inloco university

Privacy Week Insights

Um panorama de uma semana inteira de discussões sobre uso de dados, privacidade e LGPD com os mais importantes profissionais do setor.

Indíce

Introdução

Estamos há menos de um ano da implantação da Lei Geral de Proteção de Dados (LGPD) e o assunto ainda é pouco discutido entre empresas, consumidores e indústria. Recentemente, foi aprovada a criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão federal que vai editar normas e fiscalizar procedimentos sobre proteção de dados pessoais, ou seja, estamos há alguns passos da implantação e fiscalização da lei.

Seu negócio está preparado para lidar com milhares de informações de seus parceiros, colaboradores, clientes, entre outros?

Não podemos deixar nossa privacidade em segundo plano. Conveniência precisa coexistir sem prejudicar o direito individual de cada um a anonimidade. Nós da In Loco nascemos com a missão de resolver esse problema das pessoas. Queremos tornar toda interação entre máquinas e humanos mais privada e conveniente.

Por isso, realizamos uma semana inteira de discussão tratando do tema: privacidade, com os mais importantes especialistas. Esperamos que desfrute da leitura. Precisamos disseminar, conscientizar e trazer esse assunto para a pauta de todas as pessoas e empresas.

Expediente

Jornalista responsável
Lana Pinheiro

Redação
Eliane Pereira e Raul Assumpção

Revisão
Raul Assumpção

Designer
Victor Gomes

Fotos
Tato Rocha e Maurício Marconi

Colaboração
Time In Loco

Dia 1
Privacidade: o presente e o futuro

A privacidade como direito fundamental do ser humano está, cada vez mais, em risco com o avanço da tecnologia. Pagamos um preço muito alto pela conveniência que a internet proporciona: nossa liberdade. Terabytes de dados são gerados a partir de nossas interações na internet. Porém, também é a partir da coleta de dados que recebemos e consumimos conteúdos e produtos mais relevantes para o nosso dia a dia, gerando mais conveniência, fluidez, agilidade e segurança. Isso tudo nos faz questionar como está o presente com menos de um ano para a implantação da LGPD e como será o futuro das empresas e dos consumidores com relação à privacidade. Estamos dispostos a entregar todas as informações da nossa vida a máquinas e estranhos? Temos o direito de permanecer preservados?

Big data: está na hora de praticar o desapego

André Ferraz
CEO da In Loco

Daqui a um ano, em agosto de 2020, entra em vigor a Lei Geral de Proteção de Dados (LGPD), criada para garantir transparência no uso de informações de pessoas físicas e proteger sua privacidade. Não era sem tempo: passou da hora de empresas e usuários adotarem medidas de segurança e confidencialidade de dados. Para debater essa questão, a InLoco criou a Privacy Week, uma semana inteira de debates com profissionais de diversas áreas.

Já é difícil comprovar se o que encontramos na internet é verdadeiro ou não – vide a quantidade crescente de notícias falsas, sites maliciosos e golpes de todo tipo. Para complicar, somos monitorados o tempo inteiro, quer a gente concorde ou não. Por exemplo, sistemas operacionais como Android e iOS continuam a rastrear o aparelho mesmo com a geolocalização desligada (até no modo avião).

Mais que isso, essa invasão tem impacto na democracia, na medida em que o uso de ferramentas tecnológicas pode afetar os resultados de um processo eleitoral, como nos casos do Brexit e da eleição de Donald Trump, para citar dois dos mais conhecidos.

Linkedin →

Vídeo da Palestra →

Com internet das coisas (IoT) teremos uma avalanche de dados e ainda menos controle sobre os dispositivos que os capturam, além de uma infinidade de pontos por onde hackers poderão se infiltrar.

A questão não é nem “se” os dados compilados por determinada empresa vão vazar, mas quando. O volume de vazamentos vem crescendo ano a ano, e a tendência é de aumento, pois há mais empresas e dispositivos coletando informações e mais ferramentas para invasão de sistemas.

A verdade é que é mais fácil quebrar a segurança de um sistema do que construi-lo. Portanto, se a invasão é uma possibilidade real e provável, o melhor é não manter dados sensíveis armazenados. Resumindo: se não precisa do dado, não colete. Se a informação não é essencial, jogue fora. Simples assim.

Mas então como garantir a qualidade do serviço, a personalização e a lucratividade? Temos aí dois problemas: comprovação de autenticidade e controle de dados pessoais. Com soluções mutuamente excludentes, pelo menos à primeira vista: coletar mais informações para comprovar autenticidade (diminuindo o grau de privacidade) ou restringir o acesso a dados pessoais, reduzindo a qualidade do serviço prestado.

Entretanto, conveniência e privacidade podem coexistir em harmonia dentro do mesmo modelo de negócios. Para isso, os dispositivos de coleta teriam que ser “cegos” em relação ao usuário, mapeando apenas seu comportamento e coletando só a informação necessária para atender o cliente. A farmácia não precisa saber o CPF do consumidor e para o app de game não interessa a localização de quem está jogando.

Para o cofundador e CEO da In Loco, André Ferraz, o sistema de autenticação comportamental anonimizada desenvolvido pela empresa a prova de que dá para trabalhar sem identificar a pessoa, até mesmo em projetos de CRM, análise de dados e publicidade. Ou seja, é possível entregar conveniência sem invadir a privacidade de ninguém.

O desafio é mudar a mentalidade no ambiente corporativo, promovendo ações no dia a dia para conscientizar o time sobre a importância e as vantagens da confidencialidade de dados. Mais que a tecnologia, é a cultura que vai fazer isso pegar nas empresas.

Para André Ferraz, estamos pagando um preço alto para ter conveniência. Podemos reconstruir a internet colocando a privacidade no centro e nos devolvendo a liberdade e o controle sobre a rede (em vez de sermos controlados por ela).

A invasão de privacidade é o mais silencioso ato de violência. Sem privacidade, nossas liberdades individuais e coletivas correm risco. A missão agora é fazer com que o 1984 de George Orwell não se torne realidade.

Três desafios para colocar nos trilhos a LGPD

Bruno Bioni
Fundador do Data Privacy Brasil

Linkedin →

Vídeo da Palestra →

Quando o Brasil instituiu o Código de Defesa do Consumidor, em 1990, dizia-se que ele inviabilizaria os negócios. Quase 30 anos depois, o país tem uma cultura de proteção ao consumidor e as pessoas se sentem mais confiantes em fazer compras online, os carros são mais seguros, há mais cuidado na área alimentícia, para citar alguns exemplos.

Fundador do Data Privacy Brasil (que oferece cursos nas áreas de privacidade e proteção de dados), Bruno Bioni aponta três desafios a serem vencidos para que a Lei Geral de Proteção de Dados, que entra em vigor em agosto de 2020, se torne um instrumento tão respeitado quanto o Código de Defesa do Consumidor.

Primeiro desafio: obrigação ou oportunidade?

Um dos objetivos da lei é incentivar o desenvolvimento tecnológico e econômico, protegendo liberdades fundamentais. Ela vem para fixar regras gerais, definir conceitos e estabelecer direitos e deveres em uma sociedade movida por dados, trazendo mais civilidade para o ambiente digital.

No processo de adequação à lei toda empresa terá que mapear o ciclo de vida do dado – como ele chegou, qual a sua

finalidade, quem tem acesso, como será descartado. Quem internalizou essas práticas conseguiu extrair insights para seus negócios e modelos de serviço.

No Brasil, as organizações se dividirão em dois grupos: o das que vão encarar a lei como mais uma formalidade jurídica e o das que verão uma janela de oportunidade. As primeiras vão olhar a lei apenas como critério para manter e rever seus produtos. As outras criarão uma trilha de dados auditável e, com isso, desenvolverão novos produtos ou políticas públicas (lembrando que a lei vale também para o setor público).

Segundo desafio: o fator humano

Este será, possivelmente, o maior de todos. Se não conseguirmos engajar os que estão no "chão da fábrica", a coisa não vai dar certo. O conceito de privacy by design (privacidade por concepção) tem que ser incorporado a produtos, serviços ou políticas públicas desde o início, com uma abordagem centrada no usuário/ consumidor. Isso significa adotar medidas de prevenção, pensar na privacidade durante toda a concepção do projeto e proteger os dados ao longo de todo o seu ciclo de vida.

Limitações estruturais atrapalham a internalização dessa mentalidade – da falta de interação entre as equipes até a rotatividade dos funcionários encarregados de tocar o projeto. Além disso, existe a questão do clima organizacional.

Privacidade e proteção de dados têm que ser um elemento vivo dentro das organizações. Não basta o discurso, é preciso colocar em prática os princípios que a empresa se propôs a seguir.

Como encarar a Lei Geral de Proteção de Dados

Uma obrigação legal	Uma janela de oportunidade
Manutenção e revisão dos produtos existentes	Criação de novos produtos e revisão de modelo de negócio ou política pública
Análise estanque centrada no diagnóstico de riscos	Análise dinâmica centrada no que a organização pode gerar de valor
Gestão baseada em mitigação de risco	Gestão baseada em inovação
Reputação com base no medo de sanções	Reputação com base em dar mais transparência ao uso dos dados

Terceiro desafio: regulação e autorregulação

A lei é apenas um dos vetores para formatar uma cultura de proteção de dados. Além dela, é necessário uma autoridade fiscalizadora forte e atores econômicos com mentalidade aberta. Ou seja, tem que sair da bolha e falar com outros setores, como academia, governo e terceiro setor, de modo a construir uma cultura geral de data privacy.

