

REVISTA

espírito livre

LIBERDADE E
INFORMAÇÃO

<http://revista.espiritolivres.org> | #084 | Jan/Fev 2021

LGPD





Atribuição-Compartilhual 3.0 Brasil (CC BY-SA 3.0 BR)

Esta é uma licença simplificada baseada na [Licença Jurídica \(Licença Integral\)](#)

[Advertência](#)

Você tem a liberdade de:

Compartilhar — copiar, distribuir e transmitir a obra.

Remixar — criar obras derivadas.

fazer uso comercial da obra



Sob as seguintes condições:



Atribuição — Você deve creditar a obra da forma especificada pelo autor ou licenciante (mas não de maneira que sugira que estes concedem qualquer aval a você ou ao seu uso da obra).



Compartilhamento pela mesma licença — Se você alterar, transformar ou criar em cima desta obra, você poderá distribuir a obra resultante apenas sob a mesma licença, ou sob uma licença similar à presente.

Ficando claro que:

Renúncia — Qualquer das condições acima pode ser **renunciada** se você obtiver permissão do titular dos direitos autorais.

Domínio Público — Onde a obra ou qualquer de seus elementos estiver em **domínio público** sob o direito aplicável, esta condição não é, de maneira alguma, afetada pela licença.

Outros Direitos — Os seguintes direitos não são, de maneira alguma, afetados pela licença:

- Limitações e exceções aos direitos autorais ou quaisquer **usos livres** aplicáveis;
- Os **direitos morais** do autor;
- Direitos que outras pessoas podem ter sobre a obra ou sobre a utilização da obra, tais como **direitos de imagem** ou privacidade.

Aviso — Para qualquer reutilização ou distribuição, você deve deixar claro a terceiros os termos da licença a que se encontra submetida esta obra. A melhor maneira de fazer isso é com um link para esta página.

Uma mensagem para o leitor



Olá, caro leitor. Como se sabe, no mundo virtual, na Internet, onde somos bits e bytes, nossa vida se transforma em zeros e uns. Não somos dotados de carne e osso, mas de impulsos elétricos que são convertidos finalmente em dados. Estes, por sua vez, compõem o que somos nos ambientes online. Por isso que o cuidado e proteção destes mesmos dados é tão importante. A Lei Geral de Proteção de Dados Pessoais - LGPD surge com a missão de proteger tais dados dados pessoais, em meios físicos e digitais. Ela se fundamenta em diversos valores, tais como o respeito à privacidade; à autodeterminação informativa; à liberdade de expressão, de informação, comunicação e de opinião; à inviolabilidade da intimidade, da honra e da imagem; ao desenvolvimento econômico e tecnológico e a inovação; à livre iniciativa, livre concorrência e defesa do consumidor e aos direitos humanos de liberdade e dignidade das pessoas. O texto conta com 65 artigos, distribuídos em 10 capítulos e foi inspirado fortemente em linhas específicas da regulação europeia, o Regulamento Geral de Proteção de Dados.

No ambiente online, é de se esperar que o compartilhamento de informações ocorra de forma muito mais fácil, daí a necessidade de proteção. Não que no mundo físico não hajam preocupações, mas quando disponibilizamos nossos dados em um formulário na Internet, o caminho que estes dados farão até o seu real destinatário é um mistério para a ampla maioria. Acreditamos que eles estejam inicialmente protegidos, mas mesmo assim, isso deveria ser sempre um motivo de preocupação.

Dito isso, é importante observar que o tema é extremamente relevante a todos, independente se você usa software livre ou software proprietário em seu computador ou dispositivo móvel. O uso e tratamento de nossos dados está agora em voga e tal legislação visa criar um cenário protetivo neste sentido.

O nosso convite para no envio de contribuições e participações está sempre aberto. Participe! Será um prazer tê-lo conosco. 🇧🇷

João Fernando Costa Júnior
Editor-chefe

Diretor Geral

João Fernando Costa Júnior

Editor-chefe

João Fernando Costa Júnior

Revisão

João Fernando Costa Júnior

Arte e Diagramação

João Fernando Costa Júnior

Jornalista Responsável

Larissa Ventrone Costa - ES00867JP

Colaboradores desta edição

Alexandre Resende, Camila Trevisan, Carlos Souza, Eloiza Oliveira, Gisele Truzzi, Gracielle Torres, Jéssica Paula Felipe, Leonardo Barros, Lilian Fonseca, Marina Andrade, Marjori Naele Mocolin Klinczak, Nathália Ferreira, Ricardo Simonato, Rodrigo Branco e William Faria.

Capa

Carlos Eduardo Mattos da Cruz e João Fernando Costa Júnior

Imagens

Freepik, Flickr, Pixabay e PxHere.

Contato

Site: <http://revista.espiritolivres.org>

Email: revista@espiritolivres.org

Telefone: +55 27 981 124 903

ISSN Nº 2236031X

O conteúdo assinado e as imagens que o integram são de inteira responsabilidade de seus respectivos autores, não representando necessariamente a opinião da Revista Espírito Livre e de seus responsáveis. Todos os direitos sobre as imagens são reservados a seus respectivos proprietários.

03 EDITORIAL

por João Fernando Costa Júnior

05 A LGPD ENTROU EM VIGOR: O QUE AS EMPRESAS DEVEM FAZER AGORA?

por Gisele Truzzi

08 O CALCANHAR DE AQUILES DA LGPD

por Gracielle Torres

11 DESAFIOS FRENTE À LGPD

por Marjori Naiele Mocelin Klinczak

14 A LGPD E O VALOR PRECIOSO DOS DADOS

por Alexandre Resende, Rodrigo Branco e Ricardo Simonato

17 COMO CONCILIAR A LGPD E O USO DOS DADOS NAS INVESTIGAÇÕES CORPORATIVAS?

por Lilian Fonseca e Eloiza Oliveira

21 IMPACTOS DO VAZAMENTO DE DADOS PESSOAIS

por Marina Andrade

23 LGPD: O QUE AS EMPRESAS PRECISAM SE ATENTAR PARA O TRATAMENTO DE DADOS

por Camila Trevisan

26 RANSOMWARE E A LGPD: O QUE AS EMPRESAS DEVEM SE PREOCUPAR?

por William Faria

24 LGPD E A ASCENSÃO DO USO DA NUVEM

por Leonardo Barros

30 QUAL O IMPACTO DA LGPD NA ROTINA DAS ESCOLAS E DOS PROFISSIONAIS DE EDUCAÇÃO?

por Nathália Ferreira

32 A LGPD IMPACTARÁ NO MONITORAMENTO E NA INVESTIGAÇÃO EPRESARIAL?

por Jéssica Paula Felipe

34 LGPD E OS DESAFIOS NO SETOR DA SAÚDE

por Carlos Souza



Fonte: Freepik

A LGPD entrou em vigor: o que as empresas devem fazer agora?

por Gisele Truzzi

Finalmente a LGPD (Lei Geral de Proteção de Dados – Lei nº 13.709/2018) entrou em vigor. Mais exatamente dia 18/09/2020. Depois de quase 10 anos de discussões entre Congresso Nacional e sociedade, sendo 2 anos de vacância (prazo determinado para a sociedade como um todo se adequar à lei), e em um ano com tantas idas e vindas, onde muitas pessoas estavam esperando até o último momento para ver se a lei iria vingar mesmo, obviamente que este dia chegou. Agora temos um marco regulatório em relação a privacidade e proteção de dados pessoais em nosso país.

