REVISTA

GOVERNANÇA E COMPLIANCE

ACRJ

Publicação Oficial do Conselho Empresarial de Governança e Compliance da Associação Comercial do Rio de Janeiro

Número 8 | Ano 4 | abril 2021 | ISSN 2595-458X

LEI GERAL DE PROTEÇÃO DE DADOS - LGPD

REVISTA

GOVERNANÇA E COMPLIANCE ACRJ

A REVISTA GOVERNANÇA E COMPLIANCE é a publicação oficial do Conselho Empresarial de Governança e Compliance da Associação Comercial do Rio de Janeiro. Conta com a colaboração de especialistas em diversos temas para o debate e fomento da cultura da integridade, com o objetivo de produzir propostas para a melhoria do ambiente de negócios brasileiro.

ACRJ

Rio de Janeiro
Edição 8 – Ano 4 – abril de 2021
Associação Comercial do Rio de Janeiro

REVISTA GOVERNANÇA E COMPLIANCE

Publicação Oficial do Conselho Empresarial de Governança e Compliance
da Associação Comercial do Rio de Janeiro

EXPEDIENTE

Sumário

Palavra da Presidente

Caros Amigos,

A prioridade absoluta, em 2021, continua a ser o combate à pandemia do novo coronavírus. A chegada das vacinas nos dá a esperança de que aos poucos a vida voltará ao normal e a economia vai reagir. Enquanto isso, o mundo corporativo não pode ficar paralisado. Tem de olhar para frente.

Há que dar atenção às agendas de interesse estratégico para as empresas e para o desenvolvimento do país. É exatamente essa a preocupação da 8ª edição da Revista de Governança e Compliance da ACRJ, dedicada a um tema que está na ordem do dia: os efeitos da nova Lei Geral de Proteção de Dados Pessoais (LGPD).

A LGPD entrou em vigor em setembro do ano passado, com inspiração no regulamento europeu. Sua função é proteger e dar transparência ao tratamento dos dados pessoais.

Ao impedir que as empresas utilizem as informações sem o consentimento dos titulares, pessoas físicas ou jurídicas, e exigir que adotem uma série de cuidados no armazenamento dos dados, a LGPD torna-se o mais novo marco do compliance no Brasil. A montagem de estruturas de governança da informação é, sem dúvida, um grande desafio para as empresas.

A presente edição acerta em cheio ao concentrar seu foco na Lei Geral de Proteção de Dados Pessoais, com artigos de altíssima qualidade.

Boa leitura!

ANGELA COSTA
Presidente da Associação Comercial do Rio de Janeiro

Editorial

POR
HUMBERTO MOTA FILHO
Presidente do Conselho Empresarial de Governança e Compliance da ACRJ

CAROS LEITORES,

O tráfego de dados no mundo alcança números impressionantes. Segundo o International Data Corporation (IDC, 2014), os dados digitais criados, replicados e consumidos no mundo no período de um ano dobrarão de tamanho a cada dois anos. Em 2020, já estiveram no patamar de 44 zettabytes (ou 44 trilhões de gigabytes). Precisamos encontrar as melhores estratégias para fazer avançar uma agenda de governança da informação, já que não existe algo como uma receita única de sistema de governança ou de sistema de compliance.

No artigo que assino, proponho que a governança da informação seja aferida pelos elementos da segurança com a sugestão de algumas medidas e práticas que podem contribuir com o seu avanço em nosso país, a partir de dispositivos legais específicos.

Para debater a Lei Geral de Proteção de Dados Pessoais, a LGPD, a Revista Governança e Compliance chega em sua 8a edição abordando os diversos aspectos desta legislação. A tradicional publicação do Conselho Empresarial de Governança e Compliance, da Associação Comercial do Rio de Janeiro (ACRJ) escolheu este assunto por considerar de extrema importância para as instituições públicas e privadas, assim como para toda a sociedade.

Antecipadamente, registro aqui meu agradecimento pessoal, e em nome da ACRJ e do Conselho, aos especialistas que aceitaram o convite e contribuíram com seus artigos. São eles: Anderson de Paiva Gabriel, Andréa Pedrosa de Góes, Caio Ramalho, Sayera Gonzaga Voila Maganha e Walter Aranha Capanema.

Mais uma vez, não poderia deixar de agradecer à presidente Angela Costa, que nos apoia e incentiva a cada edição proposta da Revista. Também contamos sempre com o apoio do vice-presidente de Relações Institucionais e Conselhos Empresariais, José Domingos Vargas, dos conselheiros, autores e das equipes de Comunicação e de Conselhos Empresariais pela parceria sempre fundamental para a produção desta publicação, que já se tornou tradicional no meio.

Agradeço ainda o apoio institucional do Sebrae Rio.

Boa leitura!

PANDEMIA, LGPD E ESG

ANDERSON DE PAIVA GABRIEL

Juiz de Direito do Tribunal de Justiça do Rio de janeiro (TJRJ)

O ano de 2020 proporcionou muitas mudanças na vida dos brasileiros. Não só rotinas e dinâmicas especiais foram incorporadas, mas também novas palavras e expressões foram assimiladas no vocabulário cotidiano, a exemplo de pandemia e quarentena, além de alguns estrangeirismos como *lockdown*.

Ao longo do ano, contudo, outro tema passou a ser comentado com crescente frequência, a proteção de dados e, com ele, sempre vinha a menção a uma sigla: LGPD. Esse, talvez, seja um dos grandes motes do ano de 2021.

A LGPD, isto é, a Lei Geral de Proteção de Dados Pessoais[1] dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Aliás, as discussões envolvendo a proteção de dados talvez tenham sido potencializadas justamente pelo cenário pandêmico, em que mapas de calor passaram a ser divulgados para a população, com menção até a um suposto índice de isolamento. Houve preocupação com notícias apontando que uma empresa privada teria chegado a monitorar 30 milhões de celulares[2], sob o argumento de que os usuários teriam instalado voluntariamente aplicativos parceiros da empresa e consentido com a coleta de dados[3]. Em outro giro, só a cidade de Recife, por exemplo, teria rastreado pelo menos 700 mil celulares[4].

Nesse sentido, Paul Ohm[5], professor de Direito e pesquisador de Privacidade do Centro de Direito da Universidade de Georgetown, salienta ser impossível uma efetiva anonimização de dados precisos de localização, quando coletados ao longo de certo tempo.

Como se não bastasse, uma falha de segurança em um aplicativo de *contact tracing* no Catar expôs dados sensíveis de mais de um milhão de pessoas[6], enquanto nos Estados Unidos, na Dakota do Norte, descobriu-se que um aplicativo do gênero estava repassando dados para a Google e para o aplicativo *Foursquare*[7], o que revela que a preocupação não é sem fundamento ou desarrazoada.

Com efeito, o Times Privacy Project[8] se debruçou sobre um ar-

---

1 Lei nº 13.709, de 14 de agosto de 2018.

2 Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/05/18/lockdown-brasil-registra-alta-no-indice-de-isolamento-social-pela-1-vez.htm, último acesso em 30/11/2020.

3 Disponível em: https://mapabrasileirodacovid.inloco.com.br/. Acesso em 30/11/2020.

4 Disponível em: https://g1.globo.com/pe/pernambuco/noticia/2020/03/24/recife-rastreia-700-mil-celulares-para-monitorar-isolamento-social-e-direcionar-acoes-contra-coronavirus.ghtml. Acesso em 30/11/2020.

5 OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. UCLA Law Review 57 (2010). p. 1701/1777.

6 Disponível em: https://www.amnesty.org/en/latest/news/2020/05/qatar-covid19-contact-tracing-app-security-flaw/. Acesso em 30/11/2020.

7 Disponível em: https://www.newsbreak.com/news/coronavirus/0P7Uq7Na/north-dakotas-covid-19-app-has-been-sending-data-to-foursquare-and-google. Acesso em 30/11/2020.

8 Disponível em: https://www.nytimes.com/series/new-york-times-privacy-project. Acesso em 30/11/2020.

quivo contendo a compilação de dados de localização de mais de 12 milhões de americanos, abarcando seus deslocamentos por metrópoles como Washington, Nova Iorque, São Francisco e Los Angeles, durante um período de vários meses em 2016 e 2017, e refutou a suposta anonimização, segurança e consentimento em contundente matéria[9]. Na publicação, ressaltou-se, ainda, que esses dados podem mudar de mãos quase em tempo real, permitindo que alguém visualize um anúncio para um carro novo enquanto percorre uma concessionária. Além disso, esses dados podem ser revendidos, copiados, pirateados e utilizados de inúmeras formas abusivas, sem que o usuário possa recuperá-los.

E é nesse cenário que a LGPD demonstra todo o seu relevo para o Brasil contemporâneo, ainda que a sua aplicação seja expressamente excepcionada quando se tratar de tutela da segurança pública, defesa nacional, segurança do Estado ou de atividades de investigação e repressão de infrações penais.

Não se pretende aqui debater se alguns tratamentos de dados por governos e instituições no contexto pandêmico, assim como em parcerias entre agentes públicos e privados, teriam visado objetivos nobres, como conter o avanço da doença e acompanhar de forma mais eficiente pessoas já infectadas.

O que nos é relevante é a consciência que se espraia pela população, ainda que lentamente, de que os dados são o petróleo dos tempos atuais, configurando ativo extremamente valioso.

Nesse diapasão, proliferaram questionamentos, por exemplo, quanto à suposta gratuidade de alguns aplicativos de celular. Qual seria o interesse de um desenvolvedor em criar aplicativos se não auferisse qualquer valor com eles? Como bem aponta Bruce Schneier, em regra, quando o usuário não paga pelos aplicativos, é ele o produto. Com efeito, terceiros – vulgo parceiros comerciais – pagarão pelos dados de usuários coletados pelo app. Não é à toa que certos aplicativos, ao serem instalados, pedem inúmeras permissões, muitas das quais não têm qualquer pertinência para sua finalidade, a exemplo da permissão de acesso ao GPS para um aplicativo de edição de fotos. Todo esse processo ocorre sem que muitos se deem conta[10] e os debates só irão se intensificar com a vigência da LGPD.

A disciplina da proteção de dados pessoais, por expressa disposição legal, tem entre seus fundamentos não só o respeito à privacidade e à inviolabilidade da intimidade, da honra e da imagem, mas também o desenvolvimento econômico e tecnológico e a inovação, lastreando-se ainda na autodeterminação informativa.

Com o advento da LGPD, qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, terá de observar os inúmeros requisitos postos na legislação. Até mesmo o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

Além disso, a Lei estabeleceu que o titular dos dados tem direito ao acesso facilitado às informações sobre o tratamento

[9] Disponível em: https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html. Acesso em 30/11/2020.

[10] SCHNEIER, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. Nova Iorque: W. W. Norton & Company, 2016.

desses, incluindo a finalidade, forma e duração (observados os segredos comercial e industrial). Nesse sentido, deve ter acesso também à identificação do controlador e de seu contato.