Quando a lei entrar em vigor para valer, teremos segmentos que sairão na frente na formulação de códigos de boa conduta e que servirão de exemplo para o mercado. Como cada setor tem suas particularidades, a ideia é que os pares se juntem para estabelecer boas práticas a serem observadas por todos.

Por fim, a cultura de proteção de dados deve ser algo consolidado não só para os profissionais de compliance, mas também para a academia, ONGS, governos e instituições públicas e privadas. Sem isso, não conseguiremos colocar a LGPD em movimento.

Uruguai sai na frente ao promover educação sobre privacidade e proteção de dados nas escolas

Segundo a Comissão Europeia, Argentina e Uruguai são os dois únicos países da América Latina com níveis adequados de proteção de dados pessoais. A legislação argentina está em vigor desde 1994 e a uruguaia remonta a 2005, quando foi criada a Agesic (Agência de Governo Eletrônico e Sociedade da Informação e do Conhecimento, ligada à Presidência da República).

O Uruguai é um país pequeno – são 3,5 milhões de habitantes e PIB per capita de US$ 23.571 –, mas com bons indicadores: 99% das escolas e hospitais estão conectados, 85% da população usa a internet diariamente (sendo que 77% têm acesso à rede nos lugares mais pobres) e 67% utiliza os serviços de governo digital (mais de 500 disponíveis).

O país baseia sua política nessa área em três pilares: segurança, proteção de dados e transparência da informação pública. Um dos pontos mais importantes, no entanto, é a questão educacional. Assim como foi feito com a defesa do meio ambiente, a ideia é ensinar as crianças que cuidar de seus dados é importante.

Laura Nahabetián Brunet
Gerente da Divisão de Direitos dos Cidadãos da AGESIC e Assessora Jurídica do Parlamento Uruguaio

Linkedin →

Vídeo da Palestra →

Para a gerente da divisão de Direitos dos Cidadãos da Agesic, Laura Nahabetian Brunet, em uma ou duas gerações o país contará com uma população educada em proteção de dados. Trata-se de uma política pública que está dando resultado e que o governo pretende que seja incluída como matéria obrigatória no currículo escolar.

Entre os principais fundamentos da legislação do Uruguai sobre o tema (Lei 18.331) estão:

- o reconhecimento da proteção de dados como direito fundamental;
- o consentimento como eixo central do sistema;
- o respeito aos direitos ARCO (de acesso, retificação, cancelamento e oposição), incluindo o direito ao esquecimento; as obrigações associadas, como registro da base de dados e uso apenas com consentimento do titular.

A legislação prevê ainda a figura do delegado de proteção de dados em empresas públicas, ou que tratem dados sensíveis, ou ainda nas que lidem com grandes quantidades de informação. Essas organizações têm o dever de comunicar à autoridade reguladora os casos de transferência de dados para países cuja legislação não seja similar à uruguaia ou europeia (GDPR).

Uma peculiaridade do modelo local é que a Unidade Reguladora e de Controle de Dados Pessoais tem autonomia técnica e poderes de fiscalização e sanção, mas está formalmente ligada à agência de governo eletrônico. A unidade não tem equipe própria, todos são funcionários da Agesic. Mas seus diretores decidem de forma autônoma as questões de sua competência.

Em caso se descumprimento da lei, a multa pode chegar a US$ 80 mil. Mas o enfoque é trabalhar a educação, para que os cidadãos saibam seus direitos e deveres e as empresas conheçam e cumpram as regras.

Laura Brunet destaca a necessidade de conscientizar a sociedade de que privacidade é uma questão ligada ao exercício de outros direitos fundamentais, como a liberdade de expressão e de opinião. E que descuidar dela é colocar em risco a própria democracia.

Dia 2
O impacto da nova lei nos negócios: Uma abordagem prática

O acesso a internet, a popularização do mobile e o desenvolvimento da Inteligência Artificial permitiu que terabytes de dados sobre os mais diversos tipos sejam gerados por hora, dando um poder antes inimaginável a quem obtiver acesso e souber usá-los, impactando diretamente a economia mundial. Por conta disso, desde 2012 a União Europeia discute sobre a proteção de dados pessoais. No Brasil desde de 2010 há essa discussão e agora em 2018 se transformou de fato em uma lei, muito parecida com a GDRP dos europeus. A pergunta é como isso impactará novos e velhos negócios na prática de coleta, armazenamento e tratamento de dados? Desde um RG, CPF, e-mail, nome e até na localização?

O impacto da LGPD nos negócios: é hora de juntar forças para tirar a lei do papel

Os impactos da Lei Geral de Proteção de Dados (LGPD, que entra em vigor em agosto de 2020) ainda estão sendo mapeados. Mas o principal é que ela promove uma mudança de paradigma, ao colocar o titular dos dados em primeiro lugar, no centro de decisão dos negócios. Antes da LGPD, as empresas achavam que eram donas dos dados, sem se preocupar muito com questões relativas à coleta e armazenamento. Isso vai mudar.

Quem mostrar que trata dados com responsabilidade terá vantagens, principalmente no que diz respeito ao aumento da confiança do consumidor. Por outro lado, as organizações vão pensar duas vezes antes de coletar dados pessoais, aposta a head de legal da In Loco, Raíssa Moura. Até porque, um vazamento ou o mau uso das informações pode manchar a reputação da empresa.

O exemplo mais conhecido é o do uso de informações de milhões de usuários do Facebook pela consultoria Cambridge Analytica, para influenciar a opinião do eleitorado norte-

Raíssa Moura
Diretora Jurídica
da In Loco

Linkedin →

Vídeo da Palestra →

americano no pleito que culminou com a eleição de Donald Trump, em 2016. Além da queda do preço das ações (a companhia chegou a perder mais de US$ 120 bilhões em valor de mercado), a utilização da rede social caiu 20% desde abril de 2018, quando foi detonado o escândalo, segundo levantamento da Mixpanel.

Vazamentos podem ser devastadores para a reputação da empresa. Mais do que levar uma multa milionária, ela perde negócios e credibilidade. Por outro lado, a implementação de uma política efetiva de proteção de dados pode fortalecer qualquer marca. A pior opção é fazer isso só para cumprir tabela, sem adotar de fato uma cultura de respeito à privacidade.

Na In Loco, o primeiro passo foi educar as pessoas. Muitos acham que isso deve ficar para o final, mas como os funcionários vão incorporar o espírito da legislação se não forem treinados para tratar os dados de maneira correta?

As empresas que seguirem esse raciocínio vão acabar pagando muito dinheiro para consultorias sem conseguir que o projeto se sustente, por não entenderem que se trata de um processo constante e que é importante estar em conformidade com a legislação.

A adequação à lei vai reduzir custos, mesmo que, a princípio, seja necessário contratar consultores, advogados e investir em treinamento. Os efeitos serão sentidos nas despesas com armazenamento de dados, no fluxo de trabalho e na melhoria da reputação. Mais que isso, novos negócios estão surgindo, com startups que oferecem soluções para projetos de privacidade e proteção de dados.

Em resumo, as empresas que tratarem dados corretamente vão valer mais, ganhar a confiança do mercado, gerar valor para os acionistas e conquistar a confiança do público. A In Loco, por exemplo, está auditando seus parceiros e fornecedores, pois não vai fazer negócios com empresas que não tratarem dados pessoais com segurança.

Para Raíssa Moura, a LGPD é uma grande oportunidade de unir todo o mercado com o objetivo de implantar a cultura de proteção de dados no Brasil. E isso só vai acontecer se forem formados grupos multidisciplinares, com pessoal técnico, especialistas em legislação, em relações com o consumidor, comunicação, recursos humanos, entre outras áreas. Privacidade é responsabilidade de todos. A hora da união é agora.

O impacto da LGPD nos negócios: o case da Raízen e seus 7 mil postos Shell

Adaptar à legislação de privacidade e proteção de dados de uma empresa que possui aproximadamente 29.000 funcionários, distribui combustíveis a sete mil pontos de venda a varejo através de revendedores, é o desafio de Paula Malta, gerente jurídica de marketing, data privacy e conveniência da Raízen.

A empresa é uma joint venture entre Shell e Cosan, que distribui combustíveis a postos com bandeira Shell, aeroportos e para clientes no mercado B2B, além de atender demandas diversas de consumidores finais que frequentam diariamente os postos da bandeira Shell (marca licenciada a Raízen) e as lojas de conveniência Shell Select e também dos clientes que utilizam os meios de pagamento da empresa e participam de ações comerciais.

Para conhecer o público que frequenta seus pontos de venda, a Raízen criou o aplicativo móvel Shell Box, uma plataforma que permite estabelecer conexão direta com o consumidor.

Paula Malta
Gerente Jurídico de Marketing, Meios de Pagamento, Inovação e Conveniência da Raízen

Linkedin →

Vídeo da Palestra →

De olho na tramitação do projeto da LGPD, a advogada Paula Malta passou a estudar a questão da privacidade e a fazer um microtrabalho de conscientização e engajamento das áreas-chave sobre as mudanças que estavam por vir.

Como toda gestão de mudança, sobretudo de cultura, aos poucos o tema foi melhor recebido, compreendido e incorporado pelas áreas. Quando em agosto de 2018, após oito anos se arrastando no Congresso, a LGPD foi aprovada, a partir daí, o assunto realmente tomou a força necessária para o avanço das discussões.

Começaram os treinamentos e as sessões de engajamento com maior intensidade e diversificação de público, objetivando o despertar nas equipes da consciência de que um processo de adequação a lei e realidade requer mudança de comportamentos, cultura organizacional, revisão de fluxos de trabalho, processos e tecnologia.

