FIRST TECH®
Construindo relações duradouras

COMO PREPARAR OS NEGÓCIOS PARA AS NOVAS LEIS DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

LEI DE PROTEÇÃO DE DADOS E GDPR

Diferenças, convergências, quem e como é afetado

Os princípios comuns à Lei de Proteção de Dados, à GDPR e a outras legislações semelhantes não se devem apenas ao aproveitamento de referências jurídicas, mas a razões de negócio bem práticas.

Operações como transferência de dados, deslocamento de carga entre data centers, ou prestação de serviços globais tendem a ficar restritas a países com legislações equiparáveis. A lei brasileira tem alguns critérios ligeiramente diferentes de proteção e é mais precisa em itens como definição de "dados anônimos".

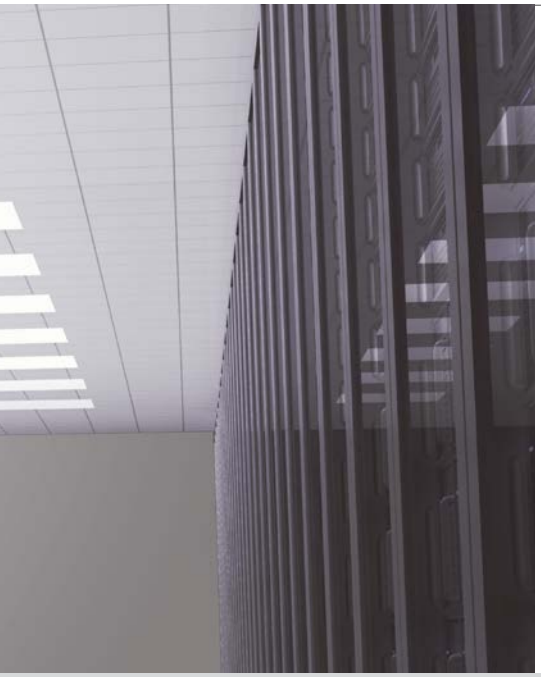
Mas os princípios de finalidade, consentimento, responsabilidades e penalidades prevalecem. Vários mecanismos da Lei de Proteção de Dados complementam ou ratificam regras já existentes, como o Marco Civil da Internet ou regulações globais como o PCI.

Em termos de tecnologia e abordagens de segurança de dados, há muito o que ser aproveitado nas empresas de setores sujeitos a alguma regulação. Mas o marco legal também reforça a atenção de parceiros, clientes e consumidores à forma com que seus dados são tratados. A percepção e intolerância a comunicações invasivas é o efeito mais festejado, que já ocupa os gestores das áreas Comercial, Marketing e Contact Center com a revisão das políticas de trabalho sobre as bases de dados. Mas os desafios afetam a praticamente todos os segmentos.

"Gerenciamento granular do dado" pode parecer uma expressão técnica, mas muito clara em determinados contextos. Em um prontuário médico, por exemplo, o sanitarista deve poder visualizar os eventos reportados, o auditor poderia ver os custos do tratamento, a indústria farmacêutica poderia ter projeções de demanda, mas a identificação pessoal do paciente - nos termos da Lei - só pode ser acessível sob autorização ou em condições muito específicas que a justifiquem.

Na prática, cada organização terá que estabelecer critérios para cada pedaço da informação sobre as pessoas (funcionários, clientes, prospects, etc.) e restringir a exposição e o risco ao que é necessário para a prestação do serviço.

Embora as obrigações legais e as penalidades, nos termos do projeto aprovado no senado, passem a vigorar a partir de 2020, muitas companhias já tiveram que se adequar à GDPR (Regulação Geral de Proteção de Dados), vigente na União Européia desde maio e se preparam para transição à uma economia de dados regulada.



DADOS PESSOAIS, SENSÍVEIS E ANÔNIMOS

O Big Data Ético

Conforme o Projeto de Lei aprovado, são objeto de proteção "os dados processados ou coletados em território nacional, ou que sirvam para a oferta de bens e serviços no mercado brasileiro".

O conceito de "dado sensível" é bem abrangente e inclui metadados como: endereço IP, localização, além de informações claramente pessoais.

