patrocínio

MICRO FOCUS

COMO SE PREPARAR PARA A NOVA LEI DE PROTEÇÃO DE DADOS?

Como já ocorre na União Europeia desde maio, quando entrou em vigor a GDPR (General Data Protection Regulation ou Regulamento Geral de Proteção de Dados), a LGPD (Lei Geral de Proteção de Dados) passa a vigorar também no Brasil, em fevereiro de 2020. Com isso, as empresas têm a responsabilidade de adequar sua política de proteção de dados às novas regras. Trata-se de um desafio tanto maior quanto mais ricos e volumosos forem os bancos de dados mantidos pelas empresas. Temas como o direito ao esquecimento, a definição de finalidade dos dados e a necessidade de obtenção do consentimento dos cidadãos são novidades que terão impacto na gestão e na estratégia das empresas.

Afinal, os cidadãos têm o direito de saber quais informações fornecem aos prestadores de serviços. E a empresa deve explicar por que requisita dados do cliente, e para qual finalidade eles serão usados. Mais do que isso, precisa ser capaz de arquivar e recuperar dados sensíveis e valiosos de seus clientes, de forma muito mais rápida e segura do que fazem os sistemas convencionais de backup. Isso tudo exige das empresas novas políticas de governança e de conformidade com as novas regras. Nesse ponto, o papel do CIO é fundamental e ele precisa contar com apoio executivo, com apoio de pessoas e empresas especializadas e, claro, com ferramentas que o ajudem a dar conta dessa tarefa.

É o que discutem os participantes desta mesa-redonda, conduzida pelo diretor de redação do Informática Hoje, **Wilson Moherdaui**. Participaram do debate: **André** Tritapepe, gerente geral de governança de TI da Braskem; **Carlos Augusto** de Oliveira, do Banco Original; **Célio** Bozola, presidente da Prodesp; **Cesar** Costa, diretor de tecnologia da Fidelity; **Curt** Zimmermann, responsável por TI e Operações da Bradesco Seguros; **Daniel** Bocalão, gerente de conectividade e segurança da informação da Sabesp; **Igohr** Schultz, diretor de infraestrutura e segurança da Vivo; **Marcel** Leonardi, consultor do Pinheiro Neto Advogados; **Rogério** Câmara, diretor executivo do Bradesco; e **Waldir** de Santis, diretor executivo da Boa Vista Serviços.

Informática Hoje - Esta é a primeira mesa-redonda que fazemos sobre o tema, mas certamente não será a última. A Lei Geral de Proteção de Dados Pessoais deveria ter entrado em vigor em 14 de agosto deste ano, mas esse prazo foi prorrogado até fevereiro de 2020. Me parece que o principal desafio de vocês é a conscientização, não só

Hamilton Penna

“Em prevenção à lavagem de dinheiro, já existe uma lei que nos obriga a coletar e tratar determinados dados, independente da vontade do cliente”.

Rogério, do Bradesco

da área de TI, mas das corporações como um todo, de que precisarão investir em capacitação, treinamento, enfim, em todas as iniciativas necessárias à adequação às novas regras. Como se trata de uma lei transversal, vai afetar a todos os setores da economia e todos os portes de empresas. Então, quero abrir esta conversa justamente pelo Marcel, para que ele faça uma introdução ao tema e, principalmente, que mostre a conexão entre o espírito da lei e a realidade que será afetada por

Marcel - Antes de assumir o papel de consultor do Pinheiro Neto, passei oito anos na área institucional do Google, então trabalhamos intensamente na elaboração desse projeto de lei. Acho que um ponto interessante a se destacar é que o primeiro grande esforço legislativo para colocar uma lei parecida com essa no Brasil começou em 2010, quando o Ministério da Justiça fez uma consulta pública, perguntou para a sociedade se isso fazia sentido ou não. Aí a coisa ficou um pouco paralisada. Em 2012, o setor de publicidade e propaganda procurou um parlamentar de São Paulo para apresentar um projeto para colocar os termos do debate. Era um projeto extremamente fraco do ponto de vista jurídico, porque a intenção era de deixar a regulação a mais flexível possível. Então ele serviu, na falta de uma expressão melhor, quase como boi de piranha, mais para colocar os termos do debate. Em 2013, surge um projeto, esse sim muito mais inspirado no modelo europeu, já com um objetivo mais claro. No segundo governo Dilma, o governo decidiu que queria o seu próprio projeto de lei e promoveu algumas discussões, também por meio de consulta pública, que redundaram no projeto 5.276, que é o que acabou resultando nesse texto final que a gente conhece hoje. Em termos de motivação estratégica de estado, a intenção era dizer mais ou menos o seguinte: o direito europeu criou, desde 1995, uma norma específica

