Quais os cuidados que um e-commerce realmente precisa ter com a Lei Geral de Proteção de Dados Pessoais?

É muito comum questionamentos sobre os impactos da LGPD no e-commerce. Por que as lojas devem se adaptar? A poucos meses da aplicação prática da LGPD, grande parte das centenas de milhares de lojas virtuais do Brasil ainda tratam o assunto com ceticismo ou descrença, como se não fossem um dos segmentos mais impactados com a norma e suas regras para o tratamento de dados pessoais.

A aplicação da GDPR (*General Data Protection Regulation*) na Europa e seus reflexos no mundo (especialmente nos Estados Unidos) também apresentou um cenário de questionamentos intensos por parte de consumidores e associações de representação de titulares de dados pessoais, bem como um crescimento dos processos judiciais envolvendo questões de proteção de dados.

Uma avaliação do Conselho Europeu de Proteção de Dados (EDPB), constatou que nos primeiros 9 meses de aplicação da GDPR houve 206.326 casos relatados de acordo com as autoridades de supervisão dos 31 países membros da Área Econômica Europeia. Além do mais, as multas chegaram a 56 milhões de euros por conta da violação de dados pelos controladores.

Assim, muito conteúdo existe na internet sobre a preparação de negócios, empresas e inclusive negócios digitais, porém, o e-commerce tem especificidades no que tange ao tratamento de dados pessoais que merecem um enfoque e reflexões dedicadas.

É importante destacar que todos os agentes de tratamento devem respeitar os princípios previstos na Lei Geral de Proteção de

Dados, 13.709/2018, sendo eles previstos no artigo 6º. da norma

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V – qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII – segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII – prevenção: adoção de medidas para prevenir a ocorrência

de danos em virtude do tratamento de dados pessoais;

IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Atento aos princípios, é também importante conhecer as premissas ou hipóteses que autorizam o tratamento de dados pessoais. Via de regra, o e-commerce trata dados pessoais com base na sua relação com o consumidor, o que se assemelha à necessidade de execução de contrato ou procedimentos preliminares de contratação, por outro lado, nem sempre esta será a premissa válida, e cada processo de negócio ou ciclo de vida novo com dados do titular precisa de uma avaliação criteriosa. As premissas previstas na Lei Brasileira para tratamento de dados são:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I – mediante o fornecimento de consentimento pelo titular;

II – para o cumprimento de obrigação legal ou regulatória pelo controlador;

III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V – quando necessário para a execução de contrato ou de

procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro;

~~*VIII – para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;*~~

VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência

IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Com efeito, existem pontos essenciais que um negócio, seja ele individual ou uma grande empresa, que trata dados pessoais, não pode ignorar, sobretudo se exerce atividade de loja virtual, considerando sua natureza básica, a execução contratual de compra e venda de produtos, onde necessariamente trata-se dados pessoais. Aqui, passamos de forma objetiva e sem apego a doutrinas, o que uma loja virtual deve primordialmente saber em relação ao e-commerce.

1. **Estabeleça um programa de proteção de dados pessoais**

O primeiro passo ou fase de um sistema de gestão de dados pessoais é a *Preparação*. É aqui que você avalia as leis

aplicáveis ao seu negócio, impactos, realiza um mapeamento de dados pessoais iniciais, identifica os riscos para seu negócio e principalmente conhece, para cada ciclo de vida, se você é um controlador de dados ou operador de dados (se você é loja, marketplace, meio de pagamento, etc.), compreendendo efetivamente as necessidades de ajustes, após analisar os riscos do relatório preliminar e correlacionar suas atividades com os princípios e hipóteses de tratamento trazidas. Nesta fase, você já poderá identificar dados coletados em excesso que devem ser minimizados nas operações ou mesmo riscos existentes nas operações, como por exemplo, o tratamento de dados baseado em uma premissa equivocada.

2. **Organize as ações que serão tomadas**

Nesta fase, atue e organize com um comitê de proteção de dados, avalie a necessidade de sistemas informatizados para te auxiliar na conformidade, programe as ações que serão necessárias para a conformidade com a loja e realize a atualização da política de privacidade (destinada ao público externo). Você pode conceber também uma política de proteção de dados, essa destinada aos seus terceirizados (meios de pagamento, hospedagem, time de *analytics*) e colaboradores. A política reforça a missão corporativa e impõe aos prestadores e funcionários sanções em casos de transgressão às regras.

3. **Implemente as ações**

Conscientização da equipe de backoffice, procedimentos de pseudonimização de dados, criptografia, realização de treinamentos. Aqui serão definidos procedimentos de aprovação para tratamento de dados pessoais, serão implementadas as medidas de segurança de dados, sejam elas técnicas ou organizacionais, bem como ocorrerá a revisão de contratos com todos os demais agentes de tratamento que manipulam dados pessoais no interesse da loja, incluindo a concepção de *data processing agreements*. Sobre as políticas, é importante que se crie uma “central de privacidade” na loja, contendo a política

e suas estratificações ou políticas específicas, como veremos a seguir. Lembre-se, não basta um servidor com sistema operacional atualizado ou um firewall. Existem situações em que somente medidas organizativas poderão reduzir riscos aos dados pessoais.