É um trabalho que começa como projeto e se transforma em um programa contínuo e perpétuo de monitoramento e aperfeiçoamento.

Para o projeto caminhar e dar certo, considerando as dimensões da Raízen, ficou clara a necessidade de contratação de uma PMO (Project Management Officer) com determinadas habilidades, incluindo não só o conhecimento da lei, mas também a capacidade de liderar uma mudança de mentalidade.

A empresa selecionou uma profissional para gerenciar o projeto de conformidade, e também optou por contratar uma consultoria externa para auxiliar nesse processo de maneira sustentável.

Um projeto, sem dúvida, desafiador, dado o grande volume de dados envolvido. Mas e por onde começar um projeto de conformidade? Deve-se começar pela realização de entrevistas com áreas-chave que realizam tratamento de dados, viabilizando o mapeamento das bases de dados. Através das conversas e entrevistas é que os mapeamentos se tornam possíveis.

Um conselho importante: atenção a contratação dos profissionais e consultorias. Deve-se observar se os profissionais e consultores disponíveis no mercado possuem experiência e conhecimento adequados a um projeto de grande responsabilidade e magnitude como esse. Deve haver um equilíbrio entre custo e benefício, objetivando o atingimento do maior e melhor nível possível de adequação a LGPD.

No caso dos fornecedores, há que se ficar atento na hora de selecionar os parceiros. Será preciso incentivar os prestadores de serviço, cuja contratação envolva tratamento de dados pessoais, a buscar conformidade mínima com a lei, pois o mercado vai acabar expurgando naturalmente quem não estiver adequado, pois os controladores de dados não irão

querer aumentar seu risco contratando operadores de dados que não estejam no mesmo nível de engajamento em relação a LGDP.

É uma jornada longa e vai exigir muito esforço conjunto das organizações, fóruns de discussão e outras iniciativas também setoriais. Além disso, em alguns pontos, teremos que aguardar determinados posicionamentos futuros que a própria lei já reserva e endereça à futura Autoridade Nacional de Proteção de Dados (ANPD).

Por seu lado, é certo que o consumidor, para “entregar” seus dados, vai escolher a empresa que melhor comprovar o cuidado com sua privacidade. E isso será um diferencial competitivo. Se perceber falhas na devida proteção dos dados, bastará a ele pedir a deleção do dado ou a sua portabilidade, migrando para a concorrência. Seguir a lei se torna, mais que nunca, uma questão de sobrevivência dos produtos e modelos de negócio.

O impacto da LGPD nos negócios: a mobilização da Globo para se adequar à lei de proteção de dados

Ana Paula Halla
Gerente Jurídico
Mídia e Conteúdo
do Grupo Globo

Linkedin

Promulgada em agosto de 2018, a Lei Geral de Proteção de Dados (LGPD) foi recebida com uma espécie de "luto" por parte do mercado. Pelo menos por aqueles que a consideram mais um obstáculo do que uma oportunidade. A primeira reação foi de negação ("a lei não vai pegar"). Depois veio a fase do pessimismo ("vou perder clientes, meus resultados vão despencar"), seguida da de ansiedade ("por onde eu começo?").

Mas sempre chega a hora de enfrentar a realidade e pensar nos mecanismos internos de tratamento de dados – sabendo que isso gera custos financeiros e humanos relevantes, risco de multas e de manchas na reputação de quem pisar na bola.

Não há dúvida de que a lei "já pegou", acredita a gerente jurídica do Grupo Globo, Ana Paula Halla. Ela mostrou como o conglomerado de mídia está se preparando para entrar em conformidade com a legislação durante a Privacy Week.

Segundo Ana Paula, a Globo enxerga a LGPD como uma grande oportunidade, por trazer segurança jurídica, incentivar a eficiência e a competitividade. E, principalmente,

porque fortalecerá a confiança dos titulares dos dados e dos parceiros de negócios.

Mesmo nas companhias com as melhores intenções, no entanto, o profissional responsável por garantir a adequação às novas regras, na certa, enfrentará resistência interna. Pensando nisso, o grupo contratou uma consultoria para auxiliar nos procedimentos.

Para quem está embarcando nesse processo, alguns pontos a serem trabalhados:

• Conscientização – é importante esclarecer a equipe em relação à LGPD, porque muitos acham que isso não vai afetar sua rotina de trabalho. Todos têm que entender que não é um projeto só do departamento jurídico, mas de toda a organização.

• Parceiros – clientes, fornecedores e prestadores de serviços precisam estar cientes de que a empresa está adequando os contratos à LGPD e, mais que isso, fazer a lição de casa, ajustando-se à nova legislação. Colaboradores e parceiros devem ficar atentos às cláusulas contratuais na hora de fechar um negócio, avaliando como o outro lado trata a proteção de dados. Muita gente ainda acha que a lei afetará apenas os gigantes, como Google e Facebook, e não se aplica aos pequenos.

• Mapeamento e revisão – não há como levar adiante um projeto de adequação sem primeiro identificar as bases de dados que a empresa possui. Mesmo quem tem políticas de privacidade, termos de uso etc. precisa fazer esse mapeamento, identificar os gaps e remediá-los. Todas as organizações vão passar por isso, mesmo as que não dispõe de um departamento jurídico grande. Elas terão que se adequar, do mesmo jeito.

• Monitoramento – é preciso entender o ambiente regulatório e acompanhar o desenrolar do assunto para ter certeza de que o negócio está de acordo com a regulamentação e com a jurisprudência que vai começar a surgir.

• Engajamento – investir em treinamento e reciclagem permanente é essencial. Além disso, o processo tem que envolver profissionais de diferentes áreas. Se a coisa ficar só na visão jurídica, o encarregado da proteção de dados será uma voz no deserto.

• Controles internos – devem ser eficientes para garantir a manutenção da conformidade. Se for necessário atender uma solicitação da autoridade reguladora, por exemplo, a empresa tem que estar preparada para fazê-lo com agilidade e precisão.

O processo é complexo, reconhece Ana Paula, mas as consequências serão piores para quem não começar a se preparar desde já. A lei entra em vigor em agosto de 2020. Um ano passa voando.

Não existe biscoito grátis

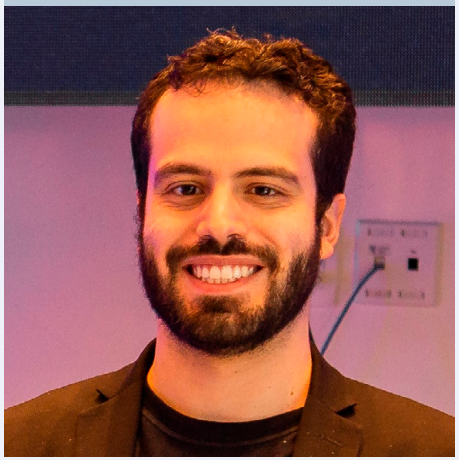
Quando a internet comercial foi formatada, lá no final dos anos 80, a ideia dos que a idealizaram era algo do tipo “tirar dos ricos para dar aos pobres”. Quer dizer, prover serviços gratuitos para os usuários e pagar a conta com dinheiro de publicidade (ou seja, dos anunciantes). Porque a conta sempre chega, e alguém tem que pagar. Esse é o modelo que perdura até hoje, com base na publicidade online.

Mas a prática de coletar informações para traçar o perfil dos usuários e entregar publicidade personalizada resultou, de um lado, em um mercado cada vez mais ávido por dados e, de outro, em menos controle, por parte das pessoas, sobre o que as empresas sabem delas e como usam isso para fazer negócios. Daí surgiram as leis que hoje colocam limites sobre o que se pode ou não fazer nessa festa de rastreamento, armazenamento e compra/ venda de dados de todo tipo.

Para Pedro Ramos, sócio do escritório Baptista da Luz Advogados e participante do evento, são pelo menos três os desafios a serem enfrentados pelas empresas nessa nova era: consentimento, transparência e controle dos dados.

O primeiro implica em informar de maneira clara ao

Pedro Ramos
Sócio da Baptista Luz Advogados e co-diretor de boas práticas de proteção de dados



Linkedin →

Vídeo da Palestra →

usuário que seus dados serão coletados para determinada finalidade – prestação de um serviço ou entrega de anúncios que realmente interessem. Entra aí a questão dos cookies, pequenos arquivos que servem para identificar o visitante de um site, mas que também estão relacionados a casos de violação de privacidade na web.

O consentimento esbarra ainda na questão do legítimo interesse – quando é justificável fazer uso da informação sem consentimento expresso (por exemplo, em casos de grave risco à saúde). Pedro Ramos acredita que essa alternativa pode, sim, ser usada pela publicidade. Se a pessoa está procurando por passagem aérea para determinado destino, provavelmente gostará de ver o anúncio de uma promoção que vai baratear sua viagem, mesmo que o envio não tenha sido solicitado ou autorizado.

Já na questão da transparência, o ponto é que a maioria dos sites não fornece mecanismos para o usuário entender que dados são coletados, de que forma, para quais fins e com quais empresas eles estão sendo compartilhados. Uma saída, já implementada por plataformas como o Google, são as centrais de privacidade, onde a pessoa consegue ver o que a empresa sabe sobre ela, retificar, excluir e até fazer download dos dados, para fins de portabilidade.

Por fim, quando se trata de controle, a legislação define que cada um é dono de seus próprios dados e deve ter o poder de controlá-los. Cabe às empresas encontrar uma forma de se adequar e, ao mesmo tempo, preservar o modelo de negócios que construíram.