a respeito disso, reformou essa norma com o GDPR, que foi aprovado em 2016, e passou a valer agora a partir de maio de 2018. Então, o Brasil precisava de uma norma parecida. Todo o setor privado ficou praticamente adormecido nesse debate; quem acabou ocupando os espaços foram os acadêmicos, os ativistas, principalmente o pessoal da área dos direitos digitais. Tirando o setor financeiro, que estava começando a se movimentar, assim como o de crédito, por razões óbvias, o pessoal estava paralisado. O resultado disso é que esse modelo europeu, mais rígido e mais restritivo, acabou sendo a origem. Muita gente se pergunta por que a gente não copiou o modelo canadense ou o modelo americano que têm regras muito mais livres. Essa é a resposta: o setor privado não entendeu que isso o afetaria. Dessa forma, prevaleceu o modelo europeu, mais restritivo, e que adota um conceito de dado pessoal amplíssimo. A lei fala que dado pessoal é tanto aquele que identifica claramente a pessoa, como seu RG, seu nome completo e seu CPF, quanto o dado que, quando combinado com outro, pode levar à sua identificação. Então quando você parte para um conceito assim amplo, fica muito difícil escapar da lei. Tem uma história dos meus tempos de Google que adoro contar que é a história da calota. Um sujeito parou o carro em frente a determinada casa na Inglaterra e o carro apareceu no Street View, que, como vocês sabem, borra rosto e placa de carro. Só que o carro do sujeito tinha uma calota colorida. Foi assim que a esposa desse sujeito descobriu que ele estava saindo com a melhor amiga dela [*risos*]. Ninguém, em sã consciência, diria que uma calota colorida de carro é um dado pessoal, mas, naquele contexto, ela identificou o sujeito.

IH - Mas, nesse tipo de situação, as empresas que coletam os dados podem ser responsabilizadas?
Marcel - Sim, porque na verdade coletar o dado e repassar para alguém é justamente o conceito de tratamento. O que a lei fala? Tratamento é


Hamilton Penna

> “É preciso garantir que de fato você tomou todos os cuidados adequados para não ferir a privacidade do cliente”.
>
> Carlos Augusto, do Banco Original

tudo que você pode fazer com os dados, da coleta ao descarte, incluindo o mero armazenamento. Então, quando a lei fala que tudo está englobado por essas atividades, quase tudo pode ser dado pessoal e quase tudo está no conceito de tratamento. Como a lei regula expressamente o tratamento de dados pessoais, fica claro por que todos os setores da economia estão atingidos por essa legislação. Sendo bem sincero, é inescapável. Não tem muita saída, porque copiamos esse modelo europeu.
Diante de tudo isso, vocês devem estar se perguntando: como a lei afeta o nosso dia a dia? A resposta é que, em lugar da liberdade que se tem hoje, a lei cria hipóteses taxativas que dizem: você só pode tratar dados pessoais se enquadrar esse tratamento em uma das dez hipóteses que a lei lhe autoriza. A primeira delas e a mais corriqueira é o consentimento. Você tem a autorização? O consentimento não é um consentimento aleatório, ele tem sempre três elementos: precisa ser livre, ou seja, precisa ter sido uma escolha real daquela pessoa optar por fazer aquilo; ela precisa ser informada, ou seja, você precisa dizer para quais motivos aqueles dados estão sedo coletados, serão tratados e vão ser utilizados; e você tem que demonstrar que obteve aquele consentimento, o que pode ser por um contrato formal ou qualquer outro meio demonstrável. O consentimento pode ser revogado. Quando ele é revogado, eventualmente o titular desses dados tem o direito de exigir da empresa, que esses dados sejam eliminados. Ocorre que os sistemas nunca foram preparados para ter um processo claro e fácil de eliminação de dados. Talvez colocar em um cluster separado ou talvez eventualmente montar um silo em que aquilo não é utilizável, o que é um pouco mais simples. Mas, efetivamente, eliminar para sempre é uma coisa mais delicada. Outra hipótese legal de tratamento é o cumprimento de um contrato: alguém celebrou um contrato com uma empresa e a base legal de tratamento daquele dado é o cumprimento desse contrato. Um exemplo banal: Imaginem que vocês tenham TV a cabo na casa de vocês e querem adicionar um ponto extra. Vão então ligar para a operadora pedindo para virem à sua casa colocar esse ponto extra em algum lugar. Normalmente, não irá alguém da operadora, mas um terceirizado. Esse terceirizado tem seu nome, seu endereço e sabe o que tem que fazer. Até fevereiro de 2020, esse sujeito pode pegar esses dados, montar uma base e lhe enviar cartão de Natal, e-mail marketing ou fazer o que ele quiser. Só que com a nova lei, se ele recebeu esses dados para a execução de determinado contrato, foi só para executar aquela atividade.

Ele não pode usar essa base de dados para uma finalidade diferente.