Possivelmente devido à contribuição das associações profissionais, o texto traz forte proteção do direito individual, sem engessar a tecnologia nem os modelos de negócios baseados em ciência de dados. Em relação a dados anonimizados, o PL impõe a garantia de que não possam ser revertidos, para identificação do dado original, com "os meios técnicos razoáveis e disponíveis na ocasião de seu tratamento".

Ou seja, a personalização de serviços, as análises estatísticas e outras formas de alavancar os dados não precisam ser descartadas, desde que as informações não sejam pessoalmente identificáveis.

Em resumo, torna-se ilegal o uso ou a transferência de dados pessoais para fins que não forem expressamente autorizados pelo cidadão.

NOVOS PROCEDIMENTOS DE COLETA, TRANSFERÊNCIA E GOVERNANÇA DOS DADOS

O dilema do mailing e dos cadastros

Os princípios de Finalidade e Consentimento norteiam tanto a GDPR quanto a lei brasileira. Em resumo, torna-se ilegal o uso ou a transferência de dados pessoais para fins que não forem expressamente autorizados pelo cidadão.

"O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais", explicita o inciso 4º do artigo 8.

"O consentimento pode ser revogado a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado", diz o inciso seguinte.

Um efeito imediato da aplicação da Lei seria premiar áreas que já se preocupam com uma relação transparente com o cliente, de forma a varrer do mercado os "data brokers" com práticas predatórias, que sorteiam torradeira para ter um mailing de vítimas de abuso informacional.

Na prática, várias empresas têm neste momento que rever as condições de captação de contatos, inclusive os procedimentos de terceiros que tenham feito a coleta.

Uma vez que o destinatário tenha manifestado com clareza sua concordância, o "me esquece" agora não se resume ao opt-out. Além da opção de não receber mais chamadas ou e-mail, deve ser possível também solicitar sua exclusão da base de dados.

DADOS EM NUVEM E TRANSFERÊNCIAS INTERNACIONAIS

Embora tenha passado de 25 a 65 artigos, entre o projeto de 2012 e o substitutivo agora aprovado, a lei não entra em detalhes sobre localização e soberania de dados. O próprio artigo 3º, que tipifica os dados sob proteção, deixa claro que a aplicação é "independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados".

Os artigos que tratam da transferência internacional de dados são relativamente flexíveis, desde que cumpridas as regras de finalidade e consentimento, não há restrições gerais ao armazenamento ou tratamento fora do país. Entretanto, deixam a cargo do "órgão competente" ratificar legislações nacionais, códigos de conduta de corporações globais e outros critérios para regular as transferências internacionais.

Normalmente, há três critérios de definição de soberania de dados: físico (onde o dado está armazenado); por jurisdição (o poder da autoridade nacional sobre o site em que está o dado); e soberania lógica (quem encripta, acessa e gerencia).

É fato que a GDPR e leis semelhantes estimulam os provedores globais a investir em data centers locais, mas as regras baseadas em localização física tendem ao desuso, como ilustra a Resolução 4568 do Banco Central do Brasil (que regula a contratação de nuvens pelas instituições financeiras), aprovada em abril deste ano.

Em resumo, a tendência do auditor ou dos certificadores de compliance é olhar a proteção da informação em si mesma. Independentemente de estar no servidor da empresa, na nuvem ou trafegando pela rede. O que importa é assegurar que o dado só possa ser visualizado, transferido ou alterado conforme as diretrizes gerais.

RESPONSABILIDADE DOS PROVEDORES, DOS PROPRIETÁRIOS DOS DADOS E OS RISCOS DESCONHECIDOS

As leis de proteção de dados não entram em detalhes sobre infraestrutura e arquitetura tecnológica, até porque comprometeria sua longevidade. As questões de segurança e compliance, assim como a distribuição de responsabilidades, são peculiares em cada caso. Mas vale mencionar como ponto de partida um esclarecimento da AWS, que diferencia "segurança da nuvem" e "segurança na nuvem".

