para exercício de atividade que não contempla esta responsabilidade. De fato, a nomeação de um empregado para exercício de atividades correlatas ao cargo para o qual foi contratado não representa, por si só, risco ou ilicitude.

Na dinâmica da relação laboral são lícitas as alterações pontuais das atividades desempenhadas pelo empregado (jus variandi), pois é neste sentido o teor do artigo 456, parágrafo único, da CLT, permitindo ao empregador determinar o exercício de atividades diversas, desde que compatíveis com a condição pessoal do trabalhador e que não represente desiquilíbrio entre a função exercida e a contraprestação ofertada. Se observados esses limites, o acréscimo de atividades ao trabalhador não enseja, por si só, o pagamento de diferença salarial por acúmulo de funções, estando remuneradas pelo salário todas as tarefas desempenhadas dentro da jornada de trabalho.

O ponto de atenção neste caso é no sentido de que o acréscimo ou alteração de atividades, não poderão desvirtuar a essência da função para a qual o trabalhador tenha sido contratado e que possam acarretar responsabilidades ou encargos de natureza distinta dos que tenham sido estipulados quando da contratação, salvo se tiverem sido renegociadas de forma bilateral as condições de trabalho, inclusive com majoração salarial, se for o caso.

Outra prática comum adotada pelas empresas impactada pela LGPD é a obtenção de "background checks" como etapa eliminatória em processos seletivos.

Em razão da ausência de regulamentação legal específica até 2018, a Jurisprudência trabalhista se firmou no sentido de que é válida a pesquisa prévia na hipótese desta se justificar em razão de previsão em lei, da natureza do ofício ou do grau especial de fidúcia exigido, como constou no documento, inclusive com tese jurídica prevalecente para tema repetitivo pela Seção de Dissídios Individuais do Tribunal Superior do Trabalho, para fins de uniformização de jurisprudência a ser seguida pelos Tribunais Regionais do Trabalho (Processo TST nº-IRR-243000-58.2013.5.13.0023 C/J PROC. Nº TST-RR-184400-89.2013.5.13.0008). Pela aplicação dos termos da Lei de Proteção de Dados às relações de trabalho, a inobservância deste critério representa risco trabalhista concreto de indenização ao prejudicado, ratificando o posicionamento adotado pelos Tribunais.

Em conclusão, a LGPD tem efetiva aplicação nas relações de trabalho e deve ser encarada como obrigação legal, ultrapassando o caráter de governança e boas práticas, ou seja, não se trata de faculdade do empregador, mas, sim, de observância mandatória, sob pena de arcar o empregador com prejuízos causados na hipótese de má utilização ou negligência quanto aos dados que seus trabalhadores lhe confiaram.

LEI GERAL DE PROTEÇÃO DE DADOS E TRIBUTAÇÃO

Quais os impactos tributários da adequação à Lei Geral de Proteção de Dados - LGPD?

Inicialmente, convém lembrar que vivemos na chamada Era da Informação, na qual, como já disseram, os "dados são o novo petróleo" .

De fato, dados, atualmente, são utilizados para desenvolver novos produtos ou serviços, para aperfeiçoá-los, para alcançar e cativar clientes, para contratar e incentivar colaboradores, desenvolver fornecedores etc. Enfim, dados e sua análise adequada hoje são vitais para a sobrevivência de qualquer empresa no mercado.

É nesse cenário, de extrema relevância e de alto volume de processamento e "enriquecimento" de dados que surgiu a LGPD, como forma de regular não só o uso e análise dos dados, mas também as possíveis consequências de seu vazamento ou compartilhamento não autorizado.

Justamente por isso, as empresas brasileiras tiveram que se adequar às regras da Lei Geral de Proteção de Dados – LGPD (e aquelas que ainda não o fizeram terão que fazê-lo). Assim, em geral, incorreram em diversas despesas, sejam despesas com pessoal, com a contratação de prestadores de serviços, cursos, licenciamento de softwares ou outras despesas correlatas.