Carlos Augusto - Mas quem é responsabilizado pelo uso indevido desse dado: o terceirizado ou a empresa que foi contratada?

Marcel - Em um primeiro momento, é o terceirizado diretamente. O problema é que se a empresa cedeu o dado para ele, sem deixar claro quais eram as instruções que tinha que seguir, ela atrai para si a responsabilidade conjunta. Isso é muito importante no setor financeiro: você tem também o tratamento de dados para o cumprimento de uma obrigação legal regulatória. Então, tem lá as normas da CVM, do Conselho Monetário Nacional, tem o Bacen, portanto, você tem que reter dados, em geral, por cinco anos. A área de marketing, por exemplo, vai pensar que pelo menos por cinco anos vai poder trabalhar sobre aquela base. A lei diz que se você está se baseando no tratamento para o cumprimento de uma obrigação legal, a finalidade desse tratamento é o estritamente o cumprimento de uma obrigação legal. Se você quiser aproveitar essa base para outras finalidades, não é mais o cumprimento de obrigação legal. Nesse caso, você vai ter que se basear em outro conceito, por exemplo o do interesse legítimo.

IH - Esse conceito existe na lei europeia?

Marcel - Sim, na lei europeia existe a base legal de tratamento conhecida como interesse legítimo. O que é essa base legal? É ela que de fato permite flexibilidade, inovação e aproveitamento de dados, de uma maneira geral, para outras finalidades.

A ideia de interesse legítimo é basicamente a seguinte: uma empresa quer usar essa base, tem as informações, seja um legado, seja uma base nova, isso não faz diferença nesse momento. Não interessa se tem ou não consentimento. Todos vocês aqui, quando o GDPR entrou em vigor, em maio, devem ter recebido aquela enxurrada de e-mails, pedindo que continuassem concordando, fazendo isso ou aquilo. Às vezes não é factível você pedir para uma base de milhões de pessoas que concordem com os novos termos. O interesse legítimo serve justamente para a empresa poder olhar para os dados e dizer: qual é o meu interesse legítimo aqui, é o combate à fraude, é alguma promoção comercial, é alguma outra atividade?

Se conseguir encontrar um interesse legítimo que justifique o uso daqueles dados, ela passa para a segunda etapa. É possível mesmo tratar esses dados para chegar ao interesse legítimo, ou é possível fazer isso de outra maneira? Normalmente uma análise está atrelada à outra, e você nem começa o primeiro raciocínio se de fato não chega à conclusão de que esses dados precisam ser utilizados.

Finalmente, o terceiro teste, que é o mais importante: eu violo algum direito? Estou atrapalhando esse titular de dados ao utilizar essas informações? Dou um exemplo. Muita gente usa os wearabales, e esses aparelhos medem a atividade física regular. Vamos imaginar que uma empresa como a Nike ou a a Adidas resolva olhar para a base de pessoas que usa esse tipo de dispositivo para saber quem tem uma atividade física regular. E aí identifica 2% de superatletas, e ofereça para eles um tênis especialmente desenvolvido para supermaratonistas. Você não consentiu essa ação, mas a empresa justifica isso com base no interesse legítimo. Outro exemplo: uma parcela desses usuários não faz exercícios regularmente, só anda de carro, pratica esporte só nos finais de semana e, portanto, correm mais risco de ter um mal súbito. Com base nessas informações, uma companhia de seguros, por exemplo, pode decidir aumentar o valor do prêmio ou até se recusar a vender o seguro? Não é preciso ser jurista para entender que no primeiro exemplo provavelmente é permitido usar essa base de dados, mas no segundo exemplo muito provavelmente não é.

IH - Mas essa interpretação do interesse legítimo não é excessivamente permissiva?

Marcel - Na verdade, o que a lei exige quando você usa o interesse legítimo é que internamente você documente o raciocínio que adotou e deixe isso reservado para quando a futura autoridade de proteção de dados eventualmente resolva fiscalizar. Sem, é claro, necessariamente revelar segredos de negócio, como a fórmula de credit scoring, de análise de risco, ou o modelo preditivo do que quer que seja. Você precisa só documentar que dados estão sendo tratados; o que você levou em consideração; por que você acha que não tem um risco, etc. E qual é o problema que pode decorrer disso? Vamos imaginar que a autoridade peça para ver esse documento, analise seu tratamento de dados com base no legítimo interesse e considere que você cruzou a linha, não poderia ter feito o que fez. Aí, ela vai não só impedir você de continuar esse tratamento, exigindo que você descarte essa base, como eventualmente vai impor penalidades. Sem querer fazer terrorismo jurídico, mas a lei prevê até R$ 50 milhões por infração.

IH - Ou até 2% do faturamento, não é isso?