Hospedar os servidores que contêm os dados e as aplicações críticas na nuvem pode simplificar. As ofertas de IaaS (infraestrutura como serviço) da Amazon ou da Microsoft incluem opções de segmentação de servidores ou de tráfego que aceleram o compliance a várias regulações setoriais (tecnicamente mais detalhadas que a legislação). Mas tudo isso é meio; o responsável pela segurança é quem responde pelos riscos de cada negócio. Administração de usuários, classificação de informações e a segurança dos dados críticos é um compromisso seu com seu cliente. Os contratos com provedores, ainda que tenham os data centers mais robustos do mundo, não prescindem de consultoria, integração e serviços gerenciados, para alinhar o extenso leque de serviços de TI aos objetivos de cada organização.

No caso de aplicações em SaaS (Software como Serviço), como Salesforce ou Office 365, pode ser interessante rever os contratos e aproveitar alguns serviços opcionais, como DLP (prevenção a vazamentos de dados) e anti-malware. Contudo, essas proteções funcionam dentro do perímetro do provedor. Não há configuração de segurança que resista a um roubo de credenciais ou a um funcionário autorizado comprometido. As organizações, portanto, continuam a ter que gerenciar todo o ciclo dos dados.

Os serviços hospedados e as aplicações homologadas estão longe de ser o maior problema. A facilidade com que departamentos e usuários "implementam" aplicações por conta própria resulta em áreas de sombra (por isso a expressão shadow IT) onde dados críticos fogem do controle. Se houver a possibilidade de alguém anotar uma informação pessoal em um pedaço de papel, ou deixar o arquivo exposto na Internet, não dá para deixá-lo saber nada sobre a vida dos clientes.

Contudo, essas proteções funcionam dentro do perímetro do provedor. Não há configuração de segurança que resista a um roubo de credenciais ou a um funcionário autorizado comprometido. As organizações, portanto, continuam a ter que gerenciar todo o ciclo dos dados.

PREJUÍZOS POTENCIAIS E RISCOS INTERNOS

Multa, reputação e adaptação do cibercrime

Além de responder pelos danos de vazamentos ou uso indevido de dados, entre as penalidades previstas da LPD, está uma multa de até 2% da receita bruta anual da organização.

É obrigatória a notificação de incidentes de vazamento ou violação ao "órgão competente", que determinará ou não a comunicação pública aos titulares dos dados e outras partes interessadas. O artigo seguinte, contudo, admite uma atenuação de eventuais sanções, caso a organização tenha demonstrado intenção com boas práticas e planos de ação auditados, de minimizar os danos.

A experiência ensina que ao resolver os problemas com ratos é preciso não descuidar das pulgas. Ou seja, toda grande solução traz pequenos novos problemas. Foi assim no segmento de pagamentos – à medida que a rápida migração para cartões com chip comprimiu a clonagem física (o skiming ou chupa-cabra), a fraude foi para o e-commerce. De forma análoga, um movimento bem-sucedido de proteção das bases de dados será uma vitória decisiva, mas que já nos obriga a antever os flancos a serem explorados pelo cibercrime.

A abrangência da LPD ao longo das organizações vai estender a questão dos dados a diversos níveis. A clareza em relação aos riscos também não é mais restrita aos tecnólogos. Certamente, descuidos ainda hoje comuns, como exposição de dados críticos aos ataques mais primários, muito em breve vão inviabilizar os negócios.

Uma das contrapartidas previsíveis desse amadurecimento das empresas, infelizmente, deve ser a proliferação de tentativas de aliciamento de funcionários ou usuários com acessos privilegiados. É claro que a maioria de seus colaboradores e parceiros não é eticamente vulnerável, mas a possibilidade de exceções à essa regra, assim como violações involuntárias, é um dos riscos que já devem ser antecipados.

Além de responder pelos danos de vazamentos ou uso indevido de dados, entre as penalidades previstas da LPD, está uma multa de até 2% da receita bruta anual da organização.

PARA QUE TANTO DADO?

Apesar de o Brasil estar relativamente atrasado na definição do marco legal, as questões de ética e privacidade de dados são novas em todo o mundo. A economia dos dados deste início de século, de certa forma, lembra o que ocorreu com a indústria alimentícia na Revolução Industrial até a consolidação das leis sanitárias. Está todo mundo aprendendo.