A finalidade da LGPD é a proteção dos dados pessoais, objetivando assim salvaguardar as informações de pessoas físicas. A lei se aplica a toda operação de tratamento de dados pessoais realizada por empresas privadas, órgãos públicos ou até mesmo por pessoas físicas, seja em ambiente online ou offline, independentemente do país onde estes responsáveis pelo tratamento estejam localizados ou do local dos dados que serão alvo deste tratamento.

As disposições gerais da LGPD já estão valendo. Ou seja: agora qualquer cidadão, titular dos dados pessoais, poderá questionar as empresas privadas ou órgãos públicos sobre como é feito o tratamento da sua informação pessoal. Esse questionamento poderá vir através de canais específicos de contato disponibilizados pela instituição, que deverá nomear um Encarregado: indivíduo ou setor responsável pelo atendimento das questões relacionadas a privacidade e proteção de dados pessoais dentro da organização. Será o Encarregado o canal de comunicação entre os agentes de tratamento de dados (controlador e operador), a ANPD (Autoridade Nacional de Proteção de Dados), o titular dos dados pessoais (pessoa física) e eventualmente outras autoridades públicas que fizerem

questionamentos. O Encarregado será o porta-voz da privacidade e da proteção de dados na instituição, devendo zelar pelo cumprimento da LGPD na organização e atendendo às solicitações dos titulares dos dados e autoridades.

A ANPD foi criada, porém ainda não foi estruturada. Isso deverá ocorrer nos próximos meses. Enquanto isso, entende-se que o Ministério Público eventualmente poderá cumprir o papel de fiscal da lei, contudo, sem imposição de multas.

Portanto, nesse momento, há sete sugestões de ações emergenciais para cumprimento da LGPD:

1. Definição do cargo de Encarregado na instituição, juntamente com o seu canal de contato específico, que deverá ser divulgado publicamente no site da organização. Assim, os titulares dos dados pessoais, ao entrarem em contato com a instituição, já saberão para onde direcionarem seus questionamentos relacionados ao tratamento de dados pessoais.

2. Revisão dos Termos de Uso e Política de Privacidade de seus sites, aplicativos e portais, com a menção do Encarregado e contato respectivo nestes documentos, bem como verificação de outros detalhes importantes relacionados à privacidade.

3. Plano de ação: é possível a elaboração de um plano de ação para implantação da LGPD, com descritivo das medidas emergenciais já adotadas, dos procedimentos em andamento e as atividades que ainda serão desenvolvidas, com cronograma específico para atendimento de cada etapa. Desta forma, a instituição já demonstra que está em processo de adequação à lei e consegue informar o prazo em que pretende finalizar a implantação, atendendo assim à eventuais questionamentos dos titulares dos dados, órgãos públicos e da ANPD.

4. Revisão da documentação jurídica: é essencial que a instituição revise seus

contratos, termos e aditivos, analisando-se um tipo de contrato por categoria (como “tipos de contratos”, podemos exemplificar os seguintes: colaborador CLT, colaborador PJ, cliente, fornecedor, prestador de serviços, estagiário, terceirizado, etc.) A revisão detalhada da documentação jurídica básica que vincula as principais relações jurídicas e comerciais da instituição é muito importante, pois, por mais que a empresa não tenha clientes pessoa física, ela possui colaboradores, e estes, como pessoas físicas que são, devem ter a proteção de seus dados pessoais de forma adequada, de acordo com a LGPD.

5. Revisão do consentimento: verificar a forma e as condições impostas no processo de obtenção dos dados pessoais que serão objeto do tratamento, a fim de garantir de que a manifestação do indivíduo é feita de forma expressa, livre, inequívoca e específica para as finalidades necessárias. Caso isto não ocorra, o tratamento dos dados pessoais deverá ocorrer com fundamentação em outra base legal da LGPD.

6. Garantia dos direitos dos titulares: a LGPD define expressamente alguns direitos dos titulares dos dados pessoais (art. 18 da lei), tais como: acesso, retificação, exclusão, portabilidade, anonimização, revogação do consentimento, entre outros. A instituição deve garantir meios válidos para que no processo de tratamento dos dados pessoais, possa atender à tais direitos quando for questionada.

7. Conscientização: é importante também que em algum momento a instituição se preocupe em conscientizar todos os seus colaboradores sobre a LGPD e o impacto de suas atividades no processo de tratamento de dados pessoais, a fim de cada funcionário compreenda a importância de sua atividade ao lidar com informações sensíveis de terceiros. Sem criar cultura interna de proteção de dados não há como atingir conformidade legal, pois as empresas são feitas de pessoas. 🧠

GISELE TRUZZI É ADVOGADA ESPECIALISTA EM DIREITO DIGITAL, FUNDADORA DE "TRUZZI ADVOGADOS".



LGPD em vigência

Saiba o que fazer a partir de agora!

7 sugestões de ações emergenciais para cumprimento da LGPD pelas empresas:



Nomeação do Encarregado

Juntamente com o seu canal de contato específico, este deverá ser divulgado publicamente no site da organização. Assim, os titulares dos dados pessoais, ao entrarem em contato com a instituição, já saberão para onde direcionarem seus questionamentos relacionados ao tratamento de dados pessoais.



Termos de Uso e Política de Privacidade

Revisar esses documentos de seus sites, aplicativos e portais, com a menção do Encarregado e contato respectivo nestes documentos, bem como verificação de outros detalhes importantes relacionados à privacidade.



Plano de Ação

Elaborar um plano de ação para implantação da LGPD, com descritivo das medidas emergenciais já adotadas, dos procedimentos em andamento e as atividades que ainda serão desenvolvidas, com cronograma específico para atendimento de cada etapa. Desta forma, a instituição já demonstra que está em processo de adequação à lei, atendendo assim à eventuais questionamentos dos titulares dos dados, órgãos públicos e da ANPD.



Conscientização

Conscientizar todos os seus colaboradores sobre a LGPD e o impacto de suas atividades no processo de tratamento de dados pessoais, a fim de cada funcionário compreenda a importância de sua atividade ao lidar com informações sensíveis de terceiros, criando-se uma cultura interna de proteção de dados.



Revisão do Consentimento

Verificar a forma e as condições impostas no processo de obtenção dos dados pessoais que serão objeto do tratamento, a fim de garantir de que a manifestação do indivíduo é feita de forma expressa, livre, inequívoca e específica para as finalidades necessárias.



Revisão da Documentação Jurídica

A revisão detalhada da documentação jurídica básica que vincula as principais relações jurídicas e comerciais da instituição é muito importante, pois, por mais que a empresa não tenha clientes pessoa física, ela possui colaboradores, e estes, como pessoas físicas que são, devem ter a proteção de seus dados pessoais de forma adequada, de acordo com a LGPD.



Garantia dos Direitos dos Titulares

A LGPD define expressamente alguns direitos dos titulares dos dados pessoais (art. 18 da lei), tais como: acesso, retificação, exclusão, portabilidade, anonimização, revogação do consentimento, entre outros. A instituição deve garantir meios válidos para que no processo de tratamento dos dados pessoais, possa atender à tais direitos quando for questionada.

contato@truzzi.com.br

www.truzzi.com.br



Fonte: Pesp

O calcanhar de Aquiles da LGPD

por Gracielle Torres

Por ter sido inspirada na GDPR (General Data Protection Regulation), lei de proteção de dados europeia, a LGPD também ficou conhecida como “GDPR brasileira”. A finalidade da LGPD é regulamentar o tratamento de dados pessoais dos cidadãos brasileiros, dentro e fora do Brasil, quer seja em meio digital ou físico. A partir de agora os brasileiros terão mais controle sobre suas informações e sua privacidade pois poderão ou não ceder dados pessoais e exigir que o captador (empresa) defina exatamente a finalidade das informações solicitadas bem como a forma como serão tratadas antes de dar seu consentimento de uso.