Marcel - É isso: 2% do faturamento, até R$ 50 milhões por infração. É claro que a autoridade vai olhar para vários fatores atenuantes: você tentou cumprir a lei? Você tem um programa interno de governança? Tem um mapeamento do seu fluxo de dados?

IH - O combate à fraude é considerado um interesse legítimo?

Marcel - A maioria dos meus colegas advogados quer a listinha pronta do que pode ser considerado interesse legítimo. Já a maioria dos meus amigos engenheiros fala que não tem que ter listinha nenhuma. Mas a gente quer a gente quer flexibilidade! Portanto, não tem listinha nenhuma, existem só precedentes na lei europeia que vão servir de guia para o modelo brasileiro. Respondendo à sua pergunta, tradicionalmente

o combate à fraude é um exemplo clássico de interesse legítimo. Outro exemplo clássico de interesse legítimo é o da obtenção de dados de um devedor, por parte do credor. Você vai precisar alimentar e enriquecer a sua base, para ter mais informações sobre o devedor e eventualmente você vai justificar isso no interesse legítimo. Trata-se de uma base de proteção do crédito. A questão é que ninguém sabe ainda qual é a extensão desse conceito de proteção do crédito.

Rogério - Isso é uma ocorrência que tornou mais complexa a aprovação do cadastro positivo, na medida em que ele recolhe dados de comportamento, de uso.

Marcel - Particularmente como acadêmico – e agora não estou falando em nome do Pinheiro Neto –, eu até entendo que a lei como está dá muita margem para se ter alterações de scoring, de cadastro positivo, mesmo sem a própria lei do cadastro positivo. Eu acho que esse inciso da lei, que colocou que proteção do crédito autoriza o tratamento, permitiria isso. Como o Brasil tem toda uma tradição contrária em relação a isso, é até preferível mesmo que haja a legislação para evitar essa discussão.

IH - Vamos ver como o Bradesco se prepara para a nova lei, diante desse quadro que o Marcel descreveu.

Rogério - Entre as áreas sob minha responsabilidade há duas aqui diretamente envolvidas, que são tecnologia e gestão de dados. Considerando esse quadro brilhantemente descrito pelo Marcel, no mercado financeiro como um todo, a questão da proteção de dados, da confidencialidade e segurança sempre foi algo muito importante para as organizações, especialmente em função das regulamentações que já existem. Nesse aspecto, nós estamos tranquilos, o mercado não vai ter muito que evoluir. Acredito que a questão toda está no

Hamilton Penna

> “Não é que a lei vai inviabilizar negócios, mas ela vai tornar mais complexa a justificativa de como são feitos esses negócios”.
>
> Marcel, do Pinheiro Neto

tratamento. O que o Bradesco está buscando de forma prática? Nós temos bilhões de dados, então a primeira fase é o diagnóstico desses dados. Temos que classificar esses dados, porque, se conseguirmos classificar corretamente dados como proteção ao crédito, vamos ter o direito de usar esse dado. Quanto ao cumprimento de ação legal, em prevenção à lavagem de dinheiro, já existe uma lei que nos obriga a coletar e tratar determinados dados, independente da vontade do cliente. Esse dado eu tenho que tratar porque se o Banco Central faz uma fiscalização e eu não tenho, sou enquadrado em outros ilícitos. A última hipótese que a gente quer tratar é a questão do consentimento. O consentimento para nós tem que ser a exceção, porque uma vez que eu peço o consentimento, decorre daí uma série de implicações que impactam a tecnologia, porque isso dá o direito de a pessoa vir até o banco e falar assim: “Olha, sabe aquele dado que deixei você capturar? Pois agora não quero mais”. E eu vou ter que excluir. Só que vou ter que excluir não só no Bradesco, mas em todas as empresas coligadas, parceiras e fornecedoras. Como eu vou poder garantir que todos excluíram aqueles dados?

Waldir - Essa é uma dificuldade enorme. Como birô, vou responder: dados do Bradesco, da Fidelity, por exemplo, entram na Boa Vista para a concessão de crédito. Essa transposição de informação, na hora em que eles cedem a informação e eu faço o tratamento, por exemplo, nas negativações, como é que vou trabalhar com isso? Me parece que a lei não é clara quanto à forma pela qual nós vamos trabalhar com isso. Dentro da Boa Vista, por enquanto estamos trabalhando com o foco no departamento jurídico. Mas a preocupação grande é, por exemplo, como eu trabalho com essas informações quando tenho que fazer uma baixa? Por exemplo: dou informação para o meu cliente de uma série de pessoas que estão devedoras na carteira dele, mas se eu tiver que baixar aquela informação, como baixo do outro lado?