Nesse contexto, cumpre indagar, sob o aspecto tributário, quais são as possíveis consequências na apuração dos tributos, em especial, do Imposto de Renda Pessoa Jurídica – IRPJ, da Contribuição Social sobre o Lucro Líquido – CSLL, da Contribuição ao PIS e da COFINS.

Em relação à apuração do IRPJ, e com maior razão da CSLL, na sistemática do Lucro Real, não nos restam dúvidas de que referidas despesas seriam dedutíveis haja vista que são absolutamente necessárias (não só por conta de sua relevância, mas também por decorrerem de exigência legal) usuais e normais (as empresas em geral estão obrigadas a se adequarem a referidas regras).

Assim, desde que as despesas estejam devidamente documentadas e comprovadas e que sua pertinência à adequação à LGPD seja demonstrada, não nos parece existam riscos à dedutibilidade de referidos dispêndios.

Todavia, com relação à apuração de PIS e COFINS, a situação demanda uma análise mais aprofundada, pelo menos em relação à apuração não-cumulativa de referidos tributos.

Ocorre que a Receita Federal, desde a instituição da não-cumulatividade de PIS e COFINS tem apresentado um entendimento bastante restritivo quanto à possibilidade de apropriação de créditos na sistemática da não-cumulatividade. Na verdade, como se podia ver nas Instruções Normativas nº 247/2002 e nº 404/2004 a Receita Federal restringia o conceito de insumos, utilizando definições análogas àquela presente na legislação de IPI.

No entanto, considerando que a materialidade do IPI (circulação de produtos industrializados ou introduzidos no território nacional pelo contribuinte) é substancialmente diversa daquela vinculada ao PIS e COFINS (auferimento de receita), é evidente que tais conceitos restritivos não poderiam ser validamente utilizados.

Por tal motivo, os contribuintes levaram a discussão ao Judiciário, sendo que em 21/11/2018, o Superior Tribunal de Justiça, no julgamento do Recurso Especial Repetitivo nº 1.221.170/PR, declarou, sob o rito dos recursos repetitivos, que o conceito legal de insumos abrange todos os bens e serviços essenciais ou relevantes à atividade-fim da pessoa jurídica, ainda que o seu emprego se dê de forma indireta no processo produtivo.

Ficou, dessa forma, assentado que o contribuinte faz jus ao crédito de PIS e COFINS sempre que determinado dispêndio for essencial ou relevante para sua atividade-fim, de modo que todos os gastos imprescindíveis para a produção/prestação de serviços poderão ser considerados como insumos.

Posto isto, em nossa opinião, em princípio, qualquer gasto incorrido pelo contribuinte com obrigações previstas pela legislação é capaz de gerar crédito a título de insumo, desde que empregados, ainda que indiretamente, na produção/prestação de serviços ligados à atividade final da empresa.

A Administração Fiscal, inclusive, em situações análogas, já se manifestou, de acordo com este entendimento, como se pode observar na Solução de Consulta COSIT nº 183/2019, na qual foi reconhecido que os Equipamentos de Proteção Individual (EPIs) podem ser considerados insumos, e na Solução de Consulta COSIT nº 1/2021, na qual foi definido que os gastos relativos a tratamento de efluentes, resíduos industriais e águas residuais indispensáveis à viabilização da atividade empresarial, em virtude de imposição da legislação, devem ser considerados insumos de produção.

Seguindo a mesma linha de raciocínio, mas, dessa vez, tratando especificamente dos gastos estabelecidos pela LGPD, a Justiça Federal já concedeu liminar em Mandado de Segurança reconhecendo a possibilidade de creditamento de PIS e COFINS sobre os dispêndios auferidos com a implementação de mecanismos e ferramentas para atendimento das obrigações estipuladas pela LGPD.

Obviamente, cada situação deve ser analisada individualmente, especialmente quanto à vinculação dos dados e seu processamento com o processo produtivo da empresa e mesmo com o auferimento de receitas. Isso porque as chances de aceitação dos créditos na esfera administrativa e na esfera judicial podem variar, caso a caso.