A lei entrou em vigor em 18 de setembro de 2020 após quase 2 anos de prazo para adequação das empresas na forma de coleta, manipulação, armazenamento e descarte de informações relativas a dados pessoais. Aqueles que descumprirem a lei poderão ser penalizados pela Agência Nacional de Proteção de Dados (ANPD), órgão regulador, já a partir de 1º de agosto de 2021. A agência poderá efetuar advertências, a proibição total ou parcial de atividades relacionadas ao tratamento de dados e até multas que poderão representar até 2% de seu faturamento total, podendo chegar a R\$ 50 milhões por infração.

A LGPD veio para proteger as informações pessoais e também coibir o tratamento irresponsável de dados, como o caso das empresas, por exemplo, que coletam informações do seu público e as vendem para outras empresas, que por sua vez as utilizam na prospecção de clientes e divulgação de produtos e serviços. Isso gera um alto grau de importunação à pessoa que acaba sendo inundada com publicidade direcionada através de canais eletrônicos além das famosas e irritantes ligações de telemarketing, até mesmo aos finais de semana.

Além disso, a lei vai exigir das empresas uma readequação de seus processos de tratamento de dados, incluindo medidas

para garantir o sigilo e segurança no armazenamento dos dados provendo assim ao consumidor, parceiro ou fornecedor a não exposição de suas informações em caso de invasões cibernéticas. Desta forma, a lei deverá impactar positivamente a vida das pessoas garantindo o direito à privacidade e a prevenção de fraudes através do sigilo de dados financeiros que quase sempre são o alvo dos vazamentos de dados, decorrentes das invasões aos sistemas.

Outro ponto importante é que a lei possui uma ampla abrangência, não se restringindo ao tratamento de dados apenas de empresas de tecnologia, e sim por pessoa natural ou por pessoa jurídica, de direito público ou privado.

O principal ponto positivo será o maior controle que os brasileiros terão sobre suas informações, sua privacidade e maior garantia de prevenção contra fraudes uma vez que seus dados pessoais e financeiros estarão mais seguros. Acredito também que a lei deverá mudar a cultura de segurança da informação dentro das empresas e isso resultará em menos ocorrências de invasões, ataques, vazamentos de dados e consequentemente menos perda de informações e paralisações que sempre resultam em perdas financeiras.

É importante ressaltar que a LGPD também dispõe sobre o tratamento de dados pessoais de crianças e de adolescentes, que a partir de agora deverá ser realizado com o consentimento específico, e em destaque, dado por pelo menos um dos pais ou pelo responsável legal. E ainda: estipula que os controladores (a quem compete às decisões referentes ao tratamento de dados pessoais) não deverão condicionar a participação de crianças em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade. Isso é demasiadamente importante para impor limites a serviços como redes sociais, aplicativos e demais portais que muitas

vezes exigem informações desnecessárias a crianças e adolescentes com a real intenção de obter leads qualificados para direcionamento de publicidade segmentada para esse público. Ao utilizar essas informações para compor peças publicitárias acabam incluindo elementos abusivos, o que é proibido pela resolução 163 do Conselho Nacional dos Direitos da Criança (Conanda).

Como aspecto negativo, vejo que o momento em que a lei entrou em vigor, em meio à pandemia trará dificuldades às empresas para o processo de adequação uma vez que o momento trouxe enormes prejuízos financeiros às empresas especialmente as pertencentes a setores que sofreram paralisações. Somando-se às dificuldades do momento atual a falta da cultura da segurança da informação em nosso país, a qual costumo chamar de “o calcanhar de Aquiles da LGPD”, os prejuízos podem vir não só para as empresas, mas também para os consumidores. E por fim um aspecto muito importante é a falta de percepção de muitos executivos de que segurança da informação é investimento e não despesa e que principalmente agora, com a lei, a prevenção deverá ser adotada como estratégia dos negócios.

Nós, profissionais da área de TI/Segurança da Informação esperamos que as empresas não demorem a tomar a decisão de buscar orientação profissional e multidisciplinar para se adequarem à lei, pois o tempo para isso será diretamente proporcional à maturidade da cultura de segurança da empresa. Se ela for inexistente, demandará muito mais trabalho e investimento do que aquela que já adota o “privacy in design”, ou seja, que já prevê a preocupação com a privacidade desde a concepção de um produto ou serviço. É importante salientar também que tão importante quanto o departamento jurídico é a participação dos profissionais especialistas em TI/Segurança da Informação, imprescindíveis para o sucesso dessa transição e uma perfeita adequação da empresa, afinal de contas são eles profundos conhecedores dos processos da empresa e estão aptos a apontar as vulnerabilidades em software/hardware e até mesmo nos processos. Não haverá espaço para amadorismo ou improvisação que podem pesar no bolso dos empresários em salgadas multas, perda de reputação ou até mesmo impedimento das atividades. 🇧🇷

GRACIELLE TORRES É ESPECIALISTA EM SEGURANÇA DIGITAL CORPORATIVA [[HTTPS://WWW.GRACIELLETORRES.COM.BR](https://www.gracielletorres.com.br)].





Fonte: Freepik

Desafios frente à LGPD

por Marjori Naele Mocelin Klinczak

A Lei Geral de Proteção de Dados (LGPD) entrou em vigor dia 18/09/2020, e em linhas gerais ela versa sobre os direitos dos titulares quanto aos seus dados pessoais (dados que permitem a identificação de uma pessoa) e sensíveis (dados referentes as características da personalidade e escolhas pessoais de cada um), não permitindo mais que as empresas captem dados dos usuários de forma massiva sem o devido consentimento do mesmo, e respeitando a finalidade que a captura se destina.

Com isso, quaisquer empresas que trabalhem com dados de usuários precisam tomar uma série de medidas para evitar que hajam vazamentos de dados, e que caso haja, que tenham um plano de resposta e contenção de danos, e também que toda a coleta de informações esteja dentro de uma das 10 hipóteses prevista no artigo 7º da LGPD.

Dessa maneira, as empresas precisam de uma adequação técnica que envolve não somente toda a empresa, mas exige uma multidisciplinaridade dos profissionais que irão trabalhar com a legislação, principalmente nos tópicos de: segurança da informação, compliance, entendimento do negócio da empresa e direito digital.

Com isso, surgem alguns desafios, principalmente relacionados a área da TI, mas não somente, sendo eles:

- Necessidade de entrevista com os colaboradores e entendimento de onde e como os dados são obtidos (via ligação, via contratos, via redes sociais, via cadastro dos usuários por sites, etc), o que é feito com eles, como são armazenados e como são descartados. Assim é necessário um controle de cada etapa do ciclo de vida, bem como a devida comprovação de que tal etapa foi cumprida de acordo, e mais difícil ainda, comprovar de forma técnica que esse descarte foi realmente feito.

- Obrigatoriedade de escolha de uma base legal para tratamento desses dados, ou seja, deve-se verificar em qual das

hipóteses descritas no artigo 7º da LGPD a coleta se enquadra, e em caso de necessidade, pedir o consentimento dos usuários quanto a esse tratamento.