Carlos Augusto - Esse também é o ponto mais relevante para nós, essa fase de diagnóstico e análise. Para cada empresa do grupo, vamos ter que ter esse tratamento. Nós decidimos que, antes de mais nada, precisamos ter uma consultoria jurídica, porque a questão aqui é a base legal. Como ela tem muita interpretação, você tem que procurar classificar da melhor maneira possível. A gente entende que, nessa jornada de diagnóstico, uma consultoria com muito conhecimento da lei pode nos auxiliar nessa classificação de dados, mais do que em

tecnologia. Em tecnologia, a dificuldade vai ser na hora em que tivermos que ter o consentimento. O meu trabalho no banco nestes meses tem sido o de mostrar que o problema não está em tecnologia, o de tecnologia é até menor, não que seja pequeno pois é extremamente complexo. Ele afeta os negócios como um todo. Hoje todo mundo é digital. A quantidade de parceiros que temos, de dados que a gente coleta, de vários birôs, de vários prestadores de serviços, isso tudo é um monte de informações e não necessariamente essas informações já estão claramente mapeadas para utilização. Só para citar um exemplo: se o cliente está operando com você através do mobile, é possível coletar um monte de dados lá. Muitas vezes eu coleto, mas não sei ainda qual é a oportunidade de negócio que aquilo vai gerar. E eu não estou pedindo consentimento ao cliente. Outro exemplo: eu compro dados de dezenas de provedores, que me confirmam informação e me fornecem dados para eu validar alguma decisão. Eu não sei como alguns desses provedores obtêm essa informação. Na verdade, sob o âmbito da nova legislação, posso estar sendo conivente com uma prática totalmente ilícita. Além disso os bancos, de maneira geral, não vendem dados, mas a gente compartilha dados, faz promoções, campanhas, ofertas cruzadas com vários parceiros também. Tem vários prestadores de serviços que são fundamentais para concluir a entrega de um serviço, fazer uma manutenção, suporte técnico, etc. Então, o espectro que precisa ser mapeado só na coleta da informação – não estou nem falando ainda do armazenamento e do tratamento – já é enorme, já que é preciso garantir que de fato você tomou todos os cuidados adequados para não ferir a privacidade do cliente. Trata-se de uma frente enorme, que afeta o modelo de negócio.

IH – A figura que me veio à cabeça, quando o Carlos Augusto fala das empresas que coletam os dados sem saber exatamente se houve consentimento, é a do receptador no Código Penal. Perante a lei, todos são obrigados a saber que estão comprando uma mercadoria roubada. Isso me leva a perguntar sobre a responsabilização criminal. Existe o risco de o responsável pelo uso da informação ser responsabilizado criminalmente?

Marcel – Claro, diretamente. Uma coisa que acho que vale a pena destacar é que se trata de uma mudança de paradigma muito forte. Sempre houve esse conceito de que se se coletam dados públicos, dados publicamente disponíveis, mas na verdade a lei acaba com essa lógica, no sentido de que, mesmo que o dado esteja público, não deixa de ser um dado pessoal. Certa vez, alguém me perguntou: "Mas se a Lei de Acesso à Informação nos obriga a divulgar, por exemplo, o salário de funcionário público, como eu posso ser responsabilizado se eu fizer isso". Minha resposta foi que o fundamento legal vai ser o cumprimento de uma obrigação de uma lei que exige que você faça isso. Qual é a grande diferença? Vamos imaginar que uma agência de marketing quer coletar dados de funcionários públicos que ganham acima de R$ 20 mil, e consulta essas bases todas. O meu fundamento legal não tem nada a ver com o que autorizou o governo a divulgar aqueles dados. Portanto, mesmo quando você tenha a base legal justificada, a lei traz uma série de princípios sobre como você pode tratar esses dados. Um deles, por exemplo, é o princípio da minimização, de acordo com o qual você não deve tratar mais dados do que aqueles que são necessários para você alcançar uma finalidade. Um exemplo caricato: me convidaram para dar uma aula em uma universidade e eu precisei preencher aquele cadastro padrão. Alguém claramente copiou esse cadastro de algum lugar. Entre os dados que pediam estava o meu tipo sanguíneo. Eu pensei: caramba, essa plateia não deve ser muito amistosa... [*risos*]

Hamilton Penna

> "Quando se fala simplesmente em descartar do dado, o que isso quer dizer? Que o dado vai deixar de existir? Mas e se a regulamentação exige que o dado seja armazenado por cinco anos?"
>
> André, da Braskem