Outra não é a razão pela qual o Conselho Nacional de Justiça editou a Recomendação Nº 73, de 20/08/2020[11], orientando aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas na LGPD, a exemplo da elaboração de um plano de ação, da disponibilização nos sites eletrônicos de informações básicas sobre a aplicação da Lei (incluindo os requisitos para o tratamento legítimo de dados, as obrigações dos controladores e os direitos dos titulares) e de formulário para exercício de direitos dos titulares de dados pessoais, e, ainda, de política de privacidade para navegação no website da instituição.

Ora, dentro desse cenário de revolução tecnológica e transformação digital, é inegável que o advento da LGPD consubstancia passo mais do que necessário na concretização dos valores constitucionais consagrados por nossa carta magna e que restavam, por vezes, ignorados no universo eletrônico. Todavia, também é indubitável que representará um grande desafio não só para as instituições públicas, mas principalmente no setor privado, tornando-se um dos grandes focos da governança e *compliance*.

No contexto atual, a despeito da importância do tratamento de dados para os mais variados segmentos da economia, há consenso de que informações pessoais devem ser processadas para finalidades legítimas, específicas, explícitas e informadas ao titular. Os titulares dos dados devem receber informações transparentes sobre as atividades de tratamento que estão sendo realizadas, os objetivos de sua realização e principais características, incluindo o período de retenção dos dados coletados. Ademais, as informações oferecidas devem ser acessíveis e que estar em linguagem clara e compreensível para os mais variados públicos. Por sua vez, os dados sensíveis necessitam mais do que nunca de uma tutela diferenciada e especial, de forma a se evitar que informações dessa natureza sejam vazadas, usadas indevidamente, comercializadas ou sirvam para embasar discriminações ilícitas ou abusivas em relação ao titular.

A nova fase da governança corporativa[12], focada no acrônimo ESG (environmental, social and governance), evidencia que o cidadão, também um consumidor, tem passado a exigir do empresariado mais que bons serviços ou produtos. À medida que a consciência do valor de dados se dissemina na população, a rápida e efetiva adequação de uma empresa aos preceitos da LGPD pode consubstanciar uma vantagem competitiva para as empresas que se preocuparem em proteger os dados de seus clientes[13].

Assim, a disciplina da proteção de dados não deve ser compreendida como óbice para o desenvolvimento econômico, efetivação de políticas públicas ou implementação de ferramentas tecnológicas, mas sim percebida como responsável por oferecer parâmetros, deveres e limites para que se consiga, em um mundo cada dia mais digital, proteger a dignidade da pessoa humana nos termos preconizados pela Constituição Federal de 1988.

[11] Disponível em: https://atos.cnj.jus.br/atos/detalhar/3432, último acesso em 30/11/2020.

[12] Disponível em: https://aesbe.org.br/esg-a-nova-fase-da-governanca-corporativa/. Acesso em 30/11/2020.

[13] Disponível em: https://www.nextlawacademy.com.br/blog/conformidade-a-lgpd-e-o-indice-esg-questoes-ambientais-sociais-e-de-governanca-vantagem-competitiva-para-as-empresas-brasileiras, último acesso em 30/11/2020.

PROTEÇÃO DE DADOS NA EDUCAÇÃO

ANDRÉA PEDROSA DE GÓES

Advogada. Pós-graduada na EMERJ

INTRODUÇÃO

A Internet e os computadores tornaram a nossa vida cada vez mais guiada por dados. Para fazer uma transação bancária, por exemplo, é necessário coletar a impressão digital. Por outro lado, em diversas outras situações realizadas no dia a dia, os dados pessoais estão sendo coletados sem, sequer, termos conhecimento de sua destinação, tampouco para qual finalidade esses dados são tratados.

Os dados, portanto, são indispensáveis para a nossa vida moderna, mas o seu uso tem sido abusivo.

Assim, com o intuito de tratar os dados pessoais da pessoa natural, foi promulgada a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), em 14 de agosto de 2018, que teve inspiração no Regulamento Europeu de Proteção de Dados (GDPR, sigla do nome em i). A função precípua da Lei é dar transparência ao tratamento dos dados pessoais e proteger os indivíduos, visando maior segurança jurídica às empresas e às pessoas, que são os titulares dos dados.

Mas, afinal, o que são dados pessoais? É a informação relacionada à pessoa natural identificada (dados que identificam diretamente uma pessoa, por exemplo: nome e sobrenome, endereço de email etc) ou identificável (uma informação, um dado desestruturado, mas que pode vir a identificar uma determinada pessoa, como o IP de uma máquina). Os dados pessoais sensíveis são aqueles que devem ser tratados com um cuidado ainda maior, porque dizem respeito à 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 vinculados a uma pessoa natural.

O tratamento de dados[1], portanto, é toda a operação realizada com o dado pessoal. É necessário que haja uma fundamentação jurídica permitindo esse tratamento. São as chamadas bases legais, que se encontram no artigo 7º da LGPD. Logo, sem a observância destas hipóteses legais, entre as quais se encontra o consentimento do titular, a necessidade para execução de um contrato, cumprimento de obrigação legal, não há que se falar que os dados estão sendo, legalmente, tratados.

Ressalta-se que se for tratar de dados pessoais sensíveis, as bases legais a serem observadas são as do artigo 11 da LGPD, dentre as quais, o consentimento específico e destacado do titular ou de seu responsável legal, para finalidades

---

[1] Artigo 5º, X – tratamento: toda operação realizada com dados pessoais como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[2] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

(...)

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador;b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

específicas e se não houver o consentimento do titular, a Lei discrimina as situações cabíveis[2].

Em relação à educação, é de grande relevância a questão do tratamento de dados pessoais, porque as instituições de ensino dependem destes, inclusive de dados sensíveis, para o próprio exercício da atividade, como será abordado ao longo do texto.

É importante mencionar os atores da LGPD, que são os denominados agentes de tratamento: o controlador e o operador. O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. É sempre o destinatário do dado pessoal. O operador é pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. A lei se refere, ainda, à figura do encarregado, pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), e pode ser um funcionário da empresa ou um terceiro, pessoa natural ou jurídica.

No presente artigo, importa analisar os impactos da LGPD na importantíssima atividade de ensino.

LGPD NO ENSINO

As instituições de ensino captam dados de alunos, pais e/ou responsáveis legais, funcionários, prestadores de serviços, visitantes e instituições parceiras. É de suma importância que o tratamento destes seja adequado, relevante, necessário.

Deve-se, ainda, justificar a finalidade a uma das bases legais, que se encontram no artigo 7º ou se for dado sensível, no artigo 11. Ademais, existem muitos dados de crianças e adolescentes sendo tratados, devendo ser observado o artigo 14 da referida Lei, eis que necessitam de um controle mais rígido no tratamento.

Dito isso, é recomendado que os dados coletados observem o conceito de data minimization, ou seja, restringir o máximo possível a coleta, afinal de contas há sempre um risco. Não olvidando a finalidade para qual estão sendo coletados. Assim, em um contrato de prestação de serviços educacionais, em regra, são coletados nome, e-mail, profissão, CPF, identidade, nacionalidade, endereço e telefone dos pais e/ou responsáveis. Pergunta-se: esses dados atendem à finalidade para o contrato de prestação de serviços educacionais? Se a resposta for afirmativa, então, são suficientes para a coleta.

Em seguida, verificar na Lei, artigo 7º, se há uma hipótese elencada que justifique esse tratamento. No presente caso, o inciso V dispõe quando necessário para execução do contrato.

Algumas instituições justificam o tratamento dos dados no contrato de prestação de serviços educacionais com base no consentimento. Não parece ser, nesta etapa, a melhor base legal. O consentimento, por praticidade e segurança, deve ser dado em último caso, já que pode ser, a qualquer momento, revogado pelo titular do direito.

No procedimento de matrícula, além dos dados mencionados no parágrafo acima, o nome do aluno e, muitas vezes, sua data de nascimento são coletados, igualmente. Sugere-se, portanto, que a matrícula seja feita em um formulário anexado ao contrato e que sejam incluídas cláusulas consentindo especificamente e de forma destacada, o tratamento de dados, em caso de crianças e adolescentes, bem como o

compartilhamento destes, para finalidades outras que não educacionais: para fins de marketing, comerciais.

Há instituições que coletam dados acerca do grau de escolaridade, data de nascimento, profissão, religião dos pais e/ou responsáveis. Lembrem-se que todos os dados colhidos são de responsabilidade do Controlador, que é a instituição de ensino. Logo, não tendo necessidade, não deve ser coletado. É interessante chamar atenção para o dado da profissão dos pais, pois esta identifica uma pessoa, especialmente quando há homônimos, tendo em vista que é possível determinar uma pessoa pela profissão. Por outro lado, em relação à religião do aluno, vê-se que, se for uma instituição religiosa, pode ter relevância, tendo em vista a diferença de credos. Contudo, por ser um dado sensível, terá de ter uma proteção mais cuidadosa.

Os dados coletados relativos à saúde do aluno, também, devem estar em um formulário à parte e ter um tratamento mais cauteloso por ser dado sensível. Então, tem que verificar quem vai acessar, onde ficará armazenado. Os dados pessoais, inclusive os dados sensíveis, não estão proibidos de serem coletados e tratados, desde que observados os regramentos da lei sob comento.

Se todo o procedimento acima estiver online, que esteja tudo previsto na política de privacidade do site, observando que o tratamento seja autorizado, a informação seja clara e destacada e justificando a finalidade à base legal.

Em se tratando de visitantes na instituição de ensino, os dados coletados devem ser ínfimos e descartados após a visitação. Se a marcação para as visitas for em agenda de papel, esta deve ficar guardada em uma gaveta, com tranca, e apenas o funcionário responsável ter acesso. A lei fala em dados pessoais, não fazendo distinção entre dados físicos ou digitais.

Em relação à transmissão de dados pessoais, como por exemplo, GFIP, DIRF, E-SOCIAL, por serem dados enviados por meio de uma obrigação legal, não há se falar em consentimento, estão respaldados nos artigos 7º,II e 11, II a) do Diploma Legal. Mesma justificativa ocorre no que diz respeito ao Censo da Educação realizada pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP).

TRATAMENTO DE DADOS PESSOAIS DE EMPREGADOS E COLABORADORES

Quando a instituição recebe um currículo ou durante o procedimento de seleção do candidato, os dados pessoais coletados devem ser o mínimo possível, inclusive, não indagando acerca de dados sensíveis. Ressalta-se, apenas, que o candidato deverá ser informado do tratamento dos dados e o tempo que estes ficarão armazenados. Se houver o interesse de manter o currículo do candidato em bancos de dados, este deve ser informado desta finalidade e consentir.