- Verificação se todos os dados armazenados são essenciais e estão de acordo com a finalidade com a qual foram coletados, por exemplo, se um email foi coletado para o fim de cadastro, ele não pode ser compartilhado com outras empresas ou usado para envio de email marketing sem o consentimento explícito do usuário.

- Em caso de disputas judiciais, cabe a empresa provar que o usuário realmente consentiu com o tratamento de seus dados e quando isso foi feito.

- Criação (caso a empresa ainda não tenha) de planos de mitigação em caso de vazamento de dados, bem como de notificação dos usuários e dos órgãos legais em caso de incidentes.

- Realização de testes de invasão periódicos nos sistemas informáticos.

- Em caso de anonimização dos dados (tornar os dados sem possibilidade de vínculo com seus titulares), poder provar isso de forma técnica.

- Necessidade de criação de um canal de contato com os titulares, onde eles poderão revogar o consentimento de tratamento dos dados ou pedir que lhes seja enviado o que a empresa possui, dentro de prazo razoável.

Temos então que a criação e entrada em vigor da LGPD cria muitos desafios não somente para a tecnologia da informação, mas para toda a empresa, que deve colocar os direitos dos titulares em foco dentro das suas operações diárias, o que exige que toda a empresa esteja em compliance e os funcionários devidamente treinados. 🇧🇷

MARJORI NAELE MOCELIN KLINCZAK É CEO NA MOSAIC WEB, PERITA JUDICIAL EM INFORMÁTICA E MEMBRO DO PARANÁ PERICIAS.

NOVO. RÁPIDO. LIVRE.
LIBRE.



The Document Foundation
apresenta:

LibreOffice



Writer



Calc



Impress



Draw



Base

A suíte de escritório em software livre mais avançada.

pt-br.libreoffice.org



A LGPD e o valor precioso dos dados

por Alexandre Resende, Rodrigo Branco e Ricardo Simonato

A LGPD (Lei Geral de Proteção de Dados Pessoais) tem sido assunto frequente no mundo corporativo e na imprensa. Sancionada em 2018, ela entrou em vigor em setembro de 2020 com o objetivo de regulamentar o tratamento de dados pessoais de clientes e usuários por parte de empresas, sejam elas públicas ou privadas. O objetivo é assegurar que as informações disponibilizadas não sejam usadas de formas que não tenham sido autorizadas. Uma proteção aos consumidores e uma grande responsabilidade para as companhias que hoje enxergam dados como ouro.

Para se ter ideia do valor de uma informação pessoal, é importante saber que grandes empresas já fazem a medição de seu "valuation" (termo em inglês que significa "Valoração de Empresas") pelos ativos de dados que têm.

A Coca-Cola, por exemplo, uma das marcas mais valiosas do globo, tem informações de consumo do mundo inteiro que estão começando a fazer parte de seu valor global. No entanto, esses dados não são da companhia, mas sim do João, da Maria e de tantos outros consumidores do popular refrigerante e de outros famosos produtos.

E por que a atribuição de tamanho valor a algo que pertence a terceiros? Porque dados pessoais são usados para gerar inteligência de negócio, além de poder proporcionar maiores fluxos de caixa futuros às companhias. Marcas que sabem com quem estão falando saem na frente. Entender o público profundamente nunca foi tão precioso.

E uma vez que nós, pessoas físicas, cedemos nossas informações às empresas precisamos ter consciência do que será feito com elas - como serão usadas, armazenadas e quem terá acesso a elas. Termos de concordância se tornaram mandatários e, a partir do momento em que aceitamos compartilhar nossas informações, as empresas são obrigadas a cuidar delas, evitando ao máximo seu vazamento.

Da teoria para a prática

Lanço aqui um questionamento: A LGPD vai fazer com que as empresas não troquem dados entre si? É provável que não. Inclusive, o consumidor já vem sendo avisado sobre essa possibilidade. Recentemente, o WhatsApp enviou aos usuários uma atualização de sua política de privacidade, e informou que passará a compartilhar os dados do seu público com as empresas do Facebook. Imaginam quantas empresas o Facebook tem?

É importante que esses termos passem a ser lidos pelos consumidores com atenção, antes de serem assinados, evitando assim, que se espantem caso temas centrais de suas conversas com colegas no aplicativo de mensagens comecem a surgir em forma de anúncio no seu feed.

Voltando ao início da reflexão e considerando que o valor dos negócios hoje se baseia em dados, seria inocência pensar que eles não serão usados como moeda. Mas o que pode ocorrer em alguns casos é a troca de dados sem a identificação da pessoa. A quem aquele dado pertence não seria o que mais importa. O que vale é contar com os atributos como fonte de aprendizado de máquina. Dessa forma, se creditaria mais ética ao processo.

O Brasil já conta com a ANPD (Agência Nacional de Proteção de Dados) e uma de suas atribuições é punir empresas que estiverem desrespeitando a lei. O órgão, porém, ainda está em maturação e não existe uma equipe 100% definida para dar conta do desafio. Hoje, a fiscalização na prática ocorre em contratos, sob pena de multa, nos quais se exige que fornecedores estejam aderentes à lei. Como não era de se estranhar, o cumprimento das regras se deu antes pelo fôrcaps econômico do que pela consciência em si.

Aqui, o compartilhamento de dados ainda costuma ser mais visto como algo que fere a nossa privacidade de forma negativa. Um exemplo é o caso emblemático de uma conhecida empresa que foi multada porque

estava usando a geolocalização de usuários e trabalhando esses dados sem o consentimento deles. Quando o consumidor toma um grande susto ao, por exemplo, passar em frente a uma loja e imediatamente receber uma mensagem com sugestão de compra naquele local, ele pode se sentir invadido e exigir seus direitos de privacidade.

Sob outra perspectiva

Mas se pararmos para pensar, a personalização - tão importante nas relações comerciais atuais, e valorizada pelos cidadãos - só é possível graças ao uso de dados. Importante lembrar que a utilização correta das informações pessoais pode trazer benefícios para os dois lados - empresa e consumidor.

Imagina se na hora de passar no caixa de uma farmácia, por exemplo, você soubesse como o seu CPF pode ser usado depois daquela compra? Se o atendente deixasse claro que a drogaria usa alguns dados para entender o padrão de consumo e avaliar se pode oferecer condições melhores para produtos diversos, inclusive para seus medicamentos de uso contínuo? Se a farmácia deixasse bem claro que, se puder compartilhar sua informação com o laboratório fabricante do medicamento, para ele analisar a possibilidade de te vender sempre com desconto um remédio que vai usar para o resto da vida, você não iria achar legal?

Claro que tudo isso precisa ser feito com o aceite dos consumidores. Assim, eles saberiam tudo o que estão fazendo, qual a intenção de uso e, também, teriam o total direito de falar no caixa da farmácia, "por favor apaga meu CPF". E o atendente na mesma hora responder: "Sim senhor(a), veja aqui, não tem mais nada registrado".

As preferências sugeridas pela Netflix são outro exemplo claro. Quanto maior a personalização, melhor tende a ser a experiência do usuário. O grande problema é que muitos business, na ânsia de coletar o máximo possível de informações, se esqueceram, ou não se preocuparam tanto em tomar conta delas. Se isso acabou acontecendo nos últimos anos, foi motivo para acender um alerta vermelho perante as autoridades de defesa do consumidor, o que incentivou a criação da LGPD.