Em relação ao que o Carlos Augusto falou, de fato hoje toda lógica de Business Intelligence e Big Data passa um pouco por isso: vamos pegar as informações e depois a gente vê o que faz com elas. Na verdade, a lei, em tese, não permite isso, pois exige que exista uma finalidade específica para o tratamento que você dá ao dado. Mesmo quando você usa o interesse legítimo, ele tem

que ser baseado em uma situação concreta e não em uma situação hipotética futura. Aí você então precisa encontrar saídas criativas para não eliminar esses dados e para poder utilizar essas informações. Uma delas, que a gente já tem visto, é tentar justificar que existem situações que demandam o tratamento contínuo, ou seja, para alcançar determinada finalidade, você não pode nunca descartar certos dados. Por exemplo, vamos imaginar, dentro do exemplo citado pelo Rogério, do cenário em que o cliente pede para você eliminar determinado dado. Faz sentido, na relação direta dele com o banco. Mas e a Inteligência que foi gerada a partir do dado dele para fazer parte de um modelo preditivo que ajuda em inúmeras outras coisas? Você vai eliminar isso também? Eu entendo que não, porque você gerou uma inteligência em cima desse dado. De toda forma, você vai ter que documentar e justificar, pois isso sempre estará sujeito a questionamentos. Então, até para tranquilizar a todos aqui, não é que a lei vai inviabilizar negócios, mas ela vai tornar mais complexa a justificativa de como são feitos esses negócios.

IH - A lei introduz nesse cenário a figura do Data Protection Officer. Qual é o papel desse sujeito?
Marcel - De fato, a lei cria a figura do DPO, que no jargão menos chique em português é o encarregado [*risos*]. Na verdade, é a pessoa física, um funcionário ou alguém que pode ser terceirizado, que tem que ser indicado pela empresa e cujo papel é o de dialogar com a Autoridade de Proteção de Dados e fazer a interface com os usuários finais, com quem de fato é o titular daqueles dados. E notem que isso existe mesmo em um cenário em que uma empresa não tenha relação direta com o consumidor.
Enfim, a figura do DPO no Direito brasileiro é muito limitada, e não está claro se vai haver ou não a responsabilidade. Não tem nada na lei que diga que você pode ser responsabilizado criminalmente, mas aí entra um pouco naquelas questões de gestão, de mandato, de quanto essa pessoa é estatutária ou não é, então pode ser que isso aconteça, sim, eventualmente, dependendo das práticas.
Rogério - Me parece que essa pessoa vai ter que ter independência com relação à hierarquia e tem autoridade para tomar decisões nessa área.
Marcel - Se eu fosse a autoridade, uma coisa que sugeriria, principalmente para as pequenas e médias empresas, seria ter, por exemplo, representações de associações de classe com um encarregado que serviria para aquele setor de uma maneira geral. Imaginem, por exemplo, a associação dos bares e restaurantes: em vez de cada bar ou restaurante ter um encarregado, haveria uma pessoa da associação que faria esse papel. O modelo europeu foi um pouco mais inteligente, pois empresas com menos de 250 empregados não precisam ter um encarregado. Mas isso a autoridade teria que regulamentar.
André - As pessoas tendem a achar que têm que fazer o armazenamento, mas me parece que falta uma composição com a área jurídica. Quando surgiu o tema do GDPR, a primeira coisa que meio à cabeça foi que se trata acima de tudo de uma questão de segurança da informação. Como estou muito no front, recebo fornecedores e pessoas que vêm para ajudar, mas às vezes me sinto desamparado, porque o fornecedor ali está integrando apenas a parte do produto que ele consegue atender. E muitas vezes você tem a questão tecnológica, que não está implicitamente relacionada com a área de negócio, nem com a área jurídica. E você precisa colocar todo mundo na mesa para entender o impacto que isso vai causar. Quando se fala simplesmente em descartar do dado, o que isso quer dizer? Que o dado vai deixar de existir? Mas e se a regulamentação exige que o dado seja armazenado por cinco anos? Em algum momento o cliente fala que não vai mais operar com você. Só que esse dado já está gravado, nos últimos três ou quatro balanços ele fez parte da composição. Então como descaracterizar algo que já foi estruturado com aquela informação? Essa é uma dificuldade que eu ainda não sei como vamos superar. O GDPR já foi implementado lá fora, só que ainda não se vê penalidade sendo aplicada, porque o próprio mercado está aprendendo como vai ser o modus operandi disso.
Marcel - Vamos deixar claro que, toda vez que você tem uma obrigação legal ou outros cenários que justificam a manutenção desse dado, você pode rejeitar essa requisição de apagar essa informação. Eu, que vim do setor de Internet, posso dizer que é exatamente esse raciocínio que a maioria das indústrias adota, no sentido de que preferem justificar e documentar toda aquela lógica de interesse legítimo, para não ter que atender a essa parte da eliminação. O próprio Google faz isso. Por exemplo: quem é usuário de G-mail sabe que na ponta a base legal é o consentimento porque, teoricamente, todo mundo lê os termos e condições e concordou [*risos*]. É engraçado porque é quase uma fantasia, porque o consentimento é dado, mas a gente sabe que as pessoas de fato não leram ou não entenderam os termos daquilo que consentiram.
Na Europa existem alguns estudos de consultorias, antes mesmo de o GDPR entrar em vigor, que já mostravam uma estatística interessante: independentemente da indústria, mais de 80% das bases legais de tratamento de dados na Europa eram de interesse legítimo. Consentimento era uma parcela diminuta. Às vezes, é preferível que o consentimento seja limitado a certos dados que são essenciais para aquilo funcionar e o resto da operação é baseado em outra hipótese legal, como

o interesse legítimo. Agora, nesse ponto a lei é implacável, porque coloca na empresa o ônus de exigir que toda a cadeia elimine a informação.