Os funcionários da instituição são regidos pelo contrato de trabalho e durante a vigência deste há tratamento de dados e a base legal é o próprio contrato de trabalho (execução de contrato), desde que não haja dados sensíveis envolvidos. Se houver tratamento destes, como dados de saúde, para oferecimento de um plano de saúde ao funcionário, esses dados poderão ser compartilhados, com base no artigo 11, parágrafo 4º da lei. Já o compartilhamento de dados a uma empresa contratada para fazer a

gestão da folha de pagamento do funcionário, por não ser um dado sensível, se justifica pela necessidade da execução de contrato, artigo 7º, inciso V da LGPD.

Como visto, praticamente, todas as áreas dentro da instituição serão afetadas pela LGPD, tais como, RH, TI, FINANCEIRA, ADMINISTRATIVA, PEDAGÓGICA.

A LGPD NAS ESCOLAS

Uma vez coletados os dados, tem que ser verificado seu fluxo dentro da entidade: onde são armazenados, quais são os tipos de dados, como são usados, por quem são usados etc. É a parte, propriamente, da implementação da lei. Em linhas gerais, o que deve ser observado nessa primeira etapa é a formação de workshops, é o momento que se faz uma análise de todos os processos de tratamento de dados da instituição, por meio de questionários avaliativos, realizações de entrevistas com funcionários que tratam dados pessoais. Recomenda-se que essa fase seja feita por áreas, que serão, posteriormente, reunidas, a fim de elaborar um parecer de análise, em que estarão identificados todos os processos, os gargalos, a vulnerabilidade técnico-jurídica (gapanalysis). É recomendada a designação, interna ou externamente, de um DPO.

Finalizada a fase de diagnóstico, será definida e implementada a governança. Neste momento, é que vai ser revista a política de privacidade e cookies, revisão dos contratos já estabelecidos, elaboração de termo(s) consentimento(s) bem como a permissão de acessos a sistemas e banco de dados, autorização para compartilhamento de dados, avaliação da finalidade do tratamento de dados e a correspondente base legal, feitura de um plano de resposta a incidentes de segurança da informação. Também, é quando se estabelecem as tecnologias necessárias à segurança da informação.

É de suma relevância, a instituição fazer uma avaliação acerca de dados pessoais no ecossistema de parceiros do seu negócio. Na contratação de serviços com terceiros, tem que se atentar para manter somente estabelecimentos que estejam em conformidade com a LGPD, ajustar todos os contratos com cláusulas mútuas de exigências de conformidade com a lei sob comento.

Se a instituição de ensino utilizar a ferramenta de armazenamento em nuvens, o provedor deste serviço deverá estar adequado à LGPD.

Com o advento da pandemia da COVID-19, as aulas online foram a opção para se dar continuidade ao aprendizado dos estudantes e mais uma vez, a observância à LGPD é imperativa, tendo em vista que dados como imagens, IP de conexão são coletados e usados. Dessa forma, escolhida uma plataforma para as aulas serem ministradas, é por ela que todas as comunicações deverão ser feitas.

CONCLUSÃO

Por fim, deve-se levar em consideração as sanções administrativas impostas pela Autoridade Nacional de Proteção de Dados (ANPD), em razão do descumprimento das normas por ela estabelecidas, dentre elas, multas, bloqueio e eliminação dos dados pessoais (artigo 52 da LGPD).

Diante do exposto, os benefícios da lei para as instituições e titulares dos dados foram positivos e o maior desafio, agora, é fazer com que a sociedade entenda a importância dessa temática e que se torne inerente a todos.

OPORTUNIDADES E DESAFIOS À LUZ DA LGPD

CAIO RAMALHO

Professor da FGV e coordenador do FGV NEST

Ao se observar as cinco marcas mais valiosas do mundo em 2020, percebe-se que nenhuma delas existia há 50 anos, sendo que três delas são ainda mais recentes, com menos de 30 anos. As marcas Apple, Google, Microsoft, Amazon e Facebook somadas são estimadas em US$ 842 bilhões[1], equivalente a, aproximadamente, metade do PIB do Brasil. E, dada a velocidade das transformações digitais que estamos vivendo, que têm se acelerado cada vez mais nos últimos 5 anos em função do rápido barateamento das tecnologias, é muito provável que as marcas que mais valerão daqui a 20 anos ainda nem tenham sido criadas.

De fato, houve uma explosão na quantidade de startups ao redor do mundo, a partir de 2014 a quantidade de unicórnios cresceu exponencialmente[2]. O termo, atualmente já conhecido por muitos, e que virou moda, foi cunhado em 2013 pela fundadora da Cowboy Ventures, Aileen Lee, para designar o quão árduo é o processo de investimento em startups pelos gestores de venture capital e, especialmente, ainda mais difícil encontrar e investir em startups que se tornam negócios bilionários[3]. Apple, Google, Microsoft, Amazon e Facebook um dia já foram startups e, por meio de rodadas de captação com investidores anjos e gestores de venture capital, tiveram o suporte necessário para crescerem e se tornarem, assim como centenas de startups nos dias atuais, unicórnios.

Embora Estados Unidos e China sejam responsáveis pela origem da maioria dos unicórnios, este é definitivamente um fenômeno global[4] que tem impactado e, principalmente, transformado – e até mesmo criado – diversos setores da economia mundial. De fato, a cada instante, surgem dezenas de milhares de startups ao redor do mundo que, por meio da criação e/ou utilização de novas tecnologias, estão sendo – ou serão em breve – responsáveis por rápidas e profundas transformações culturais e econômicas em nossa sociedade.

Mas como a Lei Geral de Proteção de Dados Pessoais (LGPD)[5] no Brasil se relaciona com esse fenômeno dos unicórnios?

Primeiro, é necessário entender que as startups de sucesso nascem a partir de grandes necessidades (ou problemas) reais da sociedade, as quais empreendedores visionários conseguem identificar como oportunidades de criação de soluções inovadoras para resolvê-las – como fizeram, por exemplo, os fundadores do Uber e do Airbnb. E não há dúvidas que ao estabelecer as diretrizes nacionais para coleta, armazenamento, tratamento e descarte de dados pessoais, a LGPD trouxe um imenso desafio às organizações, públicas e privadas – assim como a General Data Protection Regulation (GDPR) na Europa. De fato, a LGPD é (ou pelo menos poderia ter sido) o novo "bug do milênio"[6] em função das sanções, inclusive pecuniárias, pelo seu não cumprimento pelas organizações. Ademais,

[1] https://www.forbes.com/the-worlds-most-valuable-brands. Acesso em: 22/03/21.

[2] https://www.cbinsights.com/research/unicorn-tracker. Acesso em: 22/03/21.

[3] https://techcrunch.com/2013/11/02/welcome-to-the-unicorn-club. Acesso em: 22/03/21.

[4] https://www.cbinsights.com/research-unicorn-companies. Acesso em: 22/03/21.

[5] Lei nº 13.709/2018

[6] https://www.nationalgeographic.org/encyclopedia/Y2K-bug. Acesso em: 22/03/21.

a falta de preparo para se adequarem à LGPD foi acentuada pela rápida transformação digital nas organizações, esta imposta pelo isolamento social provocado pela pandemia da COVID-19 e que tornou as necessidades (e os problemas) ainda mais evidentes.

Porém, historicamente, as melhores startups surgem justamente em momentos de dificuldades (e oportunidades) como este. De fato, a LGPD tem sido um terreno fértil para o surgimento de novos negócios inovadores de alto impacto no Brasil, assim como ao redor do mundo por conta da GDPR. Usando tecnologia com o objetivo de endereçarem de forma inovadora grandes necessidades de mercado advindas, direta ou indiretamente, da LGPD, diversas soluções têm sido criadas por startups como, por exemplo, serviços de *compliance* e verificação de conformidade, controle e gestão de dados pessoais, plataformas de DPO[7] como serviço, entre outros.

Em segundo lugar, é necessário compreender que as startups necessitam de capital para se desenvolverem e, principalmente, crescerem de forma sustentável e acelerada, sendo que a falta de recursos é a segunda maior causa de mortalidade das startups ao redor do mundo[8]. Porém, uma vez que as startups usualmente não possuem ativos tangíveis para darem como garantia de empréstimos, torna-se necessário utilizar capital próprio, seja dos próprios fundadores ou então de novos sócios. Há diferentes formatos de captação de recursos com novos sócios, cada uma mais adequada de acordo com perfil, ciclo de vida e necessidade da startup, seja uma oferta pública (ex. *equity crowdfunding*[9]) ou seja por meio de negociações privadas (ex. investimento anjo[10] ou venture capital[11]).

Ao contrário do que a recente euforia sobre o assunto e os anúncios de novos unicórnios levam, erroneamente, as pessoas acreditarem, startups é sim um investimento de altíssimo risco de perdas (em média, de cada 10 negócios investidos, 30%-40% dão completamente errado) e que possui retornos esperados no longo prazo (7 a 10 anos; às vezes mais). Logo, os investidores de startups – pelo menos aqueles sérios e bem preparados, sejam profissionais ou semiprofissionais – buscarão duas coisas básicas: maximizar retornos esperados e mitigar riscos potenciais.

Na busca por retornos em seus investimentos, os gestores de venture capital e os investidores anjos procuram identificar as startups sensacionais, fundadas por empreendedores excepcionais, em mercados potencialmente muito grandes (como aqueles impactados pela LGPD, por exemplo). Esta, definitivamente, não é uma tarefa trivial, pois é necessário filtrar e investir em oportunidades que muitas vezes não são óbvios – quem imaginaria há alguns anos que o Uber ou o Airbnb poderiam dar certo? Muitos disseram "não" para esses investimentos.

Se por um lado a LGPD trouxe novas oportunidades de investimentos em startups, por outro também trouxe riscos relevantes.

---

7 Data Protection Officer (ou Encarregado da Proteção de Dados)

8 http://www.cbinsights.com/research/startup-failure-reasons-top. Acesso em: 22/03/21.

9 Instrução CVM 588/2017

10 Investidores anjos são pessoas físicas que investem seu capital próprio, atuando por meio de grupos ou associações, enquanto venture capital são gestores profissionais de recursos de terceiros para investimentos em startups que investem, normalmente, em startups que já mais desenvolvidas.

11 Historicamente, o capital inteligente (ou smart money) atribuído ao investimento anjo e ao venture capital tem sido responsável por alavancar o desenvolvimento inicial e o crescimento exponencial de milhares de startups ao redor do mundo, tais como Apple, Google, Facebook, Amazon, Microsoft, Uber e Airbnb, entre muitos outros.

A preocupação com falhas na LGPD de potenciais novos investimentos e, principalmente, de startups já investidas que constavam em seus portfólio, passou a ser prioridade antes mesmo da referida Lei ser promulgada. E como a Lei se estende a parceiros e fornecedores, o problema se tornou ainda mais crítico. Advogados foram consultados e especialistas foram convidados a opinarem sobre o tema. A pergunta-chave (e suas derivações) que teve que ser rapidamente adicionada no checklist usual dos processos de due diligence de novos investimentos foi: "seu negócio está aderente à LGPD"? O objetivo foi, naturalmente, a necessária mitigação de risco que rege o investimento consciente em startups.