Espero que, em um futuro próximo, possamos reconhecer os benefícios que a lei nos trouxe e ainda nos trará, e que a conduta responsável de empresas seja, de fato, colocada em prática. Dados são tesouro, para consumidores e companhias. Que cada um faça a sua parte a fim de usufruí-los com a máxima sabedoria. 🇧🇷

ALEXANDRE RESENDE É CIO DA SERCOM E CEO DA CONTACTONE.

RODRIGO BRANCO É CDO (CHIEF DATA OFFICER) DA SERCOM.

RICARDO SIMONATO É GERENTE DE SEGURANÇA DA INFORMAÇÃO DA SERCOM.



Festival Latino-americano de Instalação de Software Livre

Local: Faculdade Estácio - Porto Alegre

Data: 24/04/2021

Horário: 08:00 às 17:00

Em breve
programação completa





Como conciliar a LGPD e o uso de dados nas investigações corporativas?

por Lilian Fonseca e Eloiza Oliveira

A busca pelo combate à fraude e à corrupção é cada vez mais frequente e intensa nas empresas. Além de uma ameaça direta à perenidade e ao desenvolvimento dos negócios, tais irregularidades têm como consequência a perda de credibilidade diante de um mercado que está ainda mais consciente e exigente sobre a importância de práticas sustentáveis pautadas em valores éticos e em compliance.

Nas situações não passíveis de prevenção, ou seja, quando uma irregularidade já ocorreu, essa busca entra em cena como investigação corporativa, tendo o objetivo de identificar os responsáveis e indicar possíveis vulnerabilidades sistêmicas ou de governança que possibilitaram tal execução. Assim, é possível mitigar os riscos para que a empresa tome medidas cabíveis e se preserve de outros eventos semelhantes.

Para cumprir este objetivo, o tratamento de informações sensíveis é inevitável. Isso porque, durante uma análise, os investigadores possuem acesso amplo aos equipamentos corporativos dos investigados. Por meio deles são extraídas, muitas vezes, evidências robustas que respaldam a tomada de decisão. Porém, no atual contexto de vigência da Lei Geral de Proteção de Dados (LGPD), há um novo desafio: garantir a continuidade do combate à fraude e à corrupção no meio empresarial sem que a Lei seja transgredida pela própria organização ou pelos encarregados de executar as abordagens investigativas.

Nessas ocasiões, o acesso aos dispositivos eletrônicos e caixas de e-mails corporativos de atuais ou antigos colaboradores ou o monitoramento das atividades realizadas no equipamento

profissional do potencial fraudador, desde que descrito na política corporativa de segurança de informações e privacidade, são comumente conduzidos por consultorias independentes, que são contratadas por seus clientes para a apuração e o cruzamento de informações, tendo seu devido contexto, necessidade e objetivo.

Temos aqui um primeiro impasse a ser considerado com a LGPD: o acesso a dados pessoais de uma organização por um agente externo. A imparcialidade da investigação deve garantir que serão explorados apenas os dados sobre os quais há relação direta ao contexto trazido pelo próprio cliente durante a contratação dos serviços. Por exemplo, num trabalho cuja motivação trata-se de denúncia de assédio moral por parte de um funcionário e o monitoramento eventualmente dá acesso ao endereço de sua residência, não é coerente que esta informação faça parte das apurações.

Além da cautela com a imparcialidade e a coerência do objetivo da investigação, há o comprometimento preestabelecido entre a consultoria e o cliente com a confidencialidade dos trabalhos realizados, de modo a restringir o acesso unicamente ao contratante - esse, deve ser um fator sempre presente em qualquer trabalho legítimo de combate à fraude e à corrupção. Portanto, é essencial documentar formalmente a coleta forense de dados para uma investigação com cadeia de custódia e ata notarial atestando os procedimentos adotados, bem como estabelecer com clareza junto ao cliente o devido descarte das informações após o fim das análises,

evitando o vazamento a terceiros.

Também é importante refletir sobre o resguardo do acesso a dados neste contexto. Apesar da LGPD não mencionar investigações corporativas, é possível obter amparo por meio do artigo 7º, inciso IX, sobre em quais situações o tratamento de dados pessoais pode ser realizado: "quando necessário para atender os interesses legítimos do controlador ou de terceiros", desde que seja realizada a avaliação de riscos e sejam aplicados e documentados controles de minimização para eventuais comprovações no caso de questionamentos pela ANPD (Autoridade Nacional de Proteção de Dados). Assim, pode-se dizer que a empresa, no papel de detentor dos dados de seus equipamentos, ferramentas e estruturas tecnológicas, tem o direito de requerer e autorizar o tratamento das informações ali contidas para atender aos seus

interesses, inclusive para combater a ocorrência de eventos fraudulentos.

Nessa perspectiva, as investigações corporativas não serão prejudicadas ou comprometidas pela LGPD, desde que sejam capazes de se adaptar aos cuidados propostos, a partir do aperfeiçoamento de ferramentas e cautela sobre o acesso, tratamento e descarte de informações. Superando tais obstáculos, os trabalhos investigativos em empresas obtêm, inclusive, contribuição à Lei. 🇧🇷

LILIAN FONSECA É CONSULTORA DE INVESTIGAÇÃO.

ELOIZA OLIVEIRA É GERENTE DE INVESTIGAÇÃO, AMBAS ATUAM NA ICTS PROTIVITI, EMPRESA ESPECIALIZADA EM SOLUÇÕES PARA GESTÃO DE RISCOS, COMPLIANCE, AUDITORIA INTERNA, INVESTIGAÇÃO, PROTEÇÃO E PRIVACIDADE DE DADOS.



48% Desconto na Prova CompTia Linux+

Guia Completo de Estudos, com mais de 300 Questões de Simulados Online,
130 vídeo-aulas dos comandos, Linux Fedora Grátis pra treinar na Web e
Grupo de Apoio no Telegram



EASE MEDIA
ASSESSORIA E MARKETING DIGITAL

LIBERTE-SE
WWW.EASEMEDIA.COM.BR

Impactos do vazamento de dados pessoais

por Marina Andrade

O Brasil sofre com uma epidemia de vazamento de dados pessoais e expõe a falta de segurança no ambiente digital. Fóruns usados por cibercriminosos vendem os dados vazados, prática que se tornou muito rentável.

Diante dos últimos mega vazamentos, um envolvendo de 223 milhões de pessoas e outro envolvendo 100 milhões de contas de celular, fica evidente a necessidade de se investir em proteção.

A recente Lei Geral de Proteção de Dados Pessoais (Lei 13.709) traz à pessoa uma série de direitos e determina que as empresas implementem medidas técnicas e administrativas aptas a proteger os dados pessoais contra vazamentos, sob pena de duras sanções e de indenizações aos prejudicados.

Para as vítimas de vazamentos, eventos como esses trazem uma série de prejuízos, como o roubo de identidade (ocasionando a abertura de contas, compras com cartão de crédito, transferências indevidas); clonagem de aplicativos e dispositivos; novos vazamentos de dados, entre outros.

Já para as empresas, os principais impactos são: 1) impacto na reputação, pois

o vazamentos prejudicam a imagem e a credibilidade no mercado; 2) impacto financeiro: multas que podem chegar até 2% do faturamento anual global limitada a R\$ 50.000.000,00 por incidente (a serem aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD) a partir de agosto de 2021); 3) impacto na operação: a ANPD poderá suspender ou proibir a atividade da empresa, bem como poderá bloquear o banco de dados ou determinar a sua exclusão; 4) impacto jurídico: as empresas poderão sofrer ações judiciais movidas pelas vítimas, entidades de classe ou pelo Ministério Público.