A publicidade online ajudou a construir a internet que temos hoje, mas isso não dá a ninguém carta branca para fazer o que quiser. A Lei Geral de Proteção de Dados (LGPD) é uma oportunidade para se repensar modelo de negócios, transparência e criatividade da publicidade no digital. Esta é uma tarefa de todos: veículos, agências, anunciantes e audiência.

Dia 3
Cibersegurança, proteção de dados e privacidade

Nos últimos 12 meses, não se falou de outro assunto nos veículos de negócio, se não vazamento de dados, seja de informações pessoais até conversas em aplicativos ‘supostamente’ seguros e criptografados. A verdade é que onde há dado armazenado há possibilidade de vazamento. Afinal, é mais fácil destruir um sistema do que construir. A tecnologia é nossa maior aliada aliada no quesito segurança e conveniência, porém em alguns casos pode ser usada para nos prejudicar. Como sobreviveremos a essa onda de exposição e nos manteremos seguros? Quais são as técnicas que estão desenvolvimento para proteger cidadãos, empresas e a economia mundial?

Dados anônimos e pseudoanônimos: você sabe a diferença?

Segurança de dados é um assunto recorrente, mas só profissionais especializados conseguem realmente entender, desenvolver e aplicar métodos que garantam a integridade e a inviolabilidade de um banco de dados.

Para os leigos, as técnicas são um tanto complexas. Mas, além de saber quando e como utilizar essas ferramentas, quem trabalha com informações pessoais precisa entender pelo menos os conceitos básicos. E estar ciente de que todos os processos estão sujeitos a algum tipo de erro.

O engenheiro de software sênior da In Loco, Rafael Gouveia, mostrou as linhas gerais do trabalho dos profissionais de Data Protection na apresentação na Privacy Week. Começando do começo: o que são dados identificados, anônimos e pseudo-anônimos?

Dado anônimo é uma informação não identificada, ou seja, não é possível recuperar sua origem, verificar a quem ele pertence. Já o pseudo-anônimo é, em geral, identificável. Isso porque, apesar de não estar diretamente ligado a uma pessoa, com algumas operações é possível descobrir a quem ele se refere.

Rafael Gouveia
Senior Software Engineer na In Loco

Linkedin →

Vídeo da Palestra →

Tipos de dados

Identificado
Diretamente associado a identidade de um indivíduo
(Ex: CPF, E-mail, Nome, etc.)

Pseudo-anônimo
Não permite identificação de forma direta

Anônimo
Não permite identificação de forma direta ou indireta

São essas duas categorias que nos interessam no momento.

Sobre essas classes de dados, há três problemas a serem resolvidos:

Individualização: capacidade de distinguir dados e associá-los a uma única pessoa;

Linkability: capacidade de associar dados de bases diferentes;

Inferência: capacidade de deduzir, com alto grau de certeza, informações protegidas sobre algum usuário.

A pseudo-anonimização remove a associação direta da identidade de uma pessoa e reduz a capacidade de linkability, ou seja, de conectar uma base de dados com outra. Quanto mais se dificulta a associação de databases diferentes, mais complicado fica juntar informações suficientes para identificar o titular daqueles dados.

Criptografia

É uma forma de modificar dados, mas de um jeito que dá para transformá-los de volta como eram originalmente. A criptografia moderna se baseia em funções matemáticas, que podem ser determinísticas (ou seja, sempre que criptografar a mesma informação terei a mesma cifra) ou não – mas são sempre reversíveis.

As técnicas de criptografia também estão mais avançadas. Por exemplo, o sistema pode ter dois segredos: um que fecha o conteúdo (tornando-o impossível de ser lido) e outro que abre. Mais ainda: a chave que “fecha” o conteúdo fica com uma pessoa e a que “abre”, com outra. No final das contas, o que importa é que dados criptografados estão pseudo-anonimizados.

Entretanto, a criptografia não é uma técnica de anonimização – afinal, se existe uma chave, alguém vai conseguir extrair a informação original. Ou seja, de forma indireta, dá para associar a identidade da pessoa ao dado, basta decriptá-lo. Agora, imagine que você criptografou uma base de dados e perdeu ou jogou fora a chave. Aí, ninguém mais conseguirá decifrar as informações. Provavelmente, você terá um dado inútil, mas ele estará anonimizado.

Hash

Como a criptografia, as hashes também são funções matemáticas. Grosso modo, funciona assim: pega-se uma palavra, aplica-se uma função e obtêm-se um resultado que, aparentemente, não tem nenhuma relação com o dado inicial. Mas, toda vez que a mesma palavra passar pelo sistema, o resultado será igual. Com essa técnica, fica mais difícil transformar o resultado da função matemática na informação original ou associar bases de dados diversas.

As técnicas de pseudo-anonimização exigem alguns cuidados. Por exemplo, se a quantidade de informações sobre uma pessoa for muito grande, o conjunto facilitará a identificação do titular daqueles dados. E isso pode estragar toda a brincadeira.

A proposta da anonimização é resolver os problemas de individualização, linkability e inferência mencionados no início. Não é possível associar dados anonimizados a uma determinada pessoa, nem a outras bases. Além disso, será extremamente difícil fazer qualquer tipo de inferência. O processo pode ser executado via randomização (processos aleatórios) ou por generalização.

Técnicas de randomização

• Adição de erro: é quando se adicionando um “ruído” na

base, de forma proposital, para evitar que os dados sejam diretamente associados a uma pessoa. A operação exige cuidado pois, se forem colocados erros demais, perde-se a informação contida na base. Se aplicar de menos, será fácil para um especialista descobrir o truque. Agora, se o erro for colocado de forma estatística, mantêm-se as propriedades da base de dados.

• Permutação aleatória: nessa técnica, adiciona-se um erro em uma coluna, mas também trocam-se valores de colunas. Trocar aleatoriamente dados entre colunas de linhas diferentes é uma forma relativamente simples de anonimização.

• Privacidade diferencial: ainda em fase de pesquisa nos meios acadêmicos. O objetivo é definir um conceito matemático de privacidade. A ideia é a seguinte: pegar uma base de dados e tirar uma métrica. Suponhamos que o resultado dessa métrica seja X. Se tirarmos uma pessoa dessa base de dados e aplicarmos a mesma métrica, temos que conseguir o mesmo X. Trata-se de um conceito ainda muito novo e difícil de ser utilizado.

Técnicas de generalização

• K-anonimity: nesse processo, uma linha de uma tabela tem que ser indistinguível de k-1 linhas. Quanto maior o k, maior a privacidade. Se k é 5, o dado em questão não pode ser diferenciado de pelo menos outras 4 pessoas. Agora, se o k é 2, a chance de se conseguir identificar o titular é de 50% – como são só duas pessoas, o dado pertencerá a uma ou à outra. Aí fica fácil.

• l-diversity/ t-closeness: são dois conceitos criados para refinar a estratégia de K-anonimity. A ideia aqui é fazer com que cada grupo (k) tenha uma distribuição diferente de determinado dado (por exemplo, o diagnóstico de uma doença). Assim, um grupo formado por homens, nascidos em 1957, na cidade de São Paulo, pode ter como diagnóstico diabetes, infarto ou pressão alta. Intrusos não terão como saber quem tem qual doença. Quanto maior o grupo, maior a privacidade.

• Agregação: consiste em juntar os dados e extrair deles uma terceira informação. Por exemplo, se o que interessa é saber a média salarial dos engenheiros de uma empresa, basta agrupar os dados, fazer a contas e chegar ao resultado desejado. Os dados originais podem ser descartados. Outro tipo de agregação, mais complexo, é a estrutura probabilística. Funciona assim: os dados são inseridos na estrutura e ela, em vez de armazená-los, guarda características desses dados que podem ser utilizadas para fazer estimativas. Essa técnica, apesar de complexa, tem vantagens do ponto de vista computacional (as operações são realizadas mais rapidamente) e também para anonimizar as pessoas, pois reduz um conjunto grande de informações a uma estrutura menor e entrega um resultado estimado, associado a um erro.

Criptografia homomórfica

Não é nem randomização nem generalização, e sim um avanço da ciência da criptografia. Esse método permite pegar a cifra do dado (ou seja, aquele elemento que não se entende) e fazer operações matemáticas sobre ela. Essa informação é devolvida para o dono do dado, que tem a chave e vai conseguir decriptar, obtendo assim o resultado dessas operações.

Fica mais fácil de entender fazendo uma analogia. Vamos dizer que há um diamante que precisa ser lapidado, mas o joalheiro não é confiável. Então, coloca-se o diamante dentro de uma caixa dotada de luvas para manipulação do conteúdo e fecha-se a caixa com um cadeado. O joalheiro vai poder lapidar, mas não conseguirá tirar o diamante lá de dentro. Serviço pronto, o dono recebe a caixa de volta e recupera o diamante, agora em seu formato final.

Resumindo: o cliente tem uma chave que criptografa as informações a serem enviadas para o servidor. O servidor processa os dados sem entender o que está se passando, de forma anônima, e devolve o resultado para o cliente. Com a chave, ele conseguirá recuperar a informação “lapidada”. Ou seja, a empresa que vai fazer o tratamento pode operar sem conhecer os dados e, ainda assim, será capaz de atingir os seus objetivos e entregar o trabalho.

Cibersegurança e regulamentação para dispositivos conectados

Quando se estabelecem regras para a segurança de dados e proteção de informações pessoais, não dá para deixar de fora os dispositivos conectados (ou always-on), que são a base da chamada internet das coisas (IoT).