Carlos Augusto - Qualquer plataforma que se acesse hoje tem uma série de termos e condições, que muitas vezes estão escondidos, em linguagem técnica ou são extremamente longos justamente para poder cobrir todas as nuances. Isso torna muito difícil para um leigo, um cidadão comum, ter completo entendimento e de fato saber o que ele está autorizando. Nesse sentido, a legislação geralmente vem para impedir alguns abusos, ainda que muitas vezes a dose seja exagerada. Por isso é que os fornecedores globais, especialmente os europeus, estão procurando simplificar um pouco, usando uma linguagem que permita às pessoas saber o que ela está consentindo.

Marcel - Hoje têm sido adotadas três melhores práticas. Como as autorizações genéricas não são válidas, é preciso dar exemplos. Isso causou uma primeira ironia: os termos e condições da política de privacidade ficaram ainda mais longos. São coisas do tipo: "Combinaremos o dado x com o dado y e faremos tal coisa". O que apareceu então como melhor prática? É ter os termos e condições escritos em linguagem jurídica, porque quem vai ler aquilo é a autoridade, que é quem vai fiscaliza. Mas tem um terceiro documento, que explica com clareza as melhores práticas adotadas. A maioria das empresas começou a ter uma abordagem até lúdico nesse ponto. Por exemplo, quando entrou em vigor o GDPR, o Google soltou um post enorme explicando o que tinha mudado, mas ilustrado com vídeos, que é a linguagem preferida dos jovens. Mas não vamos nos iludir: mesmo assim, o consentimento como base legal acaba tendo essas fragilidades e é por isso que há que se ter cautela.

Curt - Nós, como organização, temos uma preocupação gigantesca com a questão da lei. Os bancos e as seguradoras sempre foram muito regulamentados no quesito dados. O Banco Central estabelece que dados a gente precisa deixar disponíveis. A ANS, nem se fala. Então, nas questões de seguro-saúde, há várias discussões por muito tempo de prontuários de pacientes que a gente nunca conseguiu de fato viabilizar. Talvez o cadastro positivo seja o primeiro em que a gente começa a ver que sai do outro lado, com um compartilhamento de dados entre as organizações, quebrando um pouco dessa barreira. Nós estamos num segmento acostumado com essa proteção. Além disso, a sociedade já não vê com bons olhos esse bombardeio de marketing, com inúmeras ofertas. Por outro lado, isso traz a sociedade para um outro patamar. Acho que aqui cabe uma analogia com o que vivemos há alguns anos com a Sarbannes-Oxley. Neste primeiro momento, nós, como indústria, estamos vivendo sob certo terrorismo jurídico: está todo mundo assustado com as inúmeras interpretações dos impactos da lei na vida prática. Acho que até a lei entrar em vigor e ser regulamentada, já teremos digerido esses conceitos. As mesmas consultorias que nos venderam ajuda para implementar a Sarbannes-Oxley, cinco ou seis anos depois já estavam nos vendendo a simplificação da Sarbannes-Oxley, porque de fato tínhamos criado controles, alguns até exagerados. Na verdade, eu vejo com muito bons olhos a vinda de uma regulamentação para isso e acho que de fato vai fazer a diferença para nós como consumidores. Agora, os detalhes da implantação é que vão ser decisivos. Também temos usado muito a Febraban como um catalisador desse tema para nós, da indústria financeira, porque a troca de informações é fundamental. No fundo, nós temos também o compromisso de fazer com que o sistema funcione, e que a gente não sofra com falta de informação legítima para operar o negócio.

Marcel - A analogia com a Sarbannes é interessante. É dolorido no começo, tem esse trabalho todo de estar em conformidade com a legislação, mas é positivo a médio prazo, até como vantagem competitiva. A autoridade vai olhar para as grandes empresas e descobrir quem está em conformidade e quem não está. É claro que, pelo porte da sua estrutura inicial, certamente a autoridade não vai ter braços para fiscalizar pequenas e médias empresas. Outro ponto é que, de fato, há um cenário em que a defesa do interesse legítimo pode ser feita tanto em nome da própria empresa quanto de um terceiro. Nas interpretações europeias, esse terceiro pode ser a própria sociedade, considerada de forma ampla.

Hamilton Penna

"Infraestrutura como "Até a lei entrar em vigor e ser regulamentada, já teremos digerido todos esses conceitos".

