Confidencialidade, integridade, disponibilidade, autenticidade, não repúdio e temporalidade das mensagens enviadas por meio eletrônico

Atualmente, a LGPD – Lei Geral de Proteção de dados é um dos assuntos mais discutidos na mídia. O Crypto ID montou uma coluna dedicada a proteção de dados onde são publicados artigos relevantes sobre proteção de dados. Falamos sobre a GDPR – General Data Protection Regulation que é a legislação europeia, sobre a LGPD – legislação brasileira e também a legislação de outros países.

Entrevistamos Dra. Patricia Peck, advogada e uma das maiores especialistas brasileiras em Direito Digital para falar sobre a LGPD quanto a aplicação das tecnologias que proveem garantias e evidências como confidencialidade, integridade, disponibilidade, autenticidade e não repúdio.

Crypto ID: Foi noticiado pelo Jornal Folha de São Paulo, dia 15 de março de 2019, que o Governo Federal sugere junto com a nova Reforma da Previdência a cobrança de dívidas através de redes sociais como Facebook e WhatsApp. A ideia do governo é que cobranças de dívidas virtuais se tornem um hábito e possam ser usadas para diversos tipos de dívidas. Atualmente, a cobrança de débitos é feita pela Procuradoria Geral da Fazenda Nacional (PGFN) através de cartas e e-mails.

Doutora, no seu entender o envio de cobrança referente a dívidas da União via redes sociais controladas por empresas comerciais estrangeiras estão em conformidade com a LGPD?

Patricia Peck: O meio utilizado para executar a cobrança e quem a executa deve atender ao que está estabelecido no Código de Defesa do Consumidor, artigo 42, ou seja, que a cobrança não exponha o consumidor ao ridículo, e é este o principal cuidado que sempre deve ser tomado.

Não importa se é uma cobrança presencial, por telefone, por email, por comunicador instantâneo ou mídia social. Os canais diretos são os melhores, inclusive os digitais, visto que evitam gerar desassossego do devedor e também gerar constrangimento público. Para fins da Lei de Proteção de Dados Pessoais é importante que desde o início da relação esteja seja cumprido o princípio da transparência e informado já no cadastro que as informações também serão utilizadas para fins de envio de alertas, mensagens de relacionamento e cobrança digital.

É indiferente se o meio utilizado é controlado por empresa estrangeira no caso da legislação, desde que a lei brasileira seja atendida.

Crypto ID: A responsabilidade em relação às garantias de confidencialidade, integridade, disponibilidade, autenticidade e não repúdio será das redes sociais ou das empresas, sejam elas públicas ou privadas?

Patricia Peck: A legislação de proteção de dados pessoais brasileira se aplica para toda operação de tratamento de dados pessoais de titulares pessoas naturais que seja realizada no território nacional ou que oferte produtos ou serviços destinados ao Brasil.

Sendo assim, se as redes sociais ofertam serviços em território nacional ou para quem esteja no Brasil devem atender os requisitos de garantias de confidencialidade, integridade, disponibilidade e autenticidade exigidos pela legislação.

Assim como as empresas que possuam perfis ou fanpages nestas plataformas e de algum modo capturem e façam tratamento de dados pessoais a partir delas, sejam públicas ou privadas.

A regra se aplica a todos os participantes do ecossistema que envolva o ciclo de vida do dado pessoal, todos que de algum modo tiverem alguma interação em seu fluxo, mesmo que seja mera

armazenagem. Sendo indiferente se é instituição pública ou privada.

Crypto ID: A segurança das informações, regras e limitações para o compartilhamento de dados são os temas centrais da LGPD, correto? Como as empresas podem se proteger quanto à integridade dessas informações quando são utilizadas para comunicação transacional com sua base de clientes?

Fluxo da jornada do cliente nos projetos LGPD

Patricia Peck: Para atingir níveis satisfatórios e adequados as normas, é necessário cumprir uma jornada do compliance em Privacidade e Proteção de Dados e investir em três pilares: soluções tecnológicas, revisão de contratos e procedimentos e capacitação da equipe. Acompanhe neste arquivo o fluxo da jornada do cliente nos projetos LGPD.

Alguns processos precisam ser revistos.

O primeiro de todos envolve o controle de acesso aos dados pessoais. Deve-se iniciar fazendo o inventário dos dados pessoais e então mapeando o seu fluxo dentro da instituição até que haja seu descarte, eliminação ou apagamento ou que haja compartilhamento com terceiro, ou seja, deve ser desenhado todo o fluxo do ciclo de vida do dado pessoal e o percurso que ele realiza desde a entrada até a saída.