No Brasil, o Plano Nacional de Internet das Coisas foi oficializado por decreto presidencial (nº 9.854) em junho deste ano. A partir daí, o governo vai regulamentar o desenvolvimento e funcionamento de dispositivos conectados, como eletrodomésticos "inteligentes", assistentes pessoais, roteadores, impressoras e todo tipo de aparelho de automação residencial ou com inteligência artificial.

A medida é necessária porque este é um setor ainda amplamente desregulado, na opinião de Cláudio Lucena, professor de Direito da Universidade Estadual da Paraíba (UEPB) e pesquisador da Fundação para a Ciência e a Tecnologia (FCT) de Portugal.

Em se tratando de dados, já contamos com algum tipo de regulação. Embora o debate sobre governança, transparência

Cláudio Lucena
Professor da Universidade Estadual da Paraíba e Pesquisador da FCT (Portugal)

Linkedin →

Vídeo da Palestra →

e accountability esteja longe de acabar, pelo menos há regras estabelecidas.

No caso da internet das coisas, os Estados Unidos contam com normas setoriais (as dos segmentos financeiro e de saúde, por exemplo) e de agências reguladoras. A União Europeia tem a Network and Information Security Directive (NISD) e o Brasil, o Plano Nacional de Internet das Coisas.

Mas isso é só o começo. Até porque, a própria IoT ainda está em seus primeiros estágios. Tudo é tão incipiente que nem percebemos que as "coisas" não são mais simplesmente "coisas", mas máquinas e objetos dotados de sensores projetados para coletar e transmitir dados sem parar.

Um caso que gerou polêmica na Europa foi a boneca Cayla. Ela tem um microfone bluetooth conectado que imita a voz infantil, permitindo que "converse" com a criança. Investigações mostraram que as informações gravadas nos arquivos de áudio da boneca e as transcrições das conversas poderiam ser vendidas para agências militares, de inteligência e de segurança.

Além disso, quem ligava para um dos telefones pareados automaticamente por Cayla conseguia falar com a criança através do brinquedo. O governo alemão não teve dúvida e proibiu a comercialização do produto no país, por conter um "dispositivo de vigilância ilegal".

Recomendações

- Transparência na hora de pedir consentimento
- Empoderar o indivíduo para que possa controlar e gerenciar os dados coletados
- Adesão a padrões da indústria na ausência temporária de legislação
- Leis em conformidade com padrões internacionais mínimos

Outro exemplo de rastreamento via sensores é a seguradora John Hancock. A empresa anunciou que, em vez do seguro "tradicional", vai vender apenas planos "interativos", que monitoram a saúde dos usuários via wearables (como relógios e pulseiras) e smartphones. A ideia é simples: quanto

maior a expectativa de vida do cliente, mais tempo ele ficará pagando o seguro.

Diante da falta de definições mais precisas, Cláudio Lucena defende o estabelecimento de parcerias entre os órgãos de controle e o mercado para enfrentar o desafio regulatório e de governança que se apresenta.

Manter-se dentro de padrões éticos é o mínimo que se espera dos atores em cena nesse novo palco. Para o professor Lucena, além disso, poderíamos nos basear em princípios mais abrangentes, como os direitos humanos, por exemplo, que são padrões internacionais, criados para pessoas (e não para “coisas”).

Não é o caso de colocar obstáculos ilegítimos, mas identificar os aspectos positivos e negativos da tecnologia. E usá-la para o bem comum.

Na hora da crise, não deixe as decisões com o líder

Desde 2015, tem crescido exponencialmente, na América Latina, um tipo de ataque cibernético conhecido como sequestro de dados. Quando os computadores de uma empresa são bloqueados por alguém que pede dinheiro para liberar o sistema, além de uma crise interna (e, em alguns casos, externa), ela terá uma baita dor de cabeça.

Como esse tipo de crime só faz aumentar, as organizações precisam estar preparadas. Quem ainda não tem deve começar, desde já, a formar um comitê de crise para lidar com este e outros tipos de incidentes, como vazamento de informações de clientes, por exemplo. Aconteceu com a Netshoes, em 2017 e 2018, e com o Banco Inter, no ano passado. Pode acontecer com qualquer um.

Montar um grupo de profissionais internos para lidar com situações assim não é simples. Quem será o porta-voz na hora de falar com a imprensa, os clientes, os acionistas, as autoridades? Quais áreas da empresa devem estar representadas no comitê? Quem deve participar: a diretoria, os especialistas ou o pessoal que põe a mão na massa?

Thiago Sombra
Sócio do Mattos Filho, Veiga Filho, Marrey Jr. e Quiroga Advogados

Linkedin →

Vídeo da Palestra →

Mas isso é só o começo. Na hora em que a coisa começa a pegar fogo, que atitude tomar? A empresa estabeleceu protocolos a serem seguidos em situação de crise? E se o problema acontecer em horários incomuns – à noite, no fim semana, no meio do feriado –, dá para entrar em contato imediatamente com a pessoa responsável pela primeira linha de defesa?

Providenciar um comitê de crise com representantes do jurídico, TI, comunicações, marketing, recursos humanos (em alguns casos) e estabelecer os princípios que guiarão o navio em meio à tempestade são pontos fundamentais, conforme destaca de Thiago Sombra, sócio do Mattos Filho, Veiga Filho, Marrey Jr. e Quiroga Advogados.

E quanto ao capitão? Não seria ele uma figura central nessa hora? A princípio, pode parecer que sim. Mas ter executivos com poder de decisão no front traz mais riscos que benefícios. O ideal é deixar o pessoal de nível intermediário lidar com a questão e levar as opções à cúpula quando elas estiverem amadurecidas, evitando soluções precipitadas.

Por exemplo, no caso de sequestro de sistemas, o CEO que toma a frente da negociação pode decidir pagar o resgate exigido para encerrar logo a questão. Péssima medida: hackers que pedem valores baixos estão testando a empresa para ver se ela cede à chantagem e aumentarão o preço assim que perceberem que há disposição em pagar.

Alertas e providências

Outro aspecto relevante em casos de quebra de segurança é quem deve ser avisado sobre o incidente – acionistas, sócios, investidores, fornecedores, funcionários, autoridades (como Banco Central, Anvisa etc.). É preciso mapear a legislação aplicável ao caso, de preferência com auxílio de uma consultoria jurídica, para não deixar ninguém de fora.

Por fim, deve-se pesar se a polícia vai ser acionada, e quando. Afinal, o incidente pode ter sido causado por falha humana, ou pelos chamados “hackers do bem”, que invadem sistemas para expor as vulnerabilidades da segurança. Mas também pode ser um caso de extorsão, desvio ou furto por abuso de confiança – por exemplo, um ex-funcionário que leva os dados consigo quando deixa a empresa.

A recomendação é fazer uma investigação interna para entender o que está acontecendo, onde o esquema de segurança falhou e que medidas tomar. Nesse sentido, as primeiras horas são vitais. Segundo Thiago Sombra, existem muitos casos de incidentes malconduzidos logo no início, e isso é fatal. Só depois de tomadas as devidas providências e alertados os principais interessados é que a polícia deve ser chamada.

Empresas que pretendem atrair investidores devem contar com sólidos mecanismos de segurança e se certificar

de que seus parceiros de negócios façam o mesmo. Não adianta adotar um programa robusto de proteção de dados e compartilhar informações com fornecedores nem sempre confiáveis. Além de tudo, há o risco de o caso vazar para a imprensa e prejudicar a reputação da companhia. Sem dúvida, é o pior jeito possível de se aprender a lidar segurança e proteção de dados.

Dia 4
A conexão essencial entre compliance e privacidade

Tão importante quanto o dados de clientes são os dados de colaboradores, pessoas terceirizadas e parceiros de negócio. É preciso educar a todos sobre a coleta, armazenamento e tratamento de informações. A conscientização geral será fundamental para o sucesso de qualquer negócio, pois privacidade de dados não é responsabilidade de uma pessoa, é da empresa, é de todo mundo.

Controladores, operadores e titulares dos dados quem faz o quê?

Uma novidade instituída pela Lei Geral de Proteção de Dados (LGPD) são os chamados agentes responsáveis pelo tratamento das informações: o controlador e o operador de dados. O que os distingue é o poder de decisão. O operador pode realizar o tratamento do dado, mas a pedido do controlador, que é o dono da base (ou o responsável pelas informações). O controlador é quem está no topo da cadeia de tratamento de dados.

Controlador
O dono do banco de dados, é quem toma as decisões sobre o tratamento das informações

Operador
É quem realiza o tratamento dos dados em nome do controlador

Raíssa Moura
Diretora Jurídica da In Loco

Linkedin

Vídeo da Palestra

As responsabilidades do operador e do controlador têm que estar bem estabelecidas no contrato entre as partes, alerta Raíssa Moura. A head de legal da In Loco participou da Privacy Week, evento realizado pela empresa entre os dias 12 e 16 de agosto.

É bom ficar atento às empresas que tomam decisões sobre os dados, mas, no contrato, dizem que são só operadoras. Na maioria das vezes, quem detém o database é, ao mesmo tempo, controlador e operador. Melhor assumir de vez os dois papeis, para evitar problemas.