4. **Políticas e termos de uso. Muito cuidado!**

Você precisa saber que políticas meramente descritivas oferecem uma participação básica do consumidor no processo de tratamento de seus dados. A Lei assegura uma participação maior, portanto, em seu programa de proteção de dados, estabeleça uma central de privacidade, responsável por tratar da política de privacidade e demais estratificações.

Seja transparente, use vídeos, desenhos e fuja dos textos longos e escritos em linguagem de difícil leitura ou juridiquês. Após realizar a política, peça para várias pessoas lerem e verificarem o que entenderam. É importante que a política estabeleça a declaração da empresa em relação a proteção de dados, quais dados são coletados, como são armazenados e tratados, período de retenção, quais os compartilhamentos e para quem os dados seguem para que esta empresa exerça suas atividades. A forma pela qual o titular pode se opor ao tratamento de seus dados deve ser clara.

Do mesmo modo, é importante que o consumidor conheça seus direitos, e as hipóteses em que a loja entende legitimada a tratar os seus dados. A central de privacidade deve dispor, na própria política de privacidade, de link com área para receber pedidos dos titulares, política de pixels, política de cookies, especificação de quais dados sensíveis são tratados (aqueles que podem impactar em direitos e liberdades individuais) além é claro do contato com o DPO (encarregado de proteção de dados) que deverá ser nomeado pelo e-commerce e terá as seguintes atribuições, segundo a LGPD:

Art. 41. O controlador deverá indicar encarregado pelo

tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 2º As atividades do encarregado consistem em:

I – aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II – receber comunicações da autoridade nacional e adotar providências;

III – orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV – executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Lembre-se que ao tratar dados com base na relação consumerista, execução de um contrato, ou hipótese que avaliar cabível para a finalidade específica, esteja sempre ciente de coletar e tratar somente os dados realmente necessários, evitando questionamentos do titular e até responsabilizações. Em casos de outras atividades de tratamento a serem realizadas, que não as necessárias para a compra dos produtos, pode ser necessário o consentimento do mesmo, como por exemplo, a transferência de dados a um processador para marketing direcionado (*behavioral Targeting*) ou para identificar perfis de compra dos titulares (*business*

intelligence). Atenção total aos direitos dos titulares, que poderão ser questionados na área de "*subject requests*" ou "área do titular de dados pessoais":

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I – confirmação da existência de tratamento;

II – acesso aos dados;

III – correção de dados incompletos, inexatos ou desatualizados;

IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V – portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;

V – portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência

VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX – revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

Esteja preparado para receber inúmeros questionamentos de titulares sobre os diversos direitos trazidos acima. Como veremos, nem sempre a loja é obrigada, por exemplo, a "apagar" os dados, mas precisará de uma fundamentação legal para a recusa. Esteja pronto também para responder quem são seus parceiros de negócio (como um gateway de pagamentos ou antifraude) com quem você compartilha dados. Do mesmo modo, prepare-se, pois o titular poderá alegar que os dados são desnecessários, opondo-se ao tratamento.

5. **Cuidados com o consentimento.**

Como visto, é um erro comum em muitos processos de adequação LGPD entender que o consentimento deve ser solicitado sempre. Pode até ser um risco exigir o consentimento em situações em que outras hipóteses legais poderiam se amoldar sem riscos. Porém, quando o consentimento for a hipótese escolhida, lembre-se que não basta informar ao consumidor que "ao comprar na loja ele consente com o tratamento dos seus dados pessoais de tal forma". Este consentimento informado não apresenta mais nenhuma utilidade. O consentimento deve ser *livre, expresso, inequívoco, explícito e em alguns casos até mesmo destacado (para dados sensíveis).* Portanto, não é só inserir parágrafos em uma área do site e acreditar que pode tratar os dados do titular como bem entender. Importante destacar também outra característica do consentimento que é ser *revogável*. Além disso, é de responsabilidade do controlador (loja virtual) a gestão dos consentimentos, registrando todas as manifestações dos titulares de dados de forma que possa ser analisada a qualquer momento. Na hora de finalizar o pedido pode ser considerado um pop-up de consentimento? Cada caso é um caso e deverá ser avaliado o uso e a finalidade da coleta dos dados.