Muitas startups estão se (re)estruturando para tentar ficar em conformidade com a LGPD, o que implica um potencial aumento de custos e despesas (dinheiro que a maioria delas não dispõem). Além disso, as estratégias comerciais e de marketing que utilizavam dados pessoais, e que impulsionavam o crescimento de diversas startups, tiveram que ser totalmente revistas (vários negócios desaceleram). O papel dos Conselhos nas startups, sejam Consultivos ou de Administração, passaram a ser ainda mais relevantes no acompanhamento da Governança Corporativa nos investimentos..

Isto posto, fica fácil imaginar o efeito negativo e potencialmente devastador que a insegurança jurídica (ex. atrasos na criação da Autoridade Nacional de Proteção de Dados (ANPD) e na publicação de sua estrutura regimental , indefinições quanto a manutenção da data de início ou o adiamento da LGPD , ações contra empresas com base na LGPD antes mesmo da sua entrada em vigor, etc.) pode representar, especialmente para negócios que já possuem riscos elevados como os investimentos em startups. De fato, é fundamental que se compreenda que os investidores estão dispostos a correrem os riscos inerentes aos negócios em si, porém não riscos oriundos de indefinições – ou pior, quebra de contratos – quanto ao arcabouço-jurídico institucional. Este risco é estranho ao propósito precípuo do investimento e serve, tão somente, para criar confusão e afastar o capital inteligente tão necessário para o crescimento exponencial das startups e, consequentemente, o desenvolvimento sustentável de longo prazo do Brasil.

LGPD E O IMPACTO NAS MICRO E PEQUENAS EMPRESAS

GABRIEL NOGUEIRA PORTELLA NUNES PINTO

Assessor da Ouvidoria do Sebrae Rio

Em agosto de 2018 foi sancionada a Lei nº 13.709, popularmente conhecida como Lei Geral de Proteção de Dados Pessoais ou simplesmente LGPD. A nova legislação brasileira foi inspirada em outra lei igualmente conhecida no Brasil por sua sigla, a GPDR (General Data Protection Regulation) - norma que regulamenta a proteção de dados pessoais, no âmbito da União Europeia.

Não há dúvidas que a legislação tem suma importância e faz parte de um movimento necessário de regulação das relações sociais, humanas, jurídicas e políticas no ambiente virtual, muito embora não se limite a ele. Isso porque seu objetivo é regular o uso, coleta, armazenamento e compartilhamento de dados das pessoas físicas, por empresas e instituições, públicas e privadas, bem como por pessoas humanas quando no desenvolvimento de atividades econômicas e políticas. Faz sentido regular a obtenção de dados físicos, pois uma vez obtidos, seja pelo meio que for, sua potencial circulação é instantânea a partir do mais simples processo de digitalização.

Na atualidade, os dados pessoais possuem enorme valor agregado e são estratégicos para ações comerciais e políticas. O leitor que tiver interesse em compreender melhor a importância econômica e política dos dados pessoais no mundo contemporâneo, deve assistir aos filmes "Privacidade Hackeada" e "O Dilema das Redes".

A par de sua inquestionável relevância, a LGPD entrou em vigor em um momento no mínimo inoportuno, em 18 de setembro de 2020, durante a maior crise sanitária dos últimos cem anos, com impactos econômicos ainda imensuráveis, mas certamente enormes, no qual a maioria das empresas luta pela sobrevivência, especialmente os Microempreendedores Individuais, as micro e pequenas empresas que possuem baixo capital de giro e acesso ao crédito insuficiente para suportar uma instabilidade tão longa.

Mesmo desconsiderando o contexto atual, a Lei brasileira pressupõe uma maturidade de processos, fluxos e organização das empresas que não refletem a realidade do pequeno empresário brasileiro.

Diante das alterações promovidas na LGPD pela Lei 13.853, de dezembro de 2019, que previu

que a Autoridade Nacional de Proteção de Dados (ANPD) poderia promover o tratamento favorecido e diferenciado aos pequenos empreendedores com relação às obrigações da lei em debate, o Sebrae e o Ministério da Economia (ME)organizaram um grupo de trabalho, composto por seguimentos representativo da economia do país e da sociedade civil organizada para propor uma regulamentação adequada para esse setor Entre as entidades convidadas estão a Ordem dos Advogados do Brasil (OAB), a Confederação Nacional do Comércio (CNC), a Confederação Nacional de Dirigentes Lojistas (CNDL), entre outras.

A proposta entregue à ANPD propôs a ampliação de prazos para cumprimento de obrigações, a adoção de medidas educativas antes da aplicação de sanções e a dispensa de obrigações, como por exemplo, a necessidade da empresa possuir um profissional encarregado pela função de Proteção de Dados Pessoais.

Enquanto a proposta é analisada pelo órgão, o empreendedor precisa ficar atento às ações do Sebrae, no que concerne à capacitação e apoio às micro e pequenas empresas na implantação das novas obrigações legais, além de conhecer a lei e acompanhar as atividades de divulgação de informações e compartilhar com seus funcionários.

MUITO ALÉM DA LGPD: A GOVERNANÇA DA INFORMAÇÃO CORPORATIVA

HUMBERTO MOTA FILHO

Advogado, Presidente do Conselho Empresarial de Governança e Compliance da ACRJ e do Comitê de Estudos da Transparência Pública da OAB/RJ

INTRODUÇÃO

Segundo o International Data Corporation (IDC, 2014), os dados digitais criados, replicados e consumidos no mundo no período de um ano dobrarão de tamanho a cada dois anos e, em 2020, encontravam-se no patamar de 44 zettabytes (ou 44 trilhões de gigabytes). Novos marcos legais e a expansão do universo digital obrigam as organizações a reavaliar suas estratégias em relação à guarda e uso da informação. Governos, empresas e indústrias estão se tornando mais digitais, dependentes das novas tecnologias de comunicação e conectividade, em um contexto caracterizado pelo crescimento acentuado no volume e na complexidade dos dados. Nessa sociedade do conhecimento, tanto as novas oportunidades quanto os novos desafios colocados levam a seguinte pergunta: como gerar valor para as organizações, a partir do gigantesco universo digital (FARIA e SYMPSON, 2013)? Uma possível resposta é investir na governança da informação.

Se a abundância de informação nas organizações oferece um grande potencial de desenvolvimento social e econômico ela também traz riscos operacionais e legais que precisam ser geridos e mitigados. É fundamental investir em governança para criar estratégias, políticas e procedimentos em torno da distribuição da informação dentro e fora das organizações. Em termos gerais, é possível afirmar que a governança da informação é o conjunto de normas, diretrizes e controles de responsabilidade desenvolvidos para assegurar o valor, a qualidade e o compliance das informações. Associada tanto à governança pública quanto à corporativa; a governança da informação está intimamente relacionada aos princípios da transparência e da prestação de contas (accountability), pois tanto cidadãos, quanto executivos e governantes necessitam de informações confiáveis para a tomada de decisões e para assegurar que seus dados estão protegidos e não foram adulterados, corrompidos, destruídos, descartados ou tratados e armazenados de forma indevida. Daí se revela a importância de outra indagação presente em todas as organizações nos dias de hoje: Como tratar dados com segurança jurídica?

Usualmente o termo dados é utilizado como um sinônimo do vocábulo informação, mas há também quem reconheça uma distinção semântica importante (DONEDA, 2014). Ao fazer-se essa distinção, o termo dado ganha uma conotação mais fragmentada, sugerindo uma informação em estado potencial, antes de ser transmitida ou um estado de "pré-informação", anterior à interpretação e a um processo de elaboração, enquanto o vocábulo informação alude a algo além da representação contida no dado, sendo capaz, pode isso mesmo, de se revestir de sentido instrumental e fornecer conteúdo voltado à redução de incertezas. De todo modo, em busca de uma estratégia para o tratamento de dados com transparência e segurança jurídica, é preciso ter em mente todo o ciclo de vida dos dados. Significa dizer que a organização deve ser capaz de assegurar o

valor, a qualidade e o compliance dos dados ou informações necessárias às suas atividades ao longo do tempo, desde o momento da decisão em tratá-los, até quando da escolha em se eliminar certo dado ou informação de seus arquivos.

Então, cabe indagar quais são as melhores estratégias para fazer avançar uma agenda de governança da informação, especialmente uma vez que não existe algo como uma receita única de sistema de governança ou de sistema de compliance (MENZEL, 2005).

Este artigo sugere um caminho que favoreça a busca dessa resposta, a partir de alguns marcos legais brasileiros e critérios objetivos que possam ser seguidos por empresas na governança das suas informações, em especial na coleta, tratamento, armazenamento e eliminação de documentos e dados. Nesse sentido são sugeridas quais as lógicas reitoras das políticas corporativas voltadas a essa modalidade de governança, no campo da transparência e da segurança da informação e são destacadas algumas de suas principais diretrizes, controles e responsabilidades.

Nesse artigo, propõe-se que a governança da informação seja aferida pelos elementos da segurança da informação e são apontadas algumas medidas e práticas que podem contribuir com o seu avanço em nosso país, a partir de dispositivos legais específicos.

INFORMAÇÕES SEGURAS: A LÓGICA DA CONFIANÇA

Segundo o dilema da confiança (MOTA FILHO, 2018), explorado por Ovanessoff, Plastino e Faleiro (2015), é preciso de confiança para cooperar, entretanto, também é preciso cooperar para ganhar confiança, seja na interação entre agentes públicos, agentes privados ou na interação entre agentes públicos e privados. E, de uma maneira geral, estudos apontam que a maioria dos brasileiros têm dificuldades no estabelecimento de novas relações de confiança (CNI, 2014) e que mesmo as empresas brasileiras , consideradas inovadoras, colaboram menos com outras organizações nacionais ou internacionais do que as empresas de grande parte dos países da OECD. Essas lacunas na confiança social acabam por comprometer a colaboração necessária nas relações negociais. Por seu turno, nas relações público-privadas não há razão para supor que o quadro é muito melhor.

Mais recentemente, foi feita uma pesquisa nacional a fim de investigar qual o nível de confiança dos brasileiros em suas instituições, especificamente entre as ONGs, empresas, mídia e governo (ETB, 2017). É revelador notar que nenhuma dessas organizações atingiu níveis satisfatórios de confiança. As ONGs e as empresas ao menos não despertaram a desconfiança entre os brasileiros, contudo a mídia e o governo não merecerem a confiança dos brasileiros. Essas pesquisas ainda revelaram que os brasileiros consideram as suas fontes oficiais suspeitas. A maioria dos consultados acredita que os indivíduos são mais confiáveis que as instituições, e que as informações vazadas têm mais credibilidade que os comunicados das companhias para a imprensa.