Não há um site, plataforma ou um sistema de uma empresa 100% seguro, entretanto, existem medidas preventivas e de mitigação para que, caso eventos assim ocorram, os impactos sejam os mais brandos possíveis e as penalizações menores.

A capacidade das empresas em responder a esses vazamentos e recuperar os danos causados será o grande diferencial competitivo dos próximos anos. 🇧🇷

MARINA ANDRADE É ESPECIALISTA EM PROTEÇÃO DE DADOS E SÓCIA DA LOBO & VAZ.

Liberte o seu melhor

Aproveite esta oferta especial com dois livros para os exames LPIC-101 e LPIC-102 + Curso Online



kindle

kindle



LGPD: O que as empresas precisam se atentar para o tratamento de dados

por Camila Trevisan

Provavelmente você já ouviu falar na LGPD - Lei Geral de Proteção de Dados que entrou em vigor em 18/09/2020, ressalvadas as sanções visto que somente poderão ser aplicadas a partir de agosto/2021, conforme estabelecido pela Lei 14.010/20.

A Lei veio para fomentar o desenvolvimento econômico e tecnológico das empresas, bem como, proteger direitos e liberdades fundamentais dos titulares, jamais para prejudicar qualquer modelo de negócio.

Mas uma visão errada que as empresas estão tendo sobre a LGPD é que agora será necessário coletar o consentimento de todos os titulares de sua base de dados para continuar realizando o tratamento desses dados.

O consentimento é apenas uma das dez bases legais que a legislação trouxe para autorizar as empresas a tratarem dados pessoais. Aliás, em que pese não haver sobreposição entre as bases legais, o que se aconselha é que as empresas utilizem o consentimento em último caso, ou seja, apenas quando determinada finalidade de tratamento de dados não se encaixar nas outras nove bases legais.

Frisa-se que o que determina qual base legal tem que ser usada é o caso concreto e deve ser levado em consideração a origem, a categoria e a finalidade do dado. Além disso, tem-se que para cada finalidade é necessário indicar uma base legal para justificar o tratamento daqueles dados.

Lembrando que, de acordo com a LGPD, compreende-se como tratamento de dados toda e qualquer atividade relacionada ou feita com o dado pessoal, desde o momento em que ele é coletado até o momento em que ele é excluído da base de dados.

Outro ponto importante da Lei pelo qual as empresas devem se atentar, são os direitos dos titulares e como garantir que sejam cumpridos dentro da organização. Dentre eles estão os direitos de acesso, confirmação e retificação dos dados, os quais são mais simples de serem cumpridos, bem como, os

direitos de cancelamento, oposição, portabilidade, compartilhamento de dados e revisão de decisões automatizadas, estes um pouco mais complexos e que vão exigir uma boa gestão de privacidade de dados dentro da empresa.

Ressalta-se que, antes de cumprir qualquer dos direitos acima expostos, é necessário a autenticação do usuário, devendo encontrar uma maneira eficiente de confirmar que quem está exercendo aquele direito é, de fato, o titular.

Por fim, com relação às sanções previstas na Lei, observa-se que uma das maiores preocupações das empresas é a aplicação de multa em caso de infração da mesma, entretanto, existem outras punições que podem ser muito mais prejudiciais à empresa como, por exemplo, a suspensão do exercício da atividade de tratamento de dados, ocasião em que a empresa ficará suspensa de tratar dados por determinado período, uma penalidade muito mais severa, dependendo do modelo de negócio.

Vale destacar que será avaliado, dentre outros fatores, quais foram os danos gerados para o titular e qual a gravidade daqueles danos para a aplicação de uma eventual sanção, o que demonstra a importância de uma cultura de proteção de dados efetiva dentro da empresa, uma vez que a demonstração dos esforços voltados para essa área, tornam a empresa menos propensa a ser penalizada com uma das sanções previstas na Lei.

Posto isso, apesar de ser um tema cheio de detalhes, o caminho para tratamento de dados em consonância com a LGPD é mais simples do que parece, basta que as empresas foquem sempre na transparência em suas relações com seus titulares, deixando tudo bem documentado, caso seja necessária uma prestação de contas à ANPD (Autoridade Nacional de Proteção de Dados). 🇧🇷

CAMILA TREVISAN É ADVOGADA DO ESCRITÓRIO ROCHA LEITE.

Como colaborar com o



LibreOffice ?

Desenvolvimento

Tradução

Revista

Divulgação

Patrocínio

Documentação

Doação

pt-br.libreoffice.org



Foto: Freepix

Ransomware e a LGPD: o que as empresas devem se preocupar?

por William Faria

Nos últimos meses o Brasil sofreu uma onda de ataques cibernéticos, principalmente em órgãos da administração pública, tais como os sites do Governo do Distrito Federal e do Superior Tribunal de Justiça. No dia 3 de novembro, por exemplo, os servidores do STJ foram alvos de um ataque de hackers, ministros e servidores ficaram sem acessos à e-mails e arquivos.

Ainda não se tem a dimensão e as consequências deste ataque, não se sabe, por exemplo, se os hackers conseguiram realizar cópias dos dados ou se houve vazamento de processos que correm em segredo de Justiça. De qualquer forma, esta situação serve de alerta para não apenas as repartições públicas, mas também para as empresas do setor privado, em relação às medidas preventivas de segurança cibernética.

Este ataque torna-se ainda mais grave porque estamos sob legislação LGPD, que entrou em vigor no último mês de setembro. A Lei Geral de Proteção de Dados determina todo um procedimento para atuação dos Controladores de Dados Pessoais em relação a incidentes de vazamento de dados, entre eles a comunicação da Autoridade Nacional de Proteção de Dados (ANPD) e dos titulares de dados que tiveram suas informações afetados durante a investida.

O ransomware é um vírus bastante conhecido no Brasil. Ele bloqueia dados em um computador utilizando criptografia, causando o embaralhamento das informações e, conseqüentemente, a obstrução ao acesso desses conteúdos. Hoje, o Brasil ocupa a segunda posição entre os mais atacados por esse tipo de ameaça, segundo a Trend Micro. Além disso, o país detém a liderança mundial em phishing, golpe utilizado pelo cibercriminoso para enviar o ransomware e sequestrar ou invadir uma máquina, um banco de dados ou um sistema por meio de um e-mail falso. A artimanha do ransomware consiste em após obter os dados, o hacker solicitar o pagamento de um resgate para a liberá-los, normalmente por meio de


criptomoedas, como o Bitcoin, para dificultar o rastreamento pelas autoridades policiais.

A empresa pode se sentir segura por conseguir restabelecer sua operação de forma rápida, com a subida dos backups armazenados em locais seguros e com a integridade garantida, por exemplo, como foi o caso do STJ. Quais são, no entanto, as consequências se o criminoso expuser os dados pessoais em plataformas públicas com o advento da LGPD ?

A partir de agosto de 2021, a empresa poderá sofrer multas e penalidades mediante a denúncia à ANPD. Hoje, porém, ela hoje já pode sofrer com uma enxurrada de ações na esfera cível dos titulares dos dados que foram vazados.

A adequação das companhias para a proteção e privacidade de dados pessoais deve ser pensada para além dos planos jurídicos-processuais de compliance, com investimentos em treinamentos, plataformas de cibersegurança e implementação de SOCs (Security Operations Center) para prevenir vulnerabilidades, monitorar e interromper ataques e vazamentos de dados. E, claro, possuir um bom plano de respostas a incidentes e recuperação de desastres.