Controladores e operadores devem ter políticas de tratamento de dados, de preferência, conjuntas. Boas práticas privilegiam os direitos dos titulares e medidas de segurança e proteção das informações. Um bom plano de adequação à lei deve levar em conta, entre outros, os seguintes pontos:

• Ações educativas – a maior parte dos erros acontece por falha humana, portanto, todos os colaboradores devem entender a importância da privacidade. Não adianta contar com as melhores ferramentas se as pessoas que lidam com dados não estiverem cientes das suas responsabilidades.

• Mapeamento de riscos – identificar funcionários e parceiros que têm acesso às informações e relacionar quais os tratamentos de dados que podem causar problemas aos titulares.

4 passos para estar em conformidade com a LGPD

Preparação
Fortalecer o time responsável e incentivar o comprometimento de todos na empresa

Governança e controle
Montar um comitê para decidir práticas a serem adotadas e controlar o acesso aos dados

Políticas e procedimentos
Formular políticas para incidentes, segurança de dados, relacionamento com clientes etc.

Análise
Contratação de consultoria externa para verificar se todas as medidas necessárias foram adotadas

• Avaliação de impacto e risco à privacidade – o Data Processment Impact Access é obrigatório e poderá ser solicitado pela Autoridade Nacional de Proteção de Dados

(ANPD). Restam dúvidas sobre se o Judiciário pode cobrar isso durante o período de adequação (até agosto de 2020). Definir essa questão é uma das medidas que se espera da ANPD.

• Governança – a legislação estabelece que tanto o operador quanto o controlador podem implementar boas práticas, mas o controlador é quem tem a obrigação de estabelecer um programa de governança. Não só para comprovar que está cumprindo a lei, mas para atuar com transparência e inspirar confiança entre os titulares dos dados.

• Resposta a incidentes – é aconselhável ter um plano muito bem preparado para que, em caso de crise, a empresa saiba o que fazer, quem avisar, que medidas tomar.

Como exemplo, a In Loco formou um time de pesquisa e desenvolvimento para criar as práticas e planejou um programa em quatro fases, a serem implementadas no período de um ano. São elas: preparação; governança; políticas e procedimento; e análise geral do projeto.

O essencial é fomentar a cultura da proteção de dados, de modo a conscientizar as equipes sobre a importância do tema e a responsabilidade de cada um. E sempre documentar as providências que foram tomadas ao longo do processo, para comprovar que os profissionais foram treinados e as melhores práticas, implementadas.

Does & Dont's: 10 dicas do que fazer (e do que não fazer) para implantar a cultura de proteção de dados pessoais nas empresas

Embora a confiança do consumidor tenha se tornado a moeda de troca mais importante para produtos e serviços na era digital, metade das empresas que participaram de uma pesquisa da KPMG admitiram que não têm uma visão única de todas as interações com seus clientes.

Mesmo reconhecendo que a tecnologia é uma das bases para se estabelecer relacionamentos rentáveis com a clientela, 41% das organizações não têm estratégias empresariais digitais claras, de acordo com o estudo Construindo a Confiança Técnica, produzido pela consultoria.

Em termos práticos, a gerente de cyber security e privacidade da KPMG, Isabella Becker, aponta cinco medidas a se tomar e cinco erros a serem evitados por empresas que estão trabalhando para se adequar à Lei Geral de Proteção de Dados (LGPD), que entra em vigor em agosto de 2020.

Isabella Becker
Gerente de Cyber Segurança e Privacidade na KPMG

Linkedin →

Vídeo da Palestra →

O que não fazer

• Subestimar quantidades: calcule bem desde o tempo que levará para adequar a organização até a quantidade de dados que terão que ser mapeados, sem esquecer as contas inativas, colaboradores desligados etc. (estes dados também estão no escopo da LGPD).

• Tratar a questão como um processo apenas da diretoria: o processo tem que ser de P a P, do porteiro ao presidente. Todos os colaboradores devem ter noção da lei de proteção de dados e de como a companhia está se portando em relação a ela.

• Tratar o projeto como se tivesse fim: é preciso implementar medidas para monitoramento contínuo. Um projeto de adequação é um projeto de compliance: torna-se atividade cotidiana da empresa.

• Treinar no onboarding: logo no primeiro dia de trabalho, o colaborador tem que estar inteirado de suas funções e de como a empresa lida com a legislação de privacidade. Muitos ainda acreditam que a lei não se aplica a sua área de atuação, ou que será mais uma daquelas que "não vai pegar". O processo de treinamento deve ser personalizado por área, para que cada uma entenda os desafios da legislação e como será afetada.

• Pensar na implementação antes do assessment: a hora certa de se entender qual a situação da empresa é quando se procede à avaliação (assessment). É o momento de fazer entrevistas com os colaboradores para descobrir gaps e entender onde a companhia está em relação ao que diz a lei. O ideal é sair dessa fase com um mapa do que deve ser feito para levar a empresa do ponto onde está até aquele em que quer chegar.

O que fazer

• Entrevistas de mapeamento: elas funcionam como um método indireto de conscientização, em especial para aqueles que consideram que seu trabalho não envolve informações pessoais, ou que não precisam se preocupar porque não tratam os dados, só têm acesso a eles. A própria responsabilização do gestor acontece na entrevista e na hora da validação.

• Utilizar plataformas para gestão de privacidade: essa etapa pode ser dividida em quatro pilares: documentação, mapeamento, proteção e apoio.

• Assessment paralelo de segurança de informações: a dica aqui é aproveitar a estrutura do projeto de adequação para a condução das entrevistas, para avaliar o nível de maturidade dos processos (estado atual e desejável), comparar-se com o benchmark do ISF (Information Security Forum) e avaliar a segurança cibernética utilizando os controles implementados

•Tratar incidentes de dados pessoais de maneira diferenciada :

nem tudo são dados pessoais; é preciso diferenciá-los dos demais. Nesse sentido, uma boa forma de lidar com incidentes é avaliar a natureza e categoria da ocorrência, o estado do dado envolvido, a facilidade (ou não) de identificação do titular e a gravidade das consequências.

• Ser âncora da sua indústria: práticas hoje consideradas inovadoras logo serão padrão. As empresas que se posicionarem como as primeiras de seu segmento a adotar boas práticas serão as que ditarão o caminho a ser seguido pelo mercado.

Proteção de dados e RH: como gerir os dados do funcionários dentro dos limites da privacidade

Quando se fala na Lei Geral de Proteção de Dados (LGPD), a primeira coisa que vem à mente é a adequação dos procedimentos de coleta, tratamento e armazenamento de informações dos clientes. Mas a tarefa não acaba aí: os dados dos colaboradores, pessoal terceirizado e parceiros de negócios também entram no pacote.

Sócio da Missão Compliance e do escritório PCMM Advogados, Luciano Malara aponta três tarefas que todas as empresas, de qualquer setor, devem cumprir para entrar em conformidade com a lei: prevenir, detectar e remediar.

Malara destaca que o compliance é uma parte do que se convencionou chamar de governança corporativa. A governança deveria ser incorporada à cultura de empresas de qualquer porte porque, mais que a conformidade com a lei, é uma política que tem a ver com integridade de ações e objetivos.

Princípios de gestão de colaboradores em conformidade com a LGPD:

Luciano Malara
Sócio Fundador da Missão Compliance

Linkedin →

Vídeo da Palestra →

• Equilíbrio – as empresas têm um ano para se adequar à lei, tempo suficiente para planejar e implementar as medidas necessárias.

• Conhecimento – promover a conscientização dos funcionários e das lideranças sobre o papel e a importância de cada um nessa nova cultura de proteção de dados.

• Bom senso no tratamento dos dados dos colaboradores.

• Boa fé – não ficar apenas no discurso, cumprir o combinado em termos de coleta e utilização das informações.

Diretrizes e conceitos

• Na captação de dados: cuidados extras ao descartar ou repassar currículos de candidatos a vagas na empresa.

• Tratamento: atenção ao buscar informações externas sobre os funcionários ou candidatos (em alguns casos, o background check, ou verificação de antecedentes, é permitido).

• Dados pessoais x dados sensíveis: deixar clara a diferença entre ambos. Dado pessoal é o que permite a identificação direta (nome, telefone etc.) e dado sensível revela características como etnia, religião ou alinhamento político (que não precisam ser de conhecimento da empresa).

Diante da complexidade da questão, o aconselhável é focar em três pontos: se é legítimo requisitar a informação, se ela está sendo obtida da forma certa e se será utilizada da maneira correta. Por exemplo, algumas religiões não permitem o trabalho aos sábados. O empregador não precisa perguntar a crença religiosa do candidato, basta saber se ele tem disponibilidade para trabalhar após as 18h de sexta-feira. O pedido é legítimo (pois o trabalho aos sábados, no caso, é uma exigência da função) e a resposta não envolve um dado sensível.

Prevenção
Evitar violações adotando-se regras que forneçam instruções claras de contuda nos negócios

Detecção
Através de monitoramento, auditoria, canais de denúncia etc.

Controle de danos
Responder claramente em caso de erro ou falha e manter projetos de melhoria constante

Um bom processo de compliance em RH deve começar do básico:

• Quais dados a empresa pode coletar? Em tese, qualquer um.

• Quais ela quer, precisa ou deve ter? Uma coisa é querer, outra é precisar da informação. Se a empresa não for oferecer

plano saúde, não precisa perguntar se o funcionário já tem um.

• Como essas informações serão geridas? É necessário muito cuidado com o uso que vai ser feito dos dados.

• O que guardar? Nem tudo. Uma vez comprovado o endereço, por exemplo, o documento que foi utilizado (em geral contas de água, energia, condomínio) pode ser devolvido, não precisa ficar na empresa.