Ainda que essa crise de confiança seja global, a chamada era da economia da reputação (FAGUNDES, 2017) parece intensificar suas consequências no ambiente empresarial brasileiro. Nessa nova economia da reputação, 84% do valor de mercado de uma empresa listada no S&P 500 dos EUA estão atrelados

a valores intangíveis como a reputação, e o Brasil não parece fugir dessa tendência. Os riscos reputacionais estão no topo das preocupações dos membros dos Conselhos de Administração e segundo pesquisas internacionais, as principais causas da perda de reputação são os comportamentos à margem da ética e da integridade (DELOITTE, 2014). Sem sombra de dúvida, no meio empresarial a confiança é um ativo valioso e a falta de ética é um passivo fatal, um ambiente geral de baixa confiança social, como no caso brasileiro, afeta negativamente a sociedade, os negócios e o governo.

Todos esses dados indicam a necessidade de mais governança pública e corporativa, ou seja, as soluções para o problema da confiança precisam ser legitimadas por uma agenda de mudança dos processos decisórios que incluam a sociedade desde o início das discussões. É preciso retomar níveis de confiança satisfatórios que permitam um ambiente propício ao debate público e ao desenvolvimento de mais negócios e investimentos em nosso país. É fundamental enfrentar o problema da confiança, com o diagnóstico e com as ferramentas certas.

Para avançar nessa agenda de mudança dos processos decisórios que fortalecem os laços de confiança sociais, a lógica da accountability é fundamental, mas não é suficiente. Uma estratégia efetiva para o avanço da governança da informação pede que, junto com a transparência das informações, esteja também associada à sua segurança, assim será possível ganhar a legitimidade e a credibilidade necessárias para vencer o problema da confiança (MOTA FILHO, 2018). Políticas públicas e corporativas podem auxiliar a fortalecer a segurança das informações utilizadas pelas organizações.

POLÍTICAS CORPORATIVAS PARA INFORMAÇÕES MAIS SEGURAS

A informação pode ser entendida como um bem das organizações com finalidades econômicas, na medida em que ela é necessária para o planejamento e a implementação de estratégias empresariais, com a consequente realização dos negócios e a obtenção do lucro. Mas isto é apenas parte da história. Até recentemente, o mercado tratava os dados coletados como um ativo próprio, a ser livremente utilizado e comercializado por quem deles se apropriasse, sem maiores preocupações. Entretanto, na sociedade do conhecimento, essa perspectiva se alterou. Sob uma ótica mais cuidadosa e consciente da titularidade dos dados pessoais e das potenciais consequências do seu uso indevido houve recentemente uma mudança substancial na regulação do uso de dados pessoais nos negócios empresariais, sintetizada no marco legal da LGPD. Assim, os dados pessoais coletados pelas empresas privadas revelam-se claramente como pertencentes às pessoas naturais às quais se referem, de modo que quem coleta os dados deve prestar contas do seu uso ao seu titular, seja ele seu consumidor, seu empregado, seu acionista, ou quem quer que seja. Nessa linha, o uso de dados pessoais por empresas deve respeitar as bases legais da nova LGPD, sob pena de imposição de multas pesadas aos seus infratores e risco de perdas reputacionais adicionais.

No mundo empresarial, uma estrutura de governança da informação deve atribuir responsabilidades claras pela custódia dos dados e seu fluxo de vida na corporação, integrando as áreas de

negócio com as tecnologias existentes e com os projetos de tecnologias futuras, em bases jurídicas seguras. Não há um formato único para tal estrutura. As contingências as quais a organização está exposta, seja na relação com o ambiente externo, seja na conexão com a estrutura organizacional interna, certamente afetam a sua configuração estrutural.

Apesar de não haver uma receita única para proteger dados nas organizações privadas, especialistas internacionais sugerem uma estratégia voltada ao desenvolvimento da segurança da informação, baseada na implementação de um conjunto de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware, a fim de assegurar que os objetivos do negócio sejam atendidos. A nova LGPD parece seguir essa mesma estratégia recomendada pelos especialistas[1] . Nesse sentido, a segurança da informação compreende técnicas de tecnologia da informação, mas não se esgota nelas.

Pela LGPD, além da boa-fé, as atividades de tratamento de dados pessoais devem seguir diversos princípios, dentre os quais se destaca aqui o princípio da segurança[2]. Assim sendo, tanto o controlador, responsável pelas decisões referentes ao tratamento desses dados, quanto o operador, responsável pelo tratamento dos dados em nome do controlador, são legalmente designados como os agentes de tratamento de dados incumbidos de implementar a política de proteção de dados da sua organização, ao adotarem as medidas de segurança técnicas e administrativas. As medidas técnicas circunscrevem-se ao campo da tecnologia da informação, com o uso de recursos informáticos dotados de funcionalidades voltadas à garantia da segurança da informação, tais como ferramentas de autenticação de acesso a sistemas, recursos de criptografia e segregação de servidores. Já as medidas administrativas englobam medidas gerenciais e jurídicas, tais como as políticas corporativas para a proteção de dados, contratos de confidencialidade e políticas de privacidade (JIMENE, 2019).

Os agentes de tratamento de dados pessoais, no âmbito de suas competências, individualmente ou por meio de órgãos colegiados, poderão formular e implantar regras de boas práticas e de governança que estabeleçam as condições, o regime de funcionamento, os procedimentos, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento dos dados, além das ações educativas, dos mecanismos internos de supervisão e de mitigação de riscos e de outros aspectos relacionados ao mapeamento e tratamento dos dados pessoais. Essas regras integrarão tanto a política de governança da informação quanto o programa de integridade da empresa, revelarão e documentarão o seu grau de comprometimento com a proteção de dados pessoais e eventualmente excluirão ou reduzirão a aplicação das penalidades impostas às empresas pelos incidentes de segurança da informação e seus possíveis danos pela Autoridade Nacional de Proteção de Dados[3].

Ao impor aos agentes de tratamento o dever de adotar medidas de segurança aptas a resguardar os dados pessoais, a LGPD incorpora os mesmos pilares da segurança da informação expressos na Política Nacional de

[1] Associação Brasileira de Normas Técnicas. NBR ISSO/IEC 27002: Tecnologia da Informação – Técnicas de Segurança. *Código de prática para controles de segurança da informação*. Rio de Janeiro, 2013.

[2] Art. 6º, incisos VII, VIII e X da Lei nº 13.709/2018.

[3] Parte da inspiração para formular as regras de boas práticas e de governança pelos agentes de segurança pode vir da Norma Técnica ABNT NBR ISSO/IEC 27002, da Associação Brasileira de Normas Técnicas, um verdadeiro código de boas práticas e melhores técnicas mundialmente reconhecidas para controles de segurança da informação.

Segurança da Informação (PNSI), assimilando a ideia de que tal segurança é uma questão que vai muito além da tecnologia e representa um verdadeiro desafio de governança e de política corporativa.

Assim como visto no setor público, é preciso prevenir e ter condições de mitigar os casos de incidentes de segurança que possam acarretar riscos ou danos relevantes aos titulares das informações utilizadas pelo setor privado. Vale repetir que o controlador dos dados pessoais tem o dever de comunicar a ocorrência de incidentes de segurança para a Autoridade Nacional de Proteção de Dados (ANPD) e para o titular dos dados pessoais, sempre que o incidente de segurança "possa acarretar risco ou dano relevante aos titulares", em um prazo razoável. Então, sob a ótica jurídica, para justificar a sua comunicação o incidente de segurança deve ser capaz: (i). de possibilitar a ocorrência de um perigo ou sinistro causador de dano ou prejuízo, suscetível a acarretar a responsabilidade civil na sua reparação e; caso tal incidente se efetive, (ii). os impactos negativos ou prejuízos sofridos sejam potencialmente expressivos, ao atingirem bens de ordem econômica ou moral.

No âmbito da LGPD, nem todo e qualquer incidente deve ser comunicado. No caso da perda de um pen drive, o furto de um notebook ou a interrupção de acesso a um sistema haverá um incidente de segurança do ponto de vista técnico, no âmbito da governança da tecnologia da informação, pois os dados corporativos estarão ameaçados de exposição, entretanto não necessariamente esse incidente será digno de notificação à ANPD ou aos titulares de dados, caso não se revele como uma potencial ameaça de dano aos titulares de dados pessoais, passível de reparação civil. Uma boa governança da informação conjugada com um programa de integridade efetivo deve ser capaz de mapear dentre os potenciais incidentes de segurança de informação aqueles mais relevantes e impactantes para a corporação e para os titulares dos dados pessoais envolvidos e suas possíveis consequências, com a confecção de planos preventivos e de contingência.

Seguindo a lógica da proteção jurídica no tratamento de dados, há regulamentações específicas para atividades intensivas no uso de dados pessoais como a atividade bancária, com muitos riscos de incidentes de segurança potencialmente relevantes e volumoso tráfego de dados digitais, ao redor do mundo todo, ensejando possíveis danos de grande monta. As instituições financeiras ("IFs") devem conhecer seus clientes para avaliar o risco de crédito dos seus mutuários na concessão de financiamentos ou para evitar operações de lavagem de dinheiro, por exemplo. Para tanto, tais instituições devem seguir as regulamentações do Banco Central do Brasil, a autoridade responsável pelo sistema financeiro nacional, em especial os normativos que tratam da Política de Segurança Cibernética (PSC) e sobre os requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem[4].

Vale notar, que essa PSC contempla: (i). os procedimentos e os controles adotados para reduzir a vulnerabilidade das IFs aos incidentes; (ii). os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis; (iii). o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes

[4] Resolução nº 4.658/2018, do Banco Central do Brasil.

relevantes para as atividades da instituição; e (iv). os mecanismos para disseminação da cultura de segurança cibernética nas IFs. A PSC vem confirmar que a manutenção da segurança da informação decorre de uma estratégia corporativa e de uma mudança de cultura e não somente de investimentos em novas tecnologias e oferece um roteiro para avançar na implementação dessa estratégia baseada no reconhecimento da importância da proteção de dados para a credibilidade do sistema financeiro como um todo, para a estabilidade dos negócios bancários e o desenvolvimento de novos modelos de negócios que favorecem o crescimento dessa atividade econômica.

Nessa linha, a PSC pode servir de inspiração para outros ramos de atividades econômicas que necessitem estar apoiados em sólidas medidas de segurança da informação. Em termos mais gerais, no âmbito da lógica da LGPD e dos seus limites rígidos no tratamento de dados pessoais, as medidas de segurança serão mais efetivas quando observadas desde a concepção do produto ou do serviço próprio de cada atividade empresarial. Não por acaso, a LGPD acolhe a ideia de privacy by design (CAVOUKIAN, 1990), ou seja, o desenho e o desenvolvimento de novos produtos, serviços ou mesmo modelos de negócios precisam levar em conta a segurança e o sigilo dos dados como um elemento essencial de seus projetos corporativos, desde o seu início. Isso permite a adoção de controles mais efetivos, favorece o mapeamento e a auditoria dos riscos e estimula uma mudança organizacional nas empresas com maior respeito a privacidade das pessoas naturais. Mais particularmente, a ideia de privacy by design pode assegurar não apenas o cumprimento de parâmetros regulatórios e o compliance da proteção de dados, mas servem para direcionar o agente de tratamento de dados rumo a políticas corporativas que efetivamente avaliem os impactos das atividades empresariais nos usuários de seus produtos e serviços e nos terceiros interessados. Tais políticas corporativas poderão transformar os processos de criação, desenvolvimento, aplicação e avaliação de produtos e serviços e, portanto, serão capazes de criar informações com mais valor internamente para a organização e externamente para o mercado. Informações mais seguras juridicamente tendem a diminuir a litigiosidade processual e reduzir os riscos reputacionais das atividades empresariais e, desse modo, será possível avaliar os benefícios concretos do avanço da governança da informação em tais empresas.