Ademais, justamente em função da variabilidade na probabilidade de recuperação dos créditos e mesmo por conta de diferentes perfis de cada empresa, diferentes estratégias podem ser analisadas.

Com efeito, as estratégias possíveis poderiam envolver desde a apresentação de consulta formal ao Fisco Federal ou a apresentação de mero pedido de restituição, até a elaboração de Declarações de Compensação ou mesmo a distribuição de medida judicial, cada uma com diferentes implicações em relação a custos, expectativa de aproveitamento e riscos.

Desse modo, entendemos que as empresas que investiram em sua adequação em relação à LGPD devem analisar se os dispêndios incorridos na adequação à nova legislação poderiam fazer jus à apropriação de créditos de PIS e COFINS e qual seria a melhor alternativa para sua eventual recuperação.

O CABIMENTO DE INDENIZAÇÃO POR DANOS MORAIS PELO VAZAMENTO DE DADOS PESSOAIS, À LUZ DA LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD) passou a vigorar plenamente em 01/08/2021 e, conjuntamente com sua chegada, adveio a possibilidade de aplicação das sanções previstas em seu artigo 52, em casos de infrações, especialmente em razão de vícios no tratamento de dados pessoais ou vazamento indevido, quais sejam:

I - advertência, com indicação de prazo para adoção de medidas corretivas:
II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
III - multa diária, observado o limite total a que se refere o inciso II;
IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI - eliminação dos dados pessoais a que se refere a infração;
X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Em razão das graves penalidades a que ficam sujeitos aqueles que não se adequarem aos padrões para o tratamento de dados pessoais previstos pela norma, bem como da ampla proteção conferida a estas informações, o número de demandas judiciais envolvendo a temática está crescendo exponencialmente.

A maior recorrência no Poder Judiciário até o momento, consiste em ações propostas pelos titulares dos dados, utilizando o rito de obrigação de fazer, ou pelo próprio Poder Público, em nome do coletivo, mediante a distribuição de ação civil pública. Ambas as medidas, no geral, visam um mesmo objetivo: a suspensão da divulgação dos dados pessoais disponibilizados indevidamente.

Além da suspensão de divulgação dos dados pessoais, diversos processos movidos pelos titulares pretendem ainda o recebimento de indenização, para reparação dos danos extrapatrimoniais experimentados em razão do vazamento de suas informações.

Importante consignar que, a indenização à título de danos morais, é apurada individualmente, para cada titular dos dados disponibilizados indevidamente que promover ação judicial com este pleito. Assim, um único vazamento de dados, pode gerar diversas demandas, propostas individualmente por cada um dos titulares que se sentir lesado.

Já a aplicação das sanções previstas no artigo 52, da LGPD, será realizada inicialmente de forma administrativa, pelo ato de vazamento de dados como um todo, mediante instauração de procedimento pela Autoridade Nacional de Proteção de Dados (ANPD).

Em que pese plenamente em vigor as penalidades, os processos administrativos para sua execução ainda pendem de regulamentação pela ANPD. Contudo, na hipótese de incidência desta sanção extrajudicial, ainda será cabível a instauração de procedimento judicial, visando a anulação da pena aplicada, em caso de ilegalidade, falta de provas ou inobservâncias procedimentais.

Fato é que, feito este breve paralelo sobre as penalidades previstas pela LGPD, será ainda possível que todos os indivíduos que se sintam lesados pelo vazamento de dados ou por vícios no tratamento destes, proponham medida judicial visando o recebimento de indenização por danos morais.

O grande questionamento que surge é, em quais hipóteses de vazamento ou problemas no tratamento de dados pessoais esta indenização será cabível?

Isso porque, autorizar o cabimento de reparação em todo e qualquer caso de defeito no tratamento de dados pessoais, geraria inúmeras demandas mercenárias, em que os titulares dos dados visam meramente enriquecer-se ilicitamente, sem que tenha havido efetivamente algum dano a sua esfera moral.