• Como guardar? Pode ser armazenamento físico, digital, dentro da empresa, na nuvem, em serviços terceirizados. Cada um decide o que é melhor no seu caso.

• Aonde guardar? Digitalizar e arquivar na nuvem (própria ou de fornecedores) ou guardar fisicamente são as opções mais usadas.

• Quem pode acessar? As informações devem ser de acesso restrito a quem efetivamente tem necessidade dentro do RH.

• Para que acessar? Nem todos têm que ter acesso a tudo. Assim, se houver falha humana, poucos funcionários estarão envolvidos.

• Como limitar o acesso? Controles internos não são suficientes, deve-se contar com ferramentas de segurança para proteger os dados de invasões externas.

• Como documentar? Quando a autoridade fiscalizadora pedir esclarecimentos, é preciso mostrar de forma prática quais processos foram implementados.

Por fim, a contratação de terceirizados também precisa estar de acordo com o que determina a Lei Geral de Proteção de Dados.

Novas normas para contratação de terceirizados

- Atestado de implementação
- Concordância com exibição de dados pessoais
- Programa de alinhamento entre encarregados
- Identificação de responsabilidade e ações

Dia 5
Lei geral de proteção de dados: Um debate jurídico sobre a lei brasileira.

A aprovação da Lei Geral de Proteção de Dados (LGPD) colocou o Brasil na lista de países que contam com uma legislação específica para a coleta, armazenamento, uso e tratamento dos dados dos seus cidadãos. A cada dia fica mais evidente que o modelo predominante de uso de dados é indispensável, porém pode ser irresponsável, perigoso e até abusivo. Como é que a justiça irá lidar com o tema? Quais serão as penalidades e consequências da lei no Brasil? Nosso judiciário está preparado para tratar de casos de vazamento de dados de milhares de cidadãos?

Regulamentação e educação do mercado, as duas grandes tarefas da ANPD

A aprovação da Lei Geral de Proteção de Dados (LGPD) é considerada uma conquista da sociedade brasileira, mas não foi obtida sem que se ultrapassassem diversos obstáculos. Antes do escândalo envolvendo o Facebook e a consultoria Cambridge Analytica na eleição do presidente dos Estados Unidos (em 2016), o tema mal aparecia no radar dos brasileiros, muito menos no dos parlamentares.

Membro da Comissão Especial de Proteção de Dados da OAB (Ordem dos Advogados do Brasil), o advogado e professor Fabrício Mota participou do processo que culminou com a promulgação da nova legislação. Sócio do escritório Garcia de Souza Advogados e integrante da International Association of Privacy Professionals (IAPP), ele lembra que, no início das discussões, havia interesses comerciais contrários à adoção de uma lei sobre uso de dados. O argumento era que o Brasil já contava com instrumentos jurídicos suficientes, como o Marco Civil da Internet, o Código de Defesa do Consumidor e a própria Constituição Federal.

Fabrício Mota
Sócio do Garcia de Souza Advogados e Professor de Proteção de Dados Pessoais

Linkedin →

Vídeo da Palestra →

A manipulação das redes sociais para influenciar o voto na eleição norte-americana acendeu a luz amarela no Legislativo, que finalmente aprovou uma legislação sobre de proteção de dados, em agosto de 2018. Na avaliação de Fabrício Mota, a lei brasileira é menos completa e refinada do que o General Data Protection Regulation (GDPR) europeu, mas, ainda assim, vai afetar todos os setores da sociedade.

As atenções se voltam agora para a formação da Autoridade Nacional de Proteção de Dados (ANPD), órgão federal que vai editar normas e fiscalizar procedimentos sobre proteção de dados pessoais. Caberá à ANPD elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, além de aplicar sanções em caso de descumprimento da lei.

A ANPD terá uma diretoria com cinco membros, que serão nomeados para mandatos fixos, e um Conselho Nacional de Proteção de Dados Pessoais e da Privacidade composto por 23 representantes de órgãos públicos e da sociedade civil. O receio de quem acompanha o assunto é que indicações políticas comprometam a atuação da Autoridade. Para Fabricio Mota, se a ANPD não for uma entidade de alto nível, com profissionais capacitados, não teremos um órgão respeitado.

Quer os brasileiros queiram ou não falar sobre proteção de dados, o assunto tem que entrar na pauta do dia, pois todos que lidam com informações pessoais deverão se adequar à lei – do empresário individual a agentes econômicos que forneçam ou consumam produtos e serviços.

Não há como saber, ainda, se a ANPD vai atuar para ajudar ou para prejudicar o equilíbrio das forças de mercado. A opinião dominante é que, nos primeiros meses, o órgão deve ter atuação mais educativa do que punitiva, sob pena de não conseguir criar um sistema saudável.

Embora necessária em casos extremos e persistentes de descumprimento da lei, a punição não é o caminho mais adequado. O ideal é que a ANPD paute sua atuação mais na educação do mercado, no primeiro momento, do que na aplicação de sanções.

Vale lembrar que este assunto não diz respeito apenas à União, mas também a estados e municípios, que terão de se adequar e se preparar para aplicar a lei em nível local. Esta é uma discussão que tem que ser levada às instâncias com poder de decisão. A sociedade brasileira, que foi muito atuante no processo da LGPD, tem que continuar em alerta na sua regulamentação.

Proteção de dados, novo celeiro de oportunidades para quem quiser encarar o desafio

Dirceu Santa Rosa
Sócio da Montaury Pimenta Machado & Vieira de Mello Advogados

Linkedin →

Vídeo da Palestra →

No dia 15 de agosto de 2018, o direito digital no Brasil viu surgir toda uma nova área de atuação, a da proteção de dados. Com isso, a Lei Geral de Proteção de Dados (LGPD) está dando a profissionais de diversas áreas a chance de começar de novo. Para Dirceu Santa Rosa, da Montaury Pimenta Machado &Vieira de Mello, em 2019, os especialistas em direito digital "entraram na moda".

Haverá oportunidades de todos os tipos para quem souber procurar. Da mega empresa de tecnologia à academia de ginástica, passando por prestadores autônomos e até instagramers, todos terão que se adequar à legislação, que entra em vigor em agosto de 2020. Para quem quiser aproveitar a onda, o momento de entrar nessa área é agora. A demanda será grande o suficiente para empregar profissionais em projetos de diversos níveis de complexidade.

E daqui para frente? Ainda não temos ideia de como a Autoridade Nacional de Proteção de Dados (ANPD) vai funcionar na prática – se terá um perfil regulador ou mais agressivo, no

sentido fiscalizatório e punitivo. No primeiro momento, o ideal seria que a entidade desenvolvesse um trabalho educativo, de disseminação da cultura de proteção de dados.

Com as organizações adequadas à legislação e a ANPD em funcionamento, entraremos em outra fase, na qual empresas ou consumidores vítimas de ataques, incidentes ou problemas imprevisíveis (falha humana, por exemplo) buscarão seus direitos na Justiça. Para além das disputas legais, profissionais com conhecimento em direito e tecnologia da informação serão sempre requisitados, pois o compliance é um processo constante, que não tem fim.

De olho nisso, multiplicam-se as certificações internacionais (como a da International Association of Privacy Professionals/ IAPP ou o Exin Privacy and Data Protection) e cursos específicos para formação de DPOs (data protection officers). O mercado está aquecido e a oferta de mão de obra especializada é escassa.

Para as empresas, o investimento vale a pena: estudo do Instituto Ponemon indica que o custo associado de uma invasão de dados aumentou 12% nos últimos cinco anos, chegando ao valor médio de US$ 3,92 milhões em 2019. No Brasil, o custo médio de uma violação de dados é de US$ 1,35 milhão.

A legislação europeia (General Data Protection Regulation) será importante como benchmark para a ANPD, na opinião de

Violação de dados, um problema muito caro

Mais de 50% das violações de dados foram resultado de ciberataques, que custaram às empresas US$ 1 milhão a mais, em média, do que as originadas de causas acidentais.

Violações de dados por ataques maliciosos cusaram às empresas US$ 1 milhão além do que as originadas de causas acidentais.

Quase metade das violações se devem a erro humano e falhas no sistema, custando às empresas US$ 3,5 milhões e US$ 3,24 milhões, respectivamente.

Violações originadas de terceiros, como parceiros ou fornecedores, custara às empresas US$ 370 mil a mais que a média.

Empresas com equipe e plano de resposta a incidentes reduzem em US$ 1,23 milhão os custos de violação de dados (em média) em relação às que não

Fonte: Cost of a Data Breach 2019 / Instituto Ponemon

Dirceu Santa Rosa. Entretanto, na sua análise, a adequação da legislação nacional à GDPR (como foi feito no Uruguai e no México, por exemplo) não mostrou, até agora, ser vantajosa no sentido de gerar negócios fora do mercado europeu.

Para ele, o Brasil, com seus mais de 200 milhões de potenciais titulares de dados e com escassa cultura de proteção, já tem lição de casa suficiente para se ocupar por um bom tempo. A prioridade é resolver problemas internos, definir como a ANPD vai atuar e evitar a judicialização das demandas.

Procura-se DPO para início imediato. Paga-se bem

Especialista ainda raro no mercado, o data protection officer (DPO), ou encarregado da proteção de dados (como define a lei brasileira), deve ser um profissional preparado para atuar como compliance officer de dados. Pelo menos, este é o perfil que as empresas estão buscando: o de alguém capaz de conduzir o processo de adequação da organização à Lei Geral de Proteção de Dados (LGPD), que passa a valer de verdade em agosto de 2020.