CONSIDERAÇÕES FINAIS

O emprego da lógica dos laços de confiança contribui para o tratamento de dados de forma transparente e segura no setor privado. Os marcos legais e as boas práticas de mercado existentes já servem de guia para a identificação das normas, diretrizes e dos controles de responsabilidade aplicáveis aos dados. A partir daí, é fundamental traçar as estratégias para desenvolver e aplicar políticas corporativas que contribuam para o valor, a qualidade e o compliance das informações.

Políticas corporativas para proteger dados nas organizações privadas demandam uma estratégia voltada ao desenvolvimento da segurança da informação, baseada na implementação de um conjunto de controles, in-

cluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware, a fim de assegurar que os objetivos do negócio sejam atendidos. A segurança da informação compreende tecnologia, tal como a criptografia, mas não se esgota nelas. Tais políticas englobam além das medidas técnicas, a adoção de medidas administrativas, a fim de prover segurança jurídica em contratos de confidencialidade, políticas de privacidade e na caracterização de incidentes de segurança, por exemplo.

REFERÊNCIAS

CAVOUKIAN, Ann. *Information and Privacy Comissioner of Ontario*. Publicado em agosto de 2009. Revisado em janeiro de 2011. Disponível em: www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

CONFEDERAÇÃO NACIONAL DA INDÚSTRIA (CNI). *Retratos da Sociedade Brasileira: Confiança Interpessoal*, março de 2014.

DONEDA, Danilo. *O Direito Fundamental à Proteção de Dados Pessoais*, In Direito Privado e Internet. Coordenador: Martins, Guilherme Magalhães. Ed Atlas. São Paulo, 2014, p. 63.

ETB. 2017. Edelman Trust Barometer. Trust and the CEO. Annual Global Study, 2017. https://www.ifac.org/system/files/uploads/Comms/Day%201%20-%20Trust%20Barometer%20-%20Justin%20Blake.pdf.

FAGUNDES, Suzana. *Integridade como novo paradigma da reputação*. Revista Governança e Compliance da Associação Comercial do Rio de Janeiro. n. 1, ano 1 (5 dez, 2017). Rio de Janeiro, RJ: ACRJ, 2017. pgs. 30-34.

FARIA, F. A.; SYMPSON, G. (2013). *Bridging the gap between business and IT: An information governance perspective in the banking industry*. In N. Bhansali, Data governance: Creating value from information assets (pp. 217-241). Boca Raton, USA: Taylor & Francis.

DELOITTE. Global survey on reputation risk (em itálico), 2014. Disponível em: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/gx_grc_Reputation@Risk%20survey%20report_FINAL.pdf. Acesso em: 22/03/21.

IBGC. Instituto Brasileiro de Governança Corporativa. IBGC, *Código das Melhores Práticas de Governança Corporativa*, 2015.

IBGC. Instituto Brasileiro de Governança Corporativa. *Compliance à luz da governança corporativa* / Instituto Brasileiro de Governança Corporativa. São Paulo, SP: IBGC, 2018. (Série: IBGC Orienta). 56 p.

IDC. International Data Corporation. (2014). The digital universeofopportunities: Rich data andtheincreasingvalueofthe internet ofthings. http://brazil.emc.com/leadership/digitaluniverse/2014iview/executive-summary.htm. Acesso em: 22/03/21.

IIRC. 2013. A Estrutura Internacional para Relato Integrado. Tradução: FEBRABAN - Federação Brasileira de Bancos. Março, 2014. https://integratedreporting.org/wp-content/uploads/2015/03/13-12-08-THE-INTERNATIONAL-IR-FRAMEWORK-Portugese-final-1.pdf.

JIMENE, Camilla do Vale. In: *LGPD: Lei Geral de Proteção de Dados comentada*. Viviane Nóbrega Maldonado, Renato Opice Blum, coordenadores. São Paulo: Thomson Reuters Brasil, 2019.

MENZEL, Donald C. (2005) Research on Ethics and Integrity in Governance: A Review and Assessment, Public Integrity, 7:2, 147-168. http://dx.doi.org/10.1080/10999922.2005.11051272. Acesso em: 22/03/21

MOTA FILHO, Humberto E. C. *Como manter um ambiente ético nas empresas?* In: Revista Compliance Rio. n. 1, ano 1 (out, 2018). Rio de Janeiro, 2018. pgs. 30-37.

MOTA FILHO, Humberto E. C.; ALFRADIQUE, Cláudio Nascimento. *A Governança e o controle da função pública: a transparência pública nos trinta anos da Constituição Cidadã*. In: Estado, democracia e direito no Brasil: trinta anos da constituição cidadã. Geraldo Tadeu Moreira Monteiro (Org.). Rio de Janeiro: Gramma. Cebrad, 2018.

MOTA FILHO. *Compliance e Transparência: Programas de Integridade Efetivos*. In: Compliance: o estado da arte – regulações, práticas, experiências e propostas para o avanço da cultura da integridade no Brasil e no mundo. (Orgs.). Cláudio Carneiro, Humberto E.C. Mota Filho. Curitiba: Instituto Memória. Centro de Estudos da Contemporaneidade, 2019. 192 p.

OVANESSOFF, Armen. PLASTINO, Eduardo e FALEIRO, Flaviano. *Por que o Brasil precisa aprender a confiar na inovação colaborativa*. Accenture, 2015.

IIRC. 2013. A Estrutura Internacional para Relato Integrado. Tradução: FEBRABAN - Federação Brasileira de Bancos. Março, 2014. Disponível em: https://integratedreporting.org/wp-content/uploads/2015/03/13-12-08-THE-INTERNATIONAL-IR-FRAMEWORK-Portugese-final-1.pdf. Acesso em: 22/03/21.

COMPLIANCE E LGPD: A INDISPENSÁVEL CRIAÇÃO DO PLANO DE ADEQUAÇÃO

SAYERA GONZAGA VOILA MAGANHA

Advogada, Coordenadora Adjunta e Delegada de Prerrogativas de Processo Eletrônico e de Inteligência Artificial da OAB/RJ

Compliance vem do verbo inglês comply, que quer dizer agir ou atuar de acordo com as regras e, no mundo corporativo, compliance tem efetivamente, relação com a conduta da empresa e a sua adequação com todas as leis aplicáveis ao seu negócio.

Deste modo, o compliance surge, então, com um papel de maior relevância, face às grandes mudanças trazidas pela Revolução Industrial que ocasionou uma série de inovações tecnológicas, impactos globais nos âmbitos social, econômico, político e legislativo, que trouxeram para todos, maior conscientização de estar totalmente em consonância com às leis e normas éticas que lhe são aplicáveis, a fim de evitar as chamadas violações.

E, nesse contexto, a Lei Geral de Proteção de Dados Pessoais (nº: 13.709/2018), também conhecida por LGPD, que entrou em vigor no dia 18 de setembro de 2020, surge como novo paradigma de conformidade no Brasil, tendo como objetivo proteger a privacidade dos titulares dos dados e impedir que empresas abusem das informações adquiridas, utilizando-as sem o consentimento do titular ou tornando públicos dados sensíveis.

Por este motivo que o compliance é uma das áreas que mais estão sendo afetadas com a entrada em vigor da lei, vez que ela vem regulamentar sobre como as companhias devem colher, tratar, armazenar, transferir e usar dados de clientes, funcionários, visitantes de sites e mídias sociais, isto é, o compliance surge na perspectiva de "guardião" da Lei Geral de Proteção de Dados Pessoais.

A LGPD estabelece a necessidade do uso seguro e responsável dos dados pessoais por empresas grandes ou pequenas, digitais ou não e a adequação consiste em um verdadeiro plano multidisciplinar para que toda companhia alcance esses objetivos, de modo a repensar vários aspectos do dia a dia de suas atividades, com o objetivo de cumprir as exigências da lei e proteger melhor seus clientes, funcionários e parceiros comerciais.

Para tanto, importante ter em mente que a LGPD não irá inviabilizar nenhum modelo de negócio, na verdade, irá ajudar muitos destes, pois confere um regime mais flexível e, ao mesmo tempo, mais seguro, no uso de dados pessoais, quando comparado às leis atuais.

É imprescindível que as regras e princípios de privacidade e proteção de dados pessoais sejam incorporados nos valores de toda a companhia, a fim de dar início a uma nova cultura de proteção de dados, por isso, se faz tão relevante a criação de uma visão multidisciplinar, pois a empresa precisa assumir uma perspectiva ampla de alcance, abrangendo todas as áreas que lhe perfazem e não somente operar em um ou mais setores.

Ainda neste sentido, dependendo do porte da corporação, relevante será nomear um comitê multidisciplinar para ser responsável pela elaboração do plano ideal de adequação e poder se ocupar integralmente a este projeto.

QUAIS SÃO AS ETAPAS ESSENCIAIS EM UM PLANO DE ADEQUAÇÃO?

O plano de adequação tem por objetivo garantir a conformidade ou "compliance", em outras palavras, assegurar que todos os dados pessoais sejam tratados com segurança e privacidade, impedindo sua alteração, perda, acesso, transferência ou exposição indevidas.

Não existe uma receita de bolo para fazer o programa de adequação, pois ele deve ser analisado diante das necessidades, desafios e propósitos de cada corporação, contudo seis etapas podem ser consideradas como as principais medidas a serem implementadas em qualquer modelo de negócio, a saber: **Conscientização** - **Mapeamento** - **Gap analysis** - **Planejamento** - **Implementação** - **Monitoramento**

O objetivo da **conscientização** é criar uma cultura de proteção de dados dentro da empresa para que todas as questões que envolvam sua proteção e a privacidade sejam de extrema importância e prioridade para a companhia.

Deste modo, é essencial, em qualquer plano de adequação, que primeiramente a conscientização se origine de seus administradores, pois precisam entender a importância da Lei para se preocupar então com a sua aplicabilidade prática, e, depois, obviamente porque também exigirá o investimento de recursos humanos e financeiros em prol deste programa de adequação para a vida da empresa, sua rotina e seus processos.

Não estamos falando, apenas, de evitar multas que cheguem até 50 milhões de reais por infração, mas de uma oportunidade da empresa rever seu modelo de negócio, de inovar, de criar mais valor para seus clientes e de fato melhorar a experiência deles.