A partir deste diagnóstico, devem ser verificadas as soluções técnicas e administrativas que garantam a proteção dos dados pessoais, tanto em nível de controle e gestão como quanto às regras de governança (documentação).

Este tipo de trabalho acaba tendo um maior impacto sobre a TI e a área de SI, mas também sobre o marketing (dados pessoais de clientes) e o departamento de gestão de pessoas (dados pessoais de funcionários).

Alguns procedimentos novos como o que permite o direito ao apagamento dos dados e a portabilidade também deverão ser criados. Além do procedimento para cumprir o dever de reportar uma violação.

Crypto ID: Transformação Digital é outra palavra da moda, e é inegável a necessidade das empresas em utilizar as atuais tecnologias para melhorarem seus processos e reduzirem gastos. No entanto, o que pode ser feito para que as empresas também reduzam os seus riscos jurídicos e lógicos (quanto à integridade e segurança do dado trafegado) quando realizam a transformação digital nos processos de comunicação transacional?

Patricia Peck: A Transformação Digital exige um trabalho de gestão de riscos por contratos (especialmente os relacionados aos terceirizados) e por aplicação de soluções de segurança da informação.

Portanto, é preciso ter um bom departamento jurídico especializado em tecnologia e também orçamento para implementar mais medidas e controles técnicos.

Além disso, é fundamental investir em capacitação, em um trabalho contínuo de atualização das equipes e no aprendizado dentro de um modelo de PDCA.

Crypto ID: Ainda hoje, muitas empresas utilizam a impressão e entrega física de suas correspondências para comunicação com clientes, no entanto, observamos que o mercado se movimenta para a migração para a transformação digital. Eliminar impressão de documentos e entregas físicas de mensagens seria um dos primeiros passos nessa caminhada de tornarem suas empresas mais digitais.

Essas empresas já têm conhecimento de que devem adequar seus processos de comunicação à LGPD e os procedimentos são claros quanto a isso, mas como adequar as mensagens qualificadas como comunicação transacional – quando o envio da mensagem não precisa ser precedido da autorização do cliente? Por exemplo, no caso de cobrança devida ou expiração do serviço.

Patricia Peck: A LGPD traz uma série de exceções para o tratamento dos dados pessoais em seu artigo 7º., entre eles para o cumprimento de obrigação legal, de contrato, atender ao legítimo interesse, incluindo também para fins de proteção do crédito.

Entendo que estas comunicações transacionais estariam dentro destas categorias de exceção de consentimento. Mas, devem ser nomeadas claramente como finalidades que poderão ocorrer para atender ao princípio da transparência do artigo 6º.

Logo, o ideal é atualizar a Política de Privacidade e também o contrato para que a cláusula já mencione as hipóteses de envio de mensagem. Isso não quer dizer que o cliente precise autorizar novamente, pois estaria dentro das exceções de consentimento, mas sim que precisa estar informado a respeito.

Crypto ID: As redes sociais poderão ser utilizadas para envio de comunicação transacional com validade jurídica?

Patricia Peck: Não há hoje nenhum impeditivo jurídico para este uso (poder ser usado), o risco legal ocorre na forma como se usa e para não haver abusos (situações de exposição como já mencionado com a questão de cobrança de devedor).

Crypto ID: Em sua opinião, qual é a relevância das empresas qualificarem suas mensagens e procurarem orientação jurídica e técnica para utilizarem o correio eletrônico em conformidade com a LGPD?

Patricia Peck: Em princípio, quando não há uma regulamentação, as relações são regidas livremente pelos contratos, que fazem a lei entre as partes. Agora, com uma legislação específica, mesmo os contratos devem seguir a orientação trazida pela norma.

Podemos dizer que vivíamos um período em que muitos dados dos usuários eram capturados sem o seu conhecimento, ou sem estar clara a finalidade de uso ou mesmo o prazo de uso, e agora, com as novas regras, o titular dos dados estará mais empoderado, pois tem inclusive novos direitos que devem ser respeitados, como o do apagamento e o da portabilidade, por exemplo.

As empresas que souberem tomar proveito da conformidade à LGPD podem se diferenciar do ponto de vista reputacional junto aos usuários e isso se tornar inclusive uma vantagem competitiva.