Antes da LGPD um ataque de Ransomware "apenas" paralisaria suas operações por um período. Agora, pode trazer prejuízos financeiros, jurídicos e reputacionais terríveis. As organizações, sejam elas públicas ou privadas, precisam aproveitar esse momento de adequação da LGPD e investir porque o mercado de sequestro de dados ficou mais "atrativo".

Para os próximos anos, os investimentos em Cibersegurança devem ser itens prioritário nos orçamentos corporativos. Os cibercriminosos estão com o apetite aguçado, tanto por motivos financeiros quanto por ativismos, e a LGPD está em marcha para proteger os dados dos cidadãos de qualquer violação. 

WILLIAM FARIA é DPO (DATA PROTECTION OFFICER) E ESPECIALISTA EM SEGURANÇA DA INFORMAÇÃO DA GFT BRASIL.



LGPD e a ascensão do uso da nuvem

por Leonardo Barros

Uma das obrigações previstas pela LGPD (Lei Geral de Proteção de Dados Pessoais) é que dados pessoais sejam armazenados apenas em território nacional. Em contrapartida, hoje, os grandes players de armazenamento em nuvem são estrangeiros. Diante deste cenário, é previsto que a exigência da nova Lei faça o Brasil crescer em número de operações de data centers. Neste ponto, muitas empresas estão em dúvida em relação à adoção de uma estrutura própria ou terceirizada.

Analisando o primeiro ponto, manter um data center interno envolve um custo alto, sem contar o investimento com a aquisição de uma infraestrutura composta por alimentação de energia, hardwares, ar condicionados de precisão, nobreaks, geradores, entre outros equipamentos. Já para ter segurança, que é o que evitará ataques cibernéticos, será necessário investir, entre outras coisas, em redundância, ou seja, toda a infraestrutura será em dobro.

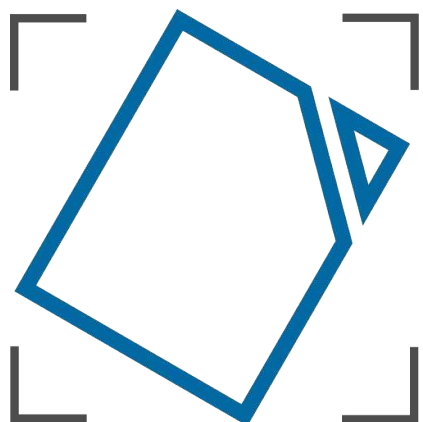
Mesmo com todo este investimento, uma infraestrutura própria não consegue atingir o padrão dos data centers certificados, que oferecem mais camadas de segurança e, por isso, se tornam seguros e disponíveis. Além de ser mais confiável e menos oneroso, terceirizar o trabalho de manutenção da segurança das informações significa manter o foco na atividade principal da empresa.

Ao hospedar os dados em uma cloud terceirizada, as empresas têm mais vantagens em estarem em compliance com a LGPD, bem como com a saúde financeira do negócio. Uma pesquisa da Global Data Protection Index revelou que, em 2018, 72% das companhias brasileiras tiveram problemas com perda ou indisponibilidade de dados.

Isso significa que essas companhias vazaram os dados de clientes, o que no cenário atual, seria uma infração à Lei, já que a LGPD alerta para a responsabilidade de guarda dos dados pessoais. E, no quesito indisponibilidade, a latência dos servidores, que é quanto tempo os dados demoram para ser entregues na nuvem, pode ocasionar a falta de acesso aos sistemas, o que vai gerar uma lentidão na execução de tarefas, prejudicando a saúde financeira da empresa.

Terceirizar a administração do ambiente de TI, a guarda e a manutenção de informações com um fornecedor especializado envolve muito mais do que estar em conformidade com a LGPD. Estamos falando de redução de custos, segurança e disponibilidade no acesso e armazenagem das informações, além da garantia de foco no negócio. 🇧🇷

LEONARDO BARROS É DIRETOR EXECUTIVO DA REPOSIT.



Document
Liberation
Own your content



Qual o impacto da LGPD na rotina das escolas e dos profissionais de educação?

por Nathália Ferreira

A Lei Geral de Proteção de Dados (LGPD) está desafiando todas as instituições brasileiras que tratam dados pessoais e, no âmbito educacional, não seria diferente. A Lei visa regulamentar o ecossistema de coleta e tratamento de dados que identificam os titulares. No caso das escolas, os donos dos dados são estudantes e seus respectivos responsáveis, além de fornecedores e profissionais de educação.

Tratando-se de números, no Censo Educacional 2019 realizado pelo INEP (Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira), foram mais de 47,9 milhões de crianças, jovens e adultos matriculados apenas na educação básica e, quanto aos docentes, mais de 2,2 milhões professores. Portanto, os desafios das instituições de ensino perante a LGPD são grandes, visto que, além do volume de titulares de dados a serem gerenciados, há a particularidade desses, em sua maioria, serem menores de idade, tornando mais complexo o processo de coleta de consentimento, no qual os responsáveis pelo estudante deverão permitir ou não a utilização de seus dados.


Este universo, para além dos desafios próprios do ramo, teve um fator exponencial em 2020 devido à pandemia da COVID-19: a digitalização dos processos, incluindo a conversão do ensino presencial para a modalidade à distância. Logo, novos dados pessoais passaram a ser coletados pelas instituições de ensino, como o IP de conexão, fotos, vídeos, cookies, avaliações socioeconômicas e, principalmente, as informações originadas a partir dos atendimentos virtuais.

Assim, faz-se necessário que as escolas públicas e as privadas estejam de acordo com a LGPD, assegurando o direito dos titulares e a segurança dessas informações, visto que, além dos dados pessoais e dos menores de idade, essas instituições de ensino possuem a transição de dados sensíveis, ou seja, que podem causar algum

tipo de dano ao titular, como as informações de saúde dispostas em atestados médicos e agendas escolares.

Iniciativas como o "Manual de Proteção de Dados para Gestores e Gestoras Públicas Educacionais", produzido pelo Centro de Inovação para a Educação Brasileira e pela UNESCO, trazem à tona diretrizes importantes, principalmente para as Secretarias de Educação. Entre as orientações estão: modelos de políticas de privacidade, termos de uso, cláusulas para inserção nos contratos e afins. Entretanto, faz-se necessário, para além da conformidade jurídica, a formação dos docentes e profissionais de educação, bem como dos estudantes e seus responsáveis sobre os aspectos da LGPD.

Os pais e responsáveis devem ser envolvidos nesta formação, já que o consentimento parental será a base de muitas atividades de tratamento por parte das instituições de ensino, principalmente das escolas particulares que possuem o compartilhamento de dados com parceiros e terceiros. A formação dos professores também se torna importante, visto que este profissional possui discricionariedade em sala de aula, na qual coleta dados pessoais diariamente por meio de trocas de mensagens nas agendas dos alunos e nas avaliações pedagógicas, principalmente dos estudantes com necessidades especiais.

Vale destacar que a Lei Geral de Proteção de Dados é um avanço jurídico e organizacional acerca do tratamento de dados pessoais e sensíveis e assegura como fundamento o desenvolvimento econômico, tecnológico e a inovação, promovendo a livre concorrência e de iniciativa, mas tendo como base os direitos fundamentais, como a liberdade, privacidade e o desenvolvimento da personalidade humana, valores que apenas acrescentarão ao ambiente educacional. 