Nesse sentindo, é de grande destaque mencionar a relevância na contratação de um profissional que exerça função consultiva e de interface entre a empresa/controlador, os titulares dos dados e a ANPD (Autoridade Nacional de Proteção de Dados), podendo ser interno ou terceirizado.

A LGPD cria a figura do Encarregado de Proteção de Dados ou também conhecido por DPO (*Data Protection Officer*), que é um profissional com conhecimento em compliance, risco e governança que deverá disseminar a cultura de proteção de dados na empresa e criar normas e procedimentos adequados à lei.

Assim, pode a empresa, nesta fase, já nomear o "Encarregado", atendendo ao que dispõe nos artigos 5º, VIII e 41 da LGPD.

É notório que as tarefas a serem exercidas pelo Encarregado serão as mais variadas e complexas possíveis, razão pela qual, deverá ser estruturada uma área com profissionais que lhes deem respaldo, inclusive, no caso de eventual e indesejado incidente de exposição de dados, porquanto, será por meio desta pessoa que a empresa irá informar, o mais rápido possível, à ANPD, segundo preconiza o artigo 48 da LGPD, correndo o risco de ser sancionada, caso não o faça ou atrase injustificadamente tal comunicação.

A partir do momento que o Comitê estiver formado e o Encarregado de dados nomeado, é hora de focar criticamente na corporação e avaliar os gaps da mesma em relação à privacidade de dados, seguindo

assim, na jornada da implementação da LGPD.

A segunda etapa importante no plano de adequação é **mapear** as atividades da empresa, para identificar quais e que tipo de dados pessoais ou de dados sensíveis ela trata e com qual finalidade, de acordo com o disposto no artigo 7º da LGPD.

É nessa análise que se verifica o fluxo dos dados, se identifica as principais exposições e contingências da corporação, devendo esta se perguntar a fonte daquele dado, a categoria que o dado se engloba, a forma que se trata ou se processa esse dado, pessoas que tem acesso a ele, local de armazenamento, se são compartilhados, o ciclo de vida deles, entre outras.

Nesta fase, necessariamente, deve-se reunir todos os funcionários para que possam elaborar um mapa fidedigno, a fim de analisar o percurso dos dados dentro da corporação.

Isso é fundamental para se compreender quais os responsáveis por cada atividade, quais colaboradores e departamentos devem ser orientados e onde devem ser aplicadas as soluções procedimentais e de segurança, melhor dizendo, deve-se verificar os acessos não autorizados aos dados pessoais tratados, situações acidentais ou ilícitas de alteração, transferência, perda, comunicação ou qualquer forma de tratamento ilegal ou inadequado.

A organização tem a grande oportunidade de mapear todos seus procedimentos, tecnologia, fluxos, falhas e imperfeições.

Também é relevante nesta etapa, averiguar qual a classe legal da companhia que trata os dados pessoais, se controladora ou operadora, em outros termos, se competir à empresa, decisões referentes ao tratamento de dados pessoais (quais dados serão coletados e para qual finalidade), será considerada como controladora, conforme disposto no artigo 5º, inciso VI, da LGPD, contudo, será considerada operadora se apenas realizar o tratamento dos dados, sob orientação do controlador.

A partir dessa distinção serão designadas as medidas de adequação que deverão ser aplicadas, bem como avaliados todos os riscos de responsabilização da empresa.

Outra medida relevante de adequação é a chamada **Gap Analysis**, cujo escopo é identificar os principais pontos de desconformidade com a legislação e indicar os recursos para mitigar os riscos legais.

Significa dizer que ao analisar o mapa, feito na etapa anterior, deverão ser localizados todos os problemas que justifiquem esta desconformidade, visando avaliar a legalidade e apontar ajustes que se façam necessários.

Pensar em soluções que não inviabilizem os modelos de negócio, contudo que possibilitem à empresa sair de uma situação de desconformidade é o propósito da LGPD que não surgiu com o intuito de extinguir corporações, mas lapidá-las para que estejam em legalidade.

Feita a análise do mapeamento, descoberta de todos os problemas e propostas as soluções, passamos à quarta fase do Plano de Adequação que é o **Planejamento**, cujo foco é esboçar a forma de implementação das soluções propostas na fase anterior, criando um plano de ação e um cronograma de execução, priorizando os departamentos que contêm maior risco.

Lembrando que compliance não pode ser feito de qualquer manei-

ra, mas precisa, necessariamente, de uma estratégia, avaliação e desempenho, porquanto segundo preceitua o art. 37 da LGPD, o controlador e o operador deverão manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Um programa de privacidade e proteção de dados pessoais é extremamente complexo e demanda esforços conjuntos de diversas partes interessadas, envolvendo as áreas jurídicas, de tecnologia e segurança da informação, contabilidade, auditoria, recursos humanos, marketing, entre outras, e, por conta dessa alta complexidade, que é indispensável demonstrar a necessidade do comprometimento dos profissionais com poder de direção em relação à adequação da empresa.

Seguindo o processo de adequação à Lei Geral de Proteção de Dados Pessoais, passamos a quinta providência do projeto que é a **Implementação**, onde se colocará em prática o plano desenvolvido na etapa anterior.

Neste momento, a empresa deverá passar por amplas alterações, pois nesta fase, de extrema relevância, deverão ser elaborados todos os tipos de documentos que se fizerem necessários, sendo criadas ou ajustadas as políticas internas de segurança da informação, criando o código de conduta ética em proteção de dados, novos aditamentos contratuais, novos modelos de cláusulas contratuais, nova política de privacidade, restrição de acesso de funcionários a determinados dados, cartilhas de boas práticas, revisão de processos automatizados, dentre outras medidas que deverão ser colocadas em prática.

E, por fim, a sexta etapa de destaque do Plano de Adequação é o **Monitoramento**, que tem o objetivo de manter uma fiscalização e revisão constante do cumprimento das diretrizes estabelecidas no programa de governança em proteção de dados, fazer as atualizações que se fizerem necessárias e garantir que a organização se mantenha em conformidade.

É uma fase que nunca acaba, pois a companhia e o encarregado de dados deverão monitorar, constantemente, todo processo de adequação para estar sempre em conformidade com a LGPD e avaliar se algo precisa ser revisto, devendo prever atualizações periódicas de seus processos, políticas de privacidade e segurança, contratos e readequação das utilizações de dados, bem como sendo fundamental para a criação da cultura de proteção de dados, cursos, seminários e workshops para desenvolvimento permanente dos colaboradores.

Em suma, estar devidamente adequado à LGPD significa dizer que os direitos dos titulares de dados pessoais estão efetivamente assegurados; que o tratamento dos dados pessoais respeita os princípios expostos nos incisos do artigo 6º da referida lei e está respaldado por uma ou mais das hipóteses previstas nos incisos do artigo 7º; que o agente de tratamento está ciente de seu papel e cumpriu com todas as suas obrigações e responsabilidades; que existe um encarregado de dados indicado; e que as medidas de segurança e boas práticas foram adotadas e são constantemente revisadas.

Portanto, as regras e princípios de privacidade e proteção de dados precisam, necessariamente, ser inseridos e previstos nos valores e missões de toda a corporação, buscando criar pilares de confiança, transparência e comprometimento, pois a LGPD não é apenas uma lei, mas um redimensionamento do direito brasileiro, que irá movimentar setores públicos e privado, grandes, médias e pequenas empresas.

RESPONSABILIDADE CIVIL

WALTER ARANHA CAPANEMA

Diretor de Inovação e Ensino da Smart3.

INTRODUÇÃO

A sociedade ainda não despertou para a importância da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei 13.709/2018): norma que coloca o indivíduo como centro das relações jurídicas que envolvam o tratamento[1] de dados pessoais, seja no mundo virtual, seja no mundo físico.

E a forma que a LGPD encontrou para ressaltar a importância do indivíduo frente a um mundo faminto por seus dados, foi, primeiramente, a de lhe atribuir um rol de direitos face aqueles que decidem como estes serão tratados ("controladores")[2] e os que, por sua vez, executam essas atividades de tratamento ("operadores")[3].

Em um segundo nível de proteção, a LGPD conferiu ao indivíduo "dono" dos dados pessoais (a que chama de "titular") uma série de garantias de ordem processual nas ações de responsabilidade civil, como a inversão do ônus da prova e a solidariedade entre controladores e operadores.

E, um dos motivos justamente para que o Brasil acorde para a LGPD são as sanções pecuniárias decorrentes das ações de responsabilidade civil. As quais, poderão, inclusive, ser muito mais pesadas que as temidas penalidades da Autoridade Nacional de Proteção de Dados, a ANPD[4].

Tendo em vista essa importância, pretende-se aqui fazer uma análise panorâmica da responsabilidade civil na LGPD.

RESPONSABILIDADE CIVIL NA LGPD

A LGPD disciplina a responsabilidade civil nos seus artigos 42 a 45. Estabelece que o controlador ou o operador serão responsáveis pelos danos de ordem moral ou material causados aos titulares em duas hipóteses:

a. violação da legislação de proteção de dados (art. 42, caput): abrange os casos em que o dano é causado não apenas pela violação da LGPD, mas de toda a legislação que trate, direta ou indiretamente, da proteção de dados pessoais, como o Marco Civil da Internet (Lei 12.965/2014), o Código de Defesa do Consumidor, a Lei de Acesso à Informação (Lei 12.527/2011), a Lei Complementar 105/2001 (sigilo das instituições financeiras), incluindo, ainda, atos normativos como a Política de Segurança Cibernética (Resolução 4.658/2018 do Bacen), dentre outras.

   Esses danos podem resultar de condutas comissivas (ações) ou omissivas, como, por exemplo, a ausência de consentimento ou de outra base legal para o envio de mensagens publicitárias (spam[5]); o desvio na finalidade do tratamento de dados pessoais ou a revisão automatizada que cause prejuízos ao titular[6].

---

[1] Art. 5º, X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

[2] Art. 5º, VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

[3] Art. 5º, VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

[4] Art. 5º, XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

b. ausência de adoção de medidas de segurança, técnicas e administrativas, aptas à proteger os dados pessoais (art. 44 parágrafo único c/c art. 46, caput): tratam-se das situações em que há normas administrativas ou técnicas de caráter impositivo, que definam requisitos e procedimentos de segurança, relativos aos dados pessoais, contra incidentes de segurança, como ataques de crackers[7] (invasões[8]), vazamentos de dados (leaks[9]) ou ataques de negação de serviço (Distributed Denial of Service – DDoS[10]). Surge, portanto, da omissão diante a uma norma impositiva de uma conduta de segurança.

Poderá ocorrer, por exemplo, quando uma norma da ANPD determine que os dados pessoais sensíveis[11], armazenados em servidores, sejam criptografados segundo determinado padrão. A ausência da adoção dessa medida, e a ocorrência de uma invasão, determinaria a responsabilização do controlador e/ou do operador.