6. **Governança e incidentes de segurança**

Na fase de *Governança* partimos do princípio de que os mecanismos, medidas técnicas e organizativas já foram implementadas. Na operação do e-commerce muitos incidentes podem ocorrer. Nesta fase, é importante executar o plano de solicitações e reclamações dos titulares dos dados e conduzir as avaliações de riscos de privacidade e proteção de dados, incluindo testes de intrusão. No que diz respeito ao plano de solicitações, o DPO (encarregado de proteção de dados) precisa estar preparado para atender às solicitações, no prazo legal, ora concedendo, ora negando, justificando legalmente a negativa do pedido do titular. Nesta fase também se mantém ativa e revisada toda a documentação de privacidade e dados e principalmente, se estabelece um plano de resposta a incidentes de violação de dados pessoais. É muito importante aqui que tudo esteja bem claro sobre o que fazer e como agir diante de um incidente com dados pessoais, envolvendo procedimentos de contenção do dano, perícia em informática, notificação à Autoridade Nacional de Proteção de Dados e comunicações aos titulares. Algumas questões ainda serão regulamentadas. Fique atento, pois as multas por omissões podem ser gravíssimas e considere ainda as ações movidas por titulares de dados violados.

7. **Evolua e prove sua conformidade**

De nada adianta superar todas as fases de um SGPI (Sistema de Gestão da Privacidade da Informação) da sua loja virtual se você não mantiver a avaliação e melhoria ligadas. Lembre-se que embora careça de regulamentação na Lei Brasileira, para cada novo processo, ciclo de vida ou operação de tratamento, pode ser necessário o relatório de impacto a proteção de dados. Esteja, nesta fase, preparado para a realização de auditorias internas e externas, executar avaliações de riscos para proteção de dados, resolver riscos e demonstrar sua conformidade, que a qualquer momento poderá ser requerida pela Autoridade Nacional de Proteção de Dados. Para a conformidade, é possível realizar auditoria na ISO 27701, que estabelece um

sistema de gerenciamento de privacidade da informação. Outra opção é recorrer às certificações e selos, que conquanto não mandatórios ou obrigações legais, são excelentes indicativos, de uma empresa terceira e independente que sua loja cumpriu ou cumpre os requisitos de conformidade

8. **Conclusões**

Se a Lei será prorrogada ou não, honestamente, entendemos não deve ser uma preocupação do empreendedor que tem um e-commerce e que necessariamente realiza tratamento de dados pessoais. A questão é: Eu preciso me adequar e quanto tempo terei para projetar, preparar, organizar, implementar as mudanças e gerir a conformidade da loja as determinações da LGPD? No Brasil, já é possível verificar procedimentos de responsabilização milionários de empresas e lojas que de certo modo foram responsabilizadas por tratamento irregular de dados pessoais. Entender a Lei Geral de Proteção de Dados no E-commerce é essencial. Como visto, iniciar um plano de conformidade, seguindo e observando as etapas acima, pode ajudar lojas virtuais a organizarem ações e a reduzirem custos e tempo na adequação, com foco em questões prioritárias. Não arrisque deixar tudo para a última hora.

Inicie a adequação

Agora que você já sabe como agir, pode acessar o site www.cyberexperts.com.br e conhecer os cursos de *"LGPD no E-commerce, implantação prática"* e os treinamentos "*Construção de áreas de privacidade, políticas de privacidade e proteção de dados".*

No Brasil o ConfiaWeb® é um serviço que avalia lojas em diversos itens de conformidade, incluindo LGPD, apresentando de forma transparente ao titular dos dados e consumidor a pontuação da loja, garantindo segurança, conformidade e nitidamente aumento de conversões. Para conhecer o Confiaweb®, primeira auditoria online e selo de legalidade de lojas

virtuais do Brasil, envie mensagem para (11) 98105-6959.

Envie-nos uma mensagem e solicite uma palestra gratuita para sua loja virtual, sobre aspectos de proteção de dados no e-commerce. Não deixe também de baixar nosso E-book "5 passos para entender a norma ISO 27701" em http://ebookiso27701.pagina.rocks/

Sobre os autores

***Prof. MSc. José Antonio Milagre**, CEO da CyberExperts, advogado especialista em direito digital, e perito em informática, Pós Graduado em Gestão de Tecnologia da Informação, Mestre e Doutorando Ciência da Informação pela UNESP, Pesquisador em Redes Sociais do NEWSDA-BR da Universidade de São Paulo (USP), Presidente da Comissão de Direito Digital da OAB/SP Regional da Vila Prudente, Arbitro fundador da Câmara Internacional de Arbitragem e Mediação em Tecnologia da Informação, E-commerce e Comunicação (CIAMTEC.br). Consultor convidado na CPI de Crimes Cibernéticos – CPICyber do Congresso Nacional. É professor de Pós-Graduação em diversas instituições. Autor pela Editora Saraiva em co-autoria com o Professor Damásio de Jesus, dos livros e "Marco Civil da Internet: Comentários à Lei 12.965/2014" e "Manual de Crimes Informáticos". É colunista da Rádio Justiça do Supremo Tribunal Federal (STF). Data Protection Officer Certified by EXIN. Fundador do Instituto de Defesa do Cidadão na Internet – IDCI. Site: www.josemilagre.com.br*

***Carolina Bonfim Coelho**, especialista em Direito Digital e Dados, membro do escritório José Milagre & Associados. Site: www.josemilagre.com.br*