NATHÁLIA FERREIRA É FORMADA EM POLÍTICAS PÚBLICAS PELA UFABC E CONSULTORA DE DATA PRIVACY DA ICTS PROTIVITI.



A LGPD impactará no monitoramento e na investigação empresarial?

por Jéssica Paula Felipe

A promulgação da Lei Geral de Proteção de Dados, ocorrida em setembro do ano passado, trouxe uma série de dúvidas para as empresas brasileiras. Entre elas, observamos questionamentos sobre quais serão os impactos da LGPD nos controles de monitoramento e de investigação empresarial.

Num primeiro momento, as empresas estarão em busca da adequação à nova Lei, iniciando pelo mapeamento do ciclo de vida de todos os dados pessoais coletados para a realização das suas atividades econômicas. O processo começa pela identificação do titular dos dados, origem e coleta, tratamento e armazenamento, destinos, quem os acessa, qual o período de arquivamento, como é realizado seu descarte e, por fim, qual a finalidade da coleta, para enquadrar as atividades nas bases legais permitida pelo art. 7º e 11º da LGPD.

Após refletir sobre todas essas questões iniciais de adequação, as empresas passarão a se preocupar com a possibilidade de manter as atividades de controle de monitoramento e de investigação empresarial, visto que este processo contém dados pessoais dos colaboradores.


Pelo Código Civil, artigo 932, inciso III, os empregadores têm a responsabilidade pela reparação dos danos causados por seus empregados no exercício do trabalho que lhes competir ou em razão dele. Ou seja, a empresa responde por qualquer ato ilegal cometido pelo seu colaborador, ainda que não haja culpa de sua parte.

Por esta razão, visando a prevenção contra atos ilícitos que possam ser perpetrados pelos funcionários, as empresas fazem uso de controles de monitoramento e investigação empresarial. Com esta medida, é possível detectar fraudes, crimes de corrupção, atitudes não permitidas pela organização, entre outras.

Se pensarmos que os bens disponibilizados pela empresa para os colaboradores executarem suas atividades, como computadores e celulares, são de propriedade da organização, direito devidamente assegurado pela Constituição Federal, isso significa que os dados armazenados nesses equipamentos são de domínio da empresa e devem ser utilizados apenas para a finalidade determinada pelo empregador.

Por isso, é muito importante que seja registrado, no momento da contratação, para que o colaborador tenha ciência que poderá ser monitorado e investigado. Essa informação deve estar expressa nos termos de recebimento dos bens, especificando que o equipamento é de propriedade da empresa e deverá ser utilizado estritamente para atividades profissionais, estando sujeito a práticas de monitoramento em situações necessárias.

Ainda é preciso aguardar as definições pela Agência Nacional de Proteção de Dados (ANPD), que fará a fiscalização e a aplicação das sanções que decorrerem do descumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) quanto às situações específicas e rotineiras da privacidade dos dados.

Isso significa que ainda não sabemos como serão tratados os impactos da LGPD nos controles de monitoramento e investigação corporativa, mas entende-se que tais práticas realizadas com a finalidade de coibir fraudes, crimes de anticorrupção, atitudes não permitidas pela organização, entre outras, não serão prejudicadas, desde que o colaborador, ao ser contratado, tenha ciência. 

JÉSSICA PAULA FELIPE É ADVOGADA, ESPECIALISTA EM COMPLIANCE, DIREITO DIGITAL E CONSULTORA DE DATA PRIVACY NA ICTS PROTIVITI.



LGPD e os desafios no setor da saúde

por Carlos Souza

O setor da saúde é seguramente um dos mais complexos em diferentes aspectos e apresenta desafios constantes, seja pela natureza de suas atividades, que envolve riscos, ou pela vasta legislação e regulamentação aplicáveis. Com a chegada da LGPD (Lei Geral de Proteção de Dados), adicionou-se uma visão que, até então, nenhuma organização estava acostumada a tratar: o fluxo e a natureza sensível de dados pessoais nos processos de negócio.

O dado pessoal se refere à informação relacionada à pessoa natural identificada ou identificável. Já o dado pessoal sensível diz sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, além de estar relacionado à saúde ou à vida sexual, genética e biometria.

Alguns setores utilizam dados pessoais e dados pessoais sensíveis de maneira intensiva, sendo a área da saúde um exemplo legítimo deste cenário. Este setor também contempla uma parcela expressiva dos ambientes que estão sujeitos aos desafios de adequação à LGPD e seus impactos.


Independentemente do nível de maturidade de suas operações, certificações e creditações, empresas deste segmento vivenciam o elevado esforço necessário para entender os requisitos da Lei, bem como o impacto das futuras sanções que serão aplicadas em caso de descumprimento.

Dentre as sanções passíveis de aplicação pela ANPD (Autoridade Nacional de Proteção de Dados), duas possibilidades se destacam a multa simples de até 2% do faturamento da pessoa jurídica e a publicização da infração após devidamente apurada e confirmada a sua ocorrência. A primeira pode gerar impacto financeiro severo e comprometer a continuidade das operações da organização. A outra afeta com intensidade a reputação corporativa e a visão do mercado sobre a integridade das operações.

Entretanto, existem boas notícias. Uma organização adequada à LGPD seguramente terá elevação de maturidade significativa em relação aos seus processos de negócio, controles e ambiente informatizado. Desta maneira, desenha-se mais claramente que a jornada de conformidade se baseia em um projeto multidisciplinar e primariamente fundamentado em Gestão de Processos de Negócio, Tecnologia da Informação e Comunicação (TIC) e Jurídico.

A avaliação de maturidade, resultante do confronto de estado atual contra os requisitos da LGPD, na maioria dos casos, indicará inicialmente baixa conformidade, um resultado que será direcionador para suportar a identificação de lacunas que serão tratadas por meio de um sólido plano de ação estruturado para geração de benefícios no curto, médio e longo prazos.

Em tempos de Covid-19, nos quais a Telemedicina está impulsionada, todo ambiente virtual que suporta e conecta paciente ao médico está intimamente ligado à LGPD e, em particular, merece atenção sob o ponto de vista de segurança de informação. A consciência sobre a coleta e tratamento dos dados minimamente necessários de pacientes e o desenho seguro de seus fluxos nos ambientes pertencentes à área da saúde, certamente ajudará a mitigar riscos de vazamento e geração de incidentes indesejados.

Diante de todos estes aspectos, a LGPD não deve ser temida ou sua implantação vista como algo que beira a impossibilidade. Engajamento, mudança cultural, gestão dos direitos de titulares de dados e seus consentimentos são elementos fundamentais para a estruturação de um programa efetivo e eficaz de governança, que reflete positivamente em toda a organização. 

CARLOS SOUZA É GERENTE DE RISCOS E PERFORMANCE NA ICTS PROTIVITI.

REVISTA *espírito* livre

LIBERDADE E
INFORMAÇÃO

Liberdade e
compartilhamento
de informação e
conhecimento

A Revista Espírito Livre é uma
publicação construída também
através da colaboração dos leitores.

Tecnologia

Software Livre

GNU/Linux

Redes

LibreOffice

Opinião

Entrevistas

E muito mais

Então

Não fique para trás!
Colabore!

Entre em
contato conosco.

revista@espiritolivre.org

Acesse a edição mensal gratuita:
<http://revista.espiritolivre.org>
E confira!