Deve-se entender que a responsabilidade civil, em ambas as hipóteses, é de natureza objetiva, em que se dispensa a discussão da existência de dolo ou culpa no caso concreto. Além disso, diante da evidente superioridade econômica e técnica dos controladores e dos operadores, a LGPD, para tentar reequilibrar essa relação, permite a inversão do ônus da prova pelo juiz (art. 42, §2º), quando "for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa". Com isso, é fundamental que os controladores e operadores tenham preocupação em documentar todas as suas atividades[12], de modo a, na eventualidade de uma ação de reponsabilidade civil, ter a possibilidade de apresentar em juízo suas provas.

A responsabilidade civil será atribuída ao controlador ou ao operador, contudo, admite-se a responsabilização solidária para garantir a efetiva indenização do

---

5 "Spam é o termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamada de UCE (do inglês Unsolicited Commercial E-mail)." NIC.BR. O que é spam? Disponível em: https://www.antispam.br/conceito/. Acesso em: 30 nov. 2020.

6 Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

7 "Quanto aos crackers, eles utilizam seus grandes conhecimentos em informática de forma menos honesta: quebrando (cracking) sistemas de segurança de softwares para ter alguma vantagem financeira lá na frente. Esse tipo de atividade é considerado ilegal e, por isso, os crackers são vistos como criminosos." UOL SEGURANÇA DIGITAL. Hackers e Crackers: quais as diferenças entre eles? Disponível em: https://seguranca.uol.com.br/antivirus/dicas/curiosidades/hackers_crackers_qual_a_diferenca_entre_eles.html#rmcl. Acesso em: 30 nov. 2020.

8 A invasão de computadores e de outros dispositivos informáticos poderá configurar o crime do art. 154-A do Código Penal: "Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa."

9 Os vazamentos são os incidentes mais lesivos, pois os dados são expostos, podem ser reutilizados e reaproveitados. Os titulares perdem, assim, o controle sobre os seus dados pessoais.

10 "O ataque do tipo DoS (Denial Of Service, em inglês), também conhecido como ataque de negação de serviço, é uma tentativa de fazer com que aconteça uma sobrecarga em um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus utilizadores. Para isso, o atacante utiliza técnicas enviando diversos pedidos de pacotes para o alvo com a finalidade de que ele fique tão sobrecarregado que não consiga mais responder a nenhum pedido de pacote. Assim, os utilizadores não conseguem mais acessar dados do computador por ele estar indisponível e não conseguir responder a nenhum pedido". CANALTECH. O que é DoS e DDoS? Disponível em: https://canaltech.com.br/produtos/o-que-e-dos-e--ddos/. Acesso em: 30 nov. 2020. Essa conduta poderá configurar o crime do Art. 266, CP: "Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento. Pena - detenção, de um a três anos, e multa. § 1o Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento."

11 Art. 5º, 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;

titular nas seguintes hipóteses (art. 42, §1º):

1. do operador, quando ofender a legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador[13] e

2. dos controladores que, por suas decisões, tenham causado dando aos titulares.

Os encarregados não estão, a princípio, incluídos na responsabilização civil pela LGPD, afinal, atuam como longa manus do controlador. Todavia, nas hipóteses específicas em que o encarregado for externo ao controlador e, diante de uma relação jurídica de natureza consumerista, poderá, por força das normas protetivas do Código de Defesa do Consumidor, aplicáveis também nas relações de proteção de dados pessoais[14], configurar a responsabilidade solidária do encarregado com o controlador e o operador[15].

Aquele que tiver reparado o dano poderá cobrar em regresso contra os demais responsáveis, "na medida de sua participação no evento danoso" (art. 42, §4º).

CAUSAS EXCLUDENTES DE RESPONSABILIDADE CIVIL

A responsabilização civil dos controladores e operadores será afastada caso estejam configuradas uma das causas excludentes, previstas no art. 43:

a. não realização do tratamento: nesse caso, obviamente, não se pode impor a responsabilidade caso as atividades de tratamento que resultaram em dano forem praticadas por outras pessoas, e não há solidariedade que atinja o ora acionado;

b. ausência de violação da legislação de proteção de dados pessoais: nesse caso, o controlador ou o operador comprovaram o compliance com a legislação de proteção de dados pessoais, razão pela qual, diante da licitude da conduta, não será responsabilizado;

c. que o dano decorreu de culpa exclusiva do titular de dados pessoais ou de terceiro: o dano causado não foi praticado pelo controlador ou pelo operador, tendo decorrido de conduta exclusiva do próprio titular ou de um terceiro estranho à relação jurídica de proteção de dados.

Devem ser consideradas, ainda, algumas causas de exclusão de responsabilidade que, muito embora não estejam expressamente previstas na LGPD, precisam ser levadas em consideração, de modo a prestigiar o desenvolvimento tecnológico e a livre iniciativa das empresas (art. 2º, V e VI). Tratam-se dos eventos imprevisíveis do caso fortuito e da força maior, abordados no art. 393 do Código Civil[16].

Todavia, integram o âmbito de responsabilidade dos controladores e dos operadores o denominado "fortuito interno", o qual "reflete um padrão de comportamento, um standard de atuação, que nada mais representa que a fixação de um quadrante à luz das condições mínimas esperadas do exercício profissional, que deve ser essencialmente dinâmico, e

---

[12] Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

[13] Pode-se entender, assim, que o operador pode se opor as instruções ilícitas do controlador.

[14] Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

[15] Art. 7º, Parágrafo único, CDC. Tendo mais de um autor a ofensa, todos responderão solidariamente pela reparação dos danos previstos nas normas de consumo.

dentro das quais a concretização dos riscos em dano é atribuível àquele que exerce a atividade"[17].

CONCLUSÃO

A responsabilidade civil na LGPD, como foi dito, surge diante da violação da legislação de proteção de dados pessoais ou do desatendimento às normas de segurança.

Exige-se, para reduzir as probabilidades de condenações judiciais, uma preocupação constante com o compliance, com uma atuação do encarregado de constante fiscalização.

Há, também, uma necessidade de educação e sensibilização da segurança da informação e da proteção de dados nas empresas, de modo top-down e incluindo as peculiaridades de cada setor (Recursos Humanos, Jurídico, Tecnologia da Informação etc).

A LGPD, portanto, não deve ser vista como um peso burocrático para as empresas, mas um sistema que lhes permite proteger de forma segura os seus maiores tesouros: os clientes e empregados.

REFERÊNCIAS

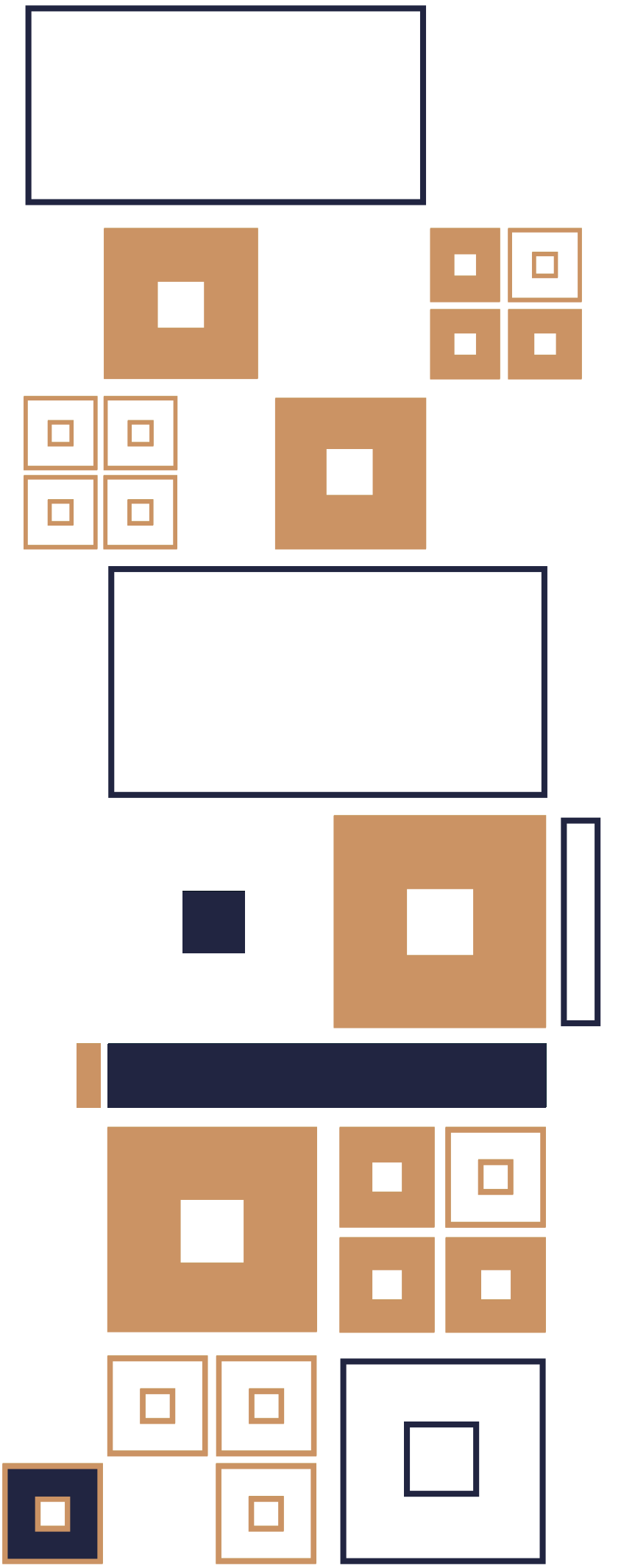
CANALTECH. *O que é DoS e DDoS?* Disponível em: https://canaltech.com.br/produtos/o-que-e-dos-e-ddos/. Acesso em: 30 nov. 2020.

NIC.BR. *O que é spam?* Disponível em: https://www.antispam.br/conceito/. Acesso em: 30 nov. 2020.

UOL SEGURANÇA DIGITAL. *Hackers e Crackers: quais as diferenças entre eles?* Disponível em: https://seguranca.uol.com.br/antivirus/dicas/curiosidades/hackers_crackers_qual_a_diferenca_entre_eles.html#rmcl. Acesso em: 30 nov. 2020.

[16] Art. 393. O devedor não responde pelos prejuízos resultantes de caso fortuito ou força maior, se expressamente não se houver por eles responsabilizado. Parágrafo único. O caso fortuito ou de força maior verifica-se no fato necessário, cujos efeitos não eram possíveis evitar ou impedir.

[17] REsp 1.786.722-SP, Rel. Min. Nancy Andrighi, Terceira Turma, por unanimidade, julgado em 09/06/2020, DJe 12/06/2020.



Prepare sua empresa para a **Lei Geral de Proteção de Dados (LGPD)**

Quer saber como a LGPD pode impactar na rotina do seu negócio? Escaneie nosso QR Code ou acesse o conteúdo exclusivo sobre o assunto em https://sites.rj.sebrae.com.br/minisite/lgpd/

SEBRAE