Nesse cenário, cabe ao Poder Judiciário afastar pedidos de indenização pelo vazamento e erros no tratamento de dados pessoais, sem que haja a efetiva comprovação de dano experimentado pelo seu titular.

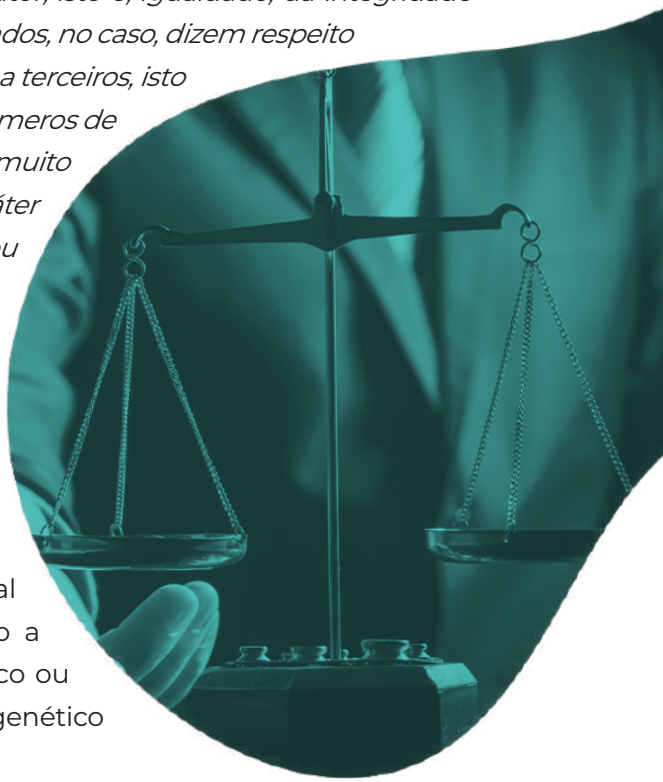
A jurisprudência ainda é escassa, não estando consolidada, contudo, para conferir uma diretriz no cabimento ou não de indenização por danos morais no vazamento de dados pessoais, podemos citar o acordão proferido em 16/11/2021, no julgamento do processo de autos nº 1008308-35.2020.8.26.0704, pela 27ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo.

No caso concreto analisado, em que pese reconhecida a violação cometida no vazamento de dados pessoais, afastou-se a pretensão de indenização, pela ausência de demonstração de prejuízo moral efetivo.

Na fundamentação do referido acórdão, para afastar o pedido indenizatório, o julgador salientou que os dados pessoais vazados no caso, não se configuravam como sensíveis, tendo sido divulgados indevidamente as seguintes informações: nome, número de CPF, data de nascimento, idade, telefones fixo e celular e endereço de e-mail.

O Tribunal de Justiça de São Paulo consignou ainda:

"O dano moral, ainda mais o sob uma perspectiva constitucionalizada do direito civil, somente se configura quando houver lesão à dignidade humana e seus substratos: liberdade, igualdade, solidariedade e integridade psicofísica. (...) No caso concreto, não está demonstrada a lesão a qualquer dos componentes da dignidade humana do autor, isto é, igualdade, da integridade psico física, da liberdade e da solidariedade. Os dados vazados, no caso, dizem respeito a informações essencialmente públicas ou de fácil acesso a terceiros, isto é, nome, CPF, data de nascimento e idade. Quanto aos números de telefone fixo e celular, bem como o endereço de e-mail, muito embora tais informações não sejam, em regra, de caráter público, também não revelam qualquer dado sensível ou que, por si só, possa comprometer a dignidade do autor, caso de conhecimento público."



Visando facilitar a compreensão desta tese, colaciona-se abaixo o conceito de dados pessoais sensíveis, definidos no artigo 5º, inciso II, da LGPD:

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Para aplicar este entendimento e afastar o dever de indenizar, de maneira inovadora, o Tribunal de Justiça de São Paulo, neste mesmo julgamento, destacou que a apuração da responsabilidade do fornecedor pelo vazamento de dados não pode se limitar a análise pela ótica tradicional, que se divide em objetiva e subjetiva, devendo ser sopesada a responsabilidade proativa, que assim conceituou o acordão:

Não se trata mais, como antigamente, de aplicação das regras da responsabilidade subjetiva ou objetiva, mas sim do que a doutrina vem definindo como responsabilidade ativa ou proativa, hipótese em que, às empresas não é suficiente o cumprimento dos artigos da lei, mas será necessária a demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas.