Crypto ID: Está previsto na LGPD a obrigatoriedade das empresas gerarem evidências de entrega para certos tipos de comunicação? Inclusive quanto a evento de temporalidade desta comunicação transacional?

Patricia Peck: Com a nova lei fica assegurado aos titulares o direito de acesso facilitado às informações sobre o tratamento dos seus dados, que devem ser apresentados de forma clara, adequada e ostensiva.

Bem como os artigos 46 a 51 tratam justamente sobre a segurança que deve ser aplicada para mitigar os riscos de vazamento.

Cabendo a Instituição o dever, inclusive, de reportar incidentes que envolvam violação dos dados pessoais dos usuários. O ônus de apresentação das evidências é da instituição que realiza o tratamento dos dados pessoais, recaindo primeiramente sobre o controlador dos dados, inclusive quanto a sua temporalidade (por quanto tempo ficou guardado e quando foi descartado).

Crypto ID: A LGPD possui alguma orientação específica quanto ao processo de entregas de comunicação? Alguma trilha de auditoria é requerida pela Legislação? A empresa infratora poderá ser penalizada se não tiver esse controle?

Patricia Peck: A LGPD não traz um processo específico para fins de trilha de auditoria, mas menciona o dever de evidenciação.

O artigo 6º., inciso X diz: 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.

Sendo assim, pode ocorrer a penalização por não ter este controle desde que haja uma violação de dados pessoais em que seja demonstrado que possa estar relacionada a esta omissão ou negligência.

Crypto ID: O que diz a LGPD em relação à integridade dos dados armazenados? As empresas precisam checar a veracidade dos dados informados?

Patricia Peck: A LGPD não exige a checagem da veracidade, até porque, em geral, o preenchimento de cadastros é declaratório. Mas há um direito do usuário no artigo 6º Inciso V relacionado à atualização dos dados pessoais que até pode permitir que a empresa possa cruzar as bases para enriquecer com bases de dados terceiras de modo a manter o cadastro mais completo e atualizado.

Artigo 6º, inciso 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;

Crypto ID: Na sua visão como as empresas devem se preparar para esta regulamentação? Qual seria o start desse processo dentro das corporações?

Patricia Peck: O primeiro passo é fazer um assessment ou seja, realizar um diagnóstico para identificar como a empresa está e o que falta para ficar em conformidade com a nova regulamentação de proteção de dados pessoais.

Isso já deve trazer uma análise de GAP e um mapa de risco com priorização das atividades mais emergenciais.

Com isso deve ser traçado um plano de ação separando em três grupos: ações relacionadas à conformidade técnica; ações relacionadas à conformidade jurídica (documentação, contratos, políticas, procedimentos); ações relacionadas à capacitação e mudança de cultura (educacionais).

E todas elas devem buscar gerar registro de evidências. Além disso, deve ser implementado um ciclo para aprendizado e uma política específica para resposta à incidentes relacionados à violação de dados pessoais e vazamentos.

Patricia Peck Pinheiro, advogada especialista em Direito Digital, doutora pela Universidade de São Paulo, com PhD em Propriedade Intelectual e Direito Internacional, pesquisadora convidada pelo Instituto Max Planck e pela Universidade de Columbia, professora convidada pela Universidade de Coimbra e pela Universidade Central do Chile.
Recebeu os Prêmio Compliance Digital pelo LEC (Legal, Ethics and Compliance) em 2017, Advogada Mais Admirada em Propriedade Intelectual de 2007 a 2018, Security Leaders em 2012 e 2015; A Nata dos Profissionais de Segurança da Informação em 2006 e 2008.
Condecorada com as medalhas militares Pacificador do Exército em 2009, Tamandaré da Marinha em 2011, Ordem do Mérito Militar em 2012 e Ordem do Mérito da Justiça Militar em 2018. Árbitra do Conselho Arbitral do Estado de São Paulo – CAESP, Vice-Presidente Jurídica da ASEGI, Conselheira de Ética da ABED, Presidente do Instituto iStart de Ética Digital. Sócia Head de Direito Digital do PG Advogados e da Peck Sleiman Education. Coordenadora e professora da pós-graduaçãoem Gestão da Inovação e Direito Digital da FIA. Autora de 22 livros de Direito Digital. Certificada EXIN em Data Privacy. (contato: patriciapeck@pgadvogados.com.br).

Fonte: CryptoID, em 20.03.2019.