Membro da IAPP (International Association of Privacy Professionals), o advogado Henrique Fabretti explica que as empresas não querem um DPO que atue apenas como ponto de contato com a autoridade reguladora, ou no treinamento dos funcionários. Elas estão preferindo contratar profissionais para liderar o processo de conformidade da organização e assegurar que ela continuará nos trilhos.

Vale destacar dois pontos em relação aos deveres e responsabilidades do DPO, que na lei brasileira são diferentes dos da europeia, o GDPR (General Data Protection Regulation).

1. O GDPR deixa claro que o DPO é responsável por

Henrique Fabretti
Especialista em Serviços de DPO e Proteção de Dados na Opice Blum

Linkedin →

Vídeo da Palestra →

monitorar os procedimentos da empresa, de modo a garantir que suas políticas e práticas cumprem a lei. Mas a LGPD, não. A legislação brasileira não diz que o DPO tem que atuar como compliance de dados. No GDPR, essa é sua principal função.

2. Segundo o GDPR, o DPO tem o dever de cooperar com a autoridade fiscalizadora. O Reino Unido prevê até responsabilização criminal se ele não colaborar. Já a LGPD usa o termo "ponto de comunicação entre a autoridade e o controle de dados", mas não atribui papel de cooperação. Entretanto, isso não quer dizer que ele pode mentir. No limite, não se poderia, em momento algum, ocultar qualquer tipo de informação.

No episódio da utilização de dados de usuários do Facebook para influenciar o eleitorado norte-americano em 2016, Fabretti lembra que a rede social fez diversas mudanças em sua política de privacidade ao longo dos últimos 15 anos, inclusive se comprometendo a não compartilhar dados de amigos dos amigos.

Assim, quando a Cambridge Analytica teve acesso a essas informações, elas chegaram a ser bloqueadas. Mas, por algum motivo, acabaram novamente liberadas para a consultoria. Seria papel do DPO, evitar que este tipo de situação acontecesse. As consequências do caso foram bastante prejudiciais à empresa, que perdeu quase 10% de participação de mercado e está lutando para recuperar isso.

Na Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados, onde Fabretti, atua como especialista em serviços de DPO e proteção de dados, a orientação para os clientes é serem discretos em relação à contratação de encarregados de dados, pois a concorrência por esses profissionais é intensa. Por outro lado, esta é uma grande oportunidade para quem se interessa em atuar na área. A dica é buscar certificações, como a da IAPP, e ter apetite para enfrentar o desafio.

Qual o perfil da sua empresa na proteção de dados - conservador, intermediário ou de risco?

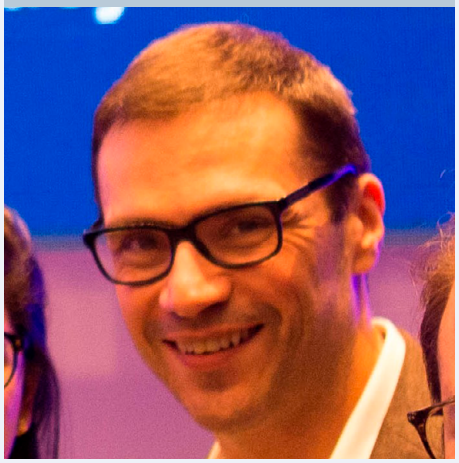
Dado é algo que identifica, ou potencialmente pode identificar, uma pessoa. Tratamento de dados é toda atividade passível de ser realizada a partir de informações. É por isso que a Lei Geral de Proteção de Dados é tão abrangente, e tem gerado tantas dúvidas e incertezas. A regulamentação da LGPD está a cargo da recém-criada Autoridade Nacional de Proteção de Dados (ANPD), que ainda tem muito trabalho pela frente.

Só que o mercado tem apenas cerca de um ano para se adequar – isso se o prazo fixado para a entrada em vigor da legislação (agosto de 2020) não for prorrogado. O que se pode fazer, no momento, é estudar os modelos adotados em outros países e ver o que faz sentido para o Brasil.

O conselho é do consultor Marcel Leonardi, do Pinheiro Neto Advogados.

Nesse cenário ainda marcado pela indefinição, a primeira coisa a fazer é decidir que postura adotar enquanto organização – tradicional, mediana, ousada? Por exemplo, a

Marcel Leonardi
Consultor no Pinheiro Neto Advogados



Linkedin →

Vídeo da Palestra →

empresa pode adotar uma política conservadora, solicitando o consentimento para toda e qualquer coleta de dados.

Mas será que não haverá um momento em que as pessoas vão se cansar e recusar a permissão? Uma alternativa seria tratar os dados com base no conceito de legitimo interesse, mas isso pressupõe riscos maiores. A empresa estaria disposta a assumi-los?

Definido o risco na primeira etapa, é hora de estabelecer o posicionamento em relação ao mercado. A empresa quer se engajar realmente nessa adequação ou será apenas um movimento aparente? Se for para valer, a cultura de proteção de dados deve se estender a toda a cadeia de negócios.

Alguns players já começam a exigir de seus fornecedores e parceiros que entrem em conformidade com a legislação. Para tanto, é necessário que eles entendam o que significa se adequar à LGPD. É bem verdade que, há um ano, quando a lei foi promulgada, o desconhecimento era maior. Mesmo assim, e considerando o prazo-limite estabelecido, a falta de informação ainda é grande.

A implementação de um projeto de adequação começa por entender quais dados a empresa possui e fazer o mapeamento disso. Não é incomum descobrir, nessa hora, uso de dados em áreas que nem se imaginava. A dica é entender, de fato, para quais finalidades as informações estão sendo usadas. Aqui é preciso contar com a sinceridade dos colaboradores para explicar o que, de verdade, eles estão fazendo com os dados.

Tudo isso dá trabalho. Marcel Leonardi alerta que as organizações estão “empurrando com a barriga”, deixando para se ocupar do assunto perto do fim do prazo. Entretanto, só a etapa de benchmark pode levar de três a quatro meses. Depois, é preciso entender a base legal onde a empresa se enquadra, atualizar políticas, mudar contratos etc. O processo é mais complexo do que aparenta.

Existe ainda o desafio do orçamento, pois não se trata de um problema puramente legal. Há questões jurídicas simples, mas cuja viabilização técnica é complexa e custosa.

Quem ainda não começou a se mexer deveria olhar para outras empresas, fazer benchmark e perceber que um ano já passou. Trata-se de um projeto mais complexo do que a maioria imagina, porque além do trabalho interno há fatores externos, como engajar os parceiros e ficar atento ao que vai decidir a autoridade regulatória.

O fato é que a LGPD vai atingir a todos, e não necessariamente pelo lado punitivo, mas por exigência do próprio mercado. A hora de se preparar é agora.

Lei Geral de Proteção de Dados: essa já pegou

Com o prazo de um ano para a entrada em vigor da LGPD (que passa a valer para valer em agosto de 2020), muito tem sido discutido sobre se a lei será daquelas que “vai pegar” ou não. Para Rodrigo Colares, sócio do Da Fonte Advogados, proteção de dados é algo que veio para ficar.

O assunto não é novo. Desde 1995, a União Europeia já contava com a Diretiva 95/46/EC, relativa ao processamento de dados pessoais. A norma exigia que cada país-membro tivesse uma agência ou comissário de proteção de dados. A Diretiva foi substituída pelo General Data Protection Regulation (GDPR), em 2018.

No Brasil, ninguém tem dúvida que a lei de direitos autorais funciona. Antigamente, os direitos patrimoniais de autor não eram regulados e as obras não tinham a proteção que têm hoje. O exemplo serve de parâmetro para a proteção de dados.

No caso de empresas de inovação ou que fazem tratamento de dados de forma intensiva, é imprescindível ter no core business uma cultura muito clara de proteção. Ou seja, é algo que tem que estar bem assimilado por todos os funcionários.

Rodrigo Colares
especialista em M&A, Tecnologia e Propriedade Intelectual e Sócio da Fonte Advogados

Linkedin →

Vídeo da Palestra →

Depois de quase uma década (o projeto da LGPD ficou por oito anos no Legislativo) chegamos em um novo momento, de aculturamento sobre a proteção de informações pessoais. A partir de agora, os modelos de negócios devem incorporar a noção de privacy by design, pensando a questão da proteção de dados desde a concepção do produto ou serviço.

Temos ainda o problema do legado – o que fazer com os dados já coletados e armazenados? Há que ser cauteloso nesse campo. Muitas empresas têm no tratamento de dados o coração do negócio, mas outras, não. Juristas e advogados podem propor estruturas que mitiguem os riscos para uma organização que não tem nos dados seu principal business.

Um caso prático (e real) de empresa que usa dados para alavancar seu negócio principal é o de uma rede atacadista em processo de transformação digital. A companhia lançou um portal de e-commerce, ciente de que o tipo de risco presente no varejo tradicional é completamente diferente do risco na internet. Segundo Colares, uma forma de lidar com a questão é separar as entidades de um mesmo grupo, para que cada uma possa tratar os dados da maneira que for melhor para os seus objetivos específicos.

Existimos para facilitar a vida das pessoas.

Somos uma empresa de tecnologia que fornece inteligência a partir de dados de localização. Nossas soluções permitem que empresas entreguem mais relevância, garantindo o anonimato dos seus consumidores. Para nós, privacidade e conveniência para as pessoas significam mais resultados para as marcas.

Atualmente somos 180 funcionários e estamos distribuídos entre Recife, São Paulo e Rio de Janeiro.

Conheça nossas soluções

inloco