Ou seja, para a apuração da responsabilidade pelo vazamento de dados e, consequentemente, do dever de indenizar, o Tribunal de Justiça entendeu que é necessário sopesar se houve observância às práticas de preservação de informações, com adoção de mecanismos eficazes de proteção, mediante adequação da política interna da empresa, à luz da LGPD.

Deste modo, tem-se uma tendência de que o dever do agente de reparar o dano causado pela não observância à LGPD, envolvendo vícios no tratamento de dados pessoais, seja analisado por um regime de responsabilidade civil próprio.

Este regime de responsabilidade proativa, presume que o agente deve adotar meios preventivos eficientes para evitar problemas no tratamento de dados pessoais, sendo passível de responsabilização aquele que não aplicar mecanismos visando diminuir o risco de lesão.
Nesse sentido, o artigo 42, da LGPD, prevê a responsabilidade dos agentes, quando não houver a aplicação das normas para proteção de dados:

Art. 42. 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.

Não obstante, não está consolidado o entendimento traçado no julgamento analisado, havendo doutrinadores que entendem que o artigo supracitado da LGPD trata da teoria subjetiva da responsabilidade civil, somente sendo passível de responsabilização e, consequentemente, do dever de indenizar, o agente que comprovadamente possui culpa pelos danos decorrentes de falhas no tratamento de dados.

Outrossim, ainda que haja certa margem para entendimentos de que o artigo 42 indica uma aproximação da responsabilidade objetiva, por conta do trecho “em razão do exercício de atividade de tratamento de dados pessoais” não nos parece que seja a melhor interpretação, uma vez que a teoria do risco e, consequentemente a aplicação da responsabilidade objetiva sejam de aplicação excepcional a situações excepcionais, o que não se coadunaria com a questão do tratamento do dado pessoal enquanto suposto risco de atividade, visto que não se concebe atualmente praticamente nenhuma atividade que em alguma medida lide com informações de pessoas físicas.

Portanto, a aplicação da responsabilidade objetiva em razão da mera atividade de tratamento de dados pessoais, seria igualar todos os agentes de tratamento como se os riscos fossem os mesmos, quando na verdade isso não se impõe, considerando que a avaliação de risco em tratamento de dados requer análise contextual de natureza do dado e do titular, volumetria, finalidade entre outros aspectos do tratamento do dado pessoal.

Não obstante, ainda é cedo para definir qual teoria será adotada em definitivo para apuração do dever de indenizar, à luz da LGPD, mas há uma tendência de que, da mesma forma que a inovação trazida pela lei, a hipótese de responsabilidade adotada seja nova, adaptando-se as especificidades da norma, como proposto pela tese proativa.

IDEALIZADORES

Autores

Anelise Freitas Martins
Ramona Trindade Mera
João de Szentmiklósy Teixeira Nogueira
Gabriela Zanatta Alves Pereira
Ícaro Fernandes Oliveira
Mauro Roberto Martins Junior
Vanessa Cristina Ziggiatti
Ricardo Hiroshi Akamine
Aline Cavalcante de Souza Sanches

Coordenador de Conteúdo

Hélio Ferreira Moraes

Revisor

Diogo Silva Marzzoco

Contato

Sites: https://www.pk.adv.br/ | https://en.pk.adv.br/
E-mail: contato@pk.adv.br
Endereço: Av. Dr. Cardoso De Melo, 1340 · 12° Andar · Vila Olímpia · 04548-004 · São Paulo · SP
Telefone: 55 11 3054-1020

PINHÃO E KOIFFMAN ADVOGADOS

Direito que **viabiliza** tecnologia e inovação