Segundo o estudo Confiança na Segurança de Dados, feito pela Gemalto com milhares de clientes no mundo, 68% admitem algum gap com a GDPR e 46% não garantem saber onde todos seus dados sensíveis estão armazenados. Outra revelação interessante é que 65% dizem que coletam dados sem saber para que servirão.

Nesse aspecto, de definição de escopo e minimização de risco, a experiência com serviços financeiros e com a indústria de pagamentos tem muito do que se aproveitar.

SOBRE NÓS

Neste artigo procuramos compartilhar algumas discussões, que vão ao encontro dos questionamentos práticos despertados com as novas regulamentações e toda atenção a ética e privacidade.

Ao longo dos últimos anos, esse tem sido um dos eixos do desenvolvimento do portfólio de soluções e da estratégia de serviços da **First Tech.**

Há **23 anos do mercado,** atuamos como provedora de soluções e serviços de tecnologia, sendo especializada no desenvolvimento e implantação de projetos de infraestrutura de contact center, voz, videoconferência, dados, segurança da informação e meios de pagamento.

Somos reconhecidos por customizar, desenvolver e implementar soluções sob medida, além de todo gerenciamento da infraestrutura.

Para tirar suas dúvidas e saber mais sobre o impacto dos novos requisitos de compliance e privacidade em sua organização, marque uma conversa com um de nossos consultores.

COMO PROTEGER?

Tendo em vista as novas vulnerabilidades, os frequentes ataques e as normas de conformidade cada vez mais rigorosas, sua empresa precisa ampliar a proteção de dados para mais ambientes, sistemas, aplicativos, processos e usuários.

A plataforma de segurança de dados Vormetric, oferece recursos para proteger dados em repouso e controlar o acesso a bancos de dados, arquivos e containers, além de proteger ativos localizados em nuvem, ambiente web, big data e ambientes físicos.

Com os recursos abrangentes e unificados dessa plataforma, sua empresa pode responder rapidamente às novas ameaças e se preparar para novas conformidades de segurança.

VEJA ABAIXO QUAIS OS REQUERIMENTOS SÃO POSSÍVEIS DE ATENDER COM ESSAS SOLUÇÕES:

Requerimento	PCI DSS	Tecnologia Thales
Proteger dados do titular do cartão	3.4, 3.5, 3.6	Transparent Encryption; Application Encryption; Tokenization; Cloud Data Security; HSM-based Key Protection
Criptografar a transmissão de dados	4.1	HSM-based Key Protection
Restringir acesso aos dados do titular do cartão	7.2	Policy-based Access Controls; User and Device Authentication; Encryption Key Management
Identificar e autenticar o acesso aos sistemas	8.1, 8.3, 8.7	User and Device Authentication; Policy-based Access Controls; HSM-based Key Protection
Rastrear acesso aos dados do titular do cartão	10.1, 10.2, 10.3	Security Intelligence; Policy-based Access Controls

Padrão de Segurança	GDPR	HIPAA | HITECH	Tecnologia Thales
Criptografia de dados	Artigo 6, 25, 32	164.312(a)(2)(iv) 164.312(e)(2)(ii)	Transparent Encryption; Application Encryption; Cloud Encryption Gateway; Cloud Data Security
Comunicação de violação	Artigo 33, 34	164.400-414	Transparent Encryption; Application Encryption; Cloud Encryption Gateway; Cloud Data Security
Controles de acesso a dados	Artigo 5	164.312(a)(1)	Policy-based Access Controls; User and Device Authentication
Evidências de acesso a dados	Artigo 5	164.312(b) 164.312(c)(1)	Security Intelligence

FIRST TECH®

Construindo relações duradouras

www.first-tech.com

MATRIZ
Rua Cerro Corá, 1.038 | Alto da Lapa
São Paulo - SP | **Tel.: (11) 3024-3200**

FILIAL
Rua da Assembleia, 10 - conj. 1819 | Centro
Rio de Janeiro - RJ | **Tel.: (21) 3543-1650**