Curt, da Bradesco Seguros

Então, essa lógica de defender a higidez do sistema é uma tese que eventualmente dá para ser construída. Em um primeiro momento – e aqui estou sendo bastante otimista –, vamos lembrar que todas essas interpretações europeias são conservadoras, porque é do Direito europeu. Dependendo de quem for a autoridade aqui, ou as pessoas que a compuserem, poderá haver interpretações um pouco mais flexíveis. Mas também pode ser o contrário, pode haver coisas mais restritivas. Mesmo na Europa, há modelos muito diferentes entre si. Por exemplo, a autoridade de que mais gosto, de longe, é a do Reino Unido, a Information Comission Officer, que é vista como de vanguarda, preocupada com a inovação. De outro lado, há a autoridade espanhola, que é vista como mais preocupada com o aspecto arrecadatório da lei. Até porque, no caso do modelo espanhol, o orçamento da autoridade vem das próprias multas que ela arrecada. Aí é difícil dizer que não tem um certo conflito de interesse.

IH – E de onde virá o orçamento da autoridade brasileira?

Marcel – Ainda não se sabe, porque todos os dispositivos sobre a autoridade foram vetados, por um motivo muito simples: como ela foi criada no âmbito da tramitação na Câmara dos Deputados, existia um risco concreto e real. A primeira empresa que fosse multada contrataria um advogado para algar que ela foi criada de maneira inconstitucional, e portanto a multa não é válida. Para evitar que isso acontecesse, houve o veto. De toda forma, a maneira como a autoridade estava planejada previa que seriam três pessoas dirigindo a entidade, estas sim com poder de decisão, auxiliadas por um conselho de 23, sendo 11 representantes do governo, quatro do setor privado, quatro da sociedade civil e quatro do setor acadêmico. Seria mais uma autarquia. Essa autoridade seria muito mais um Cade do que propriamente uma agência. É muito mais um corpo técnico especializado nesse assunto e é minha esperança que tenha noção da dimensão da responsabilidade que tem.

Hamilton Penna

> “Uma mudança de cultura e de processos dentro da empresa depende das pessoas, e aí provavelmente vamos encontrar algumas barreiras, que não serão tecnológicas”.
>
> Cesar, da Fidelity

IH – Cesar, a Fidelity tem acompanhado o passo do grupo Bradesco nesse tema?

Cesar – Na Fidelity, a gente também acaba sendo meio e não fim, então muito do que for definido nos nossos clientes e nossos parceiros vai acabar acontecendo dentro da Fidelity. Por isso, o momento é mais de estudo, de análise do departamento jurídico junto com o nosso pessoal de compliance. Eu sou um dos integrantes desse comitê. A gente faz sempre uma analogia com algumas das nossas certificações. Nós temos o PCI, que hoje é uma certificação extremamente importante no meio de pagamento. Sem essa certificação, você praticamente não pode trabalhar com bandeiras como Visa, Mastercard e American Express. Então, na parte de proteção, de guarda, de armazenagem, transmissão e recepção de dados, a gente se sente bastante confortável. Uma das nossas dúvidas é se vão ser feitas auditorias, análises, como é que vamos prestar conta. Esse vai ser um processo mais estruturado, como o que a gente passa nas certificações? Como esse processo se inicia? Quais são as evidências que você tem que coletar ao longo desse processo? Temos trabalhado não como uma visão de TI puramente: TI vai ser mais uma área que vai ser facilitadora no final. É o processo em si que realmente nos preocupa bastante, porque ele muda muito a cultura da empresa e a forma de a empresa trabalhar. Nós dependemos disso, porque várias linhas de negócio estão ligadas ao interesse legítimo. Por exemplo, nós temos cobrança, temos uma área enorme de prevenção a fraudes que controla todos os dados transacionais dos cartões e que os cruza com dados demográficos. Como eu disse, há uma regulação muito forte sobre a parte transacional. O prazo também é uma preocupação, porque uma mudança de cultura e de processos dentro da empresa depende das pessoas, e aí provavelmente vamos encontrar algumas barreiras que não serão tecnológicas, mas sim mais ligadas aos processos.

Marcel – A proteção de dados é um tema do negócio. Na Europa, as empresas que de fato conseguiram ter um grau alto de compliance foram aquelas que levaram isso para o nível de board. Quando o GDPR foi anunciado, foi uma coisa impressionante, pois no dia 1 em que a lei foi aprovada e ia entrar em vigor só dali a dois anos, já havia no Google todo um plano de mapeamento de quais produtos eram prioritários, quais iriam entrar primeiro em compliance, e é óbvio que primeiro foi o que gera dinheiro, que era a parte de publicidade. Como vi essa fórmula dar certo não só No Google mas em várias outras empresas, este seria o conselho que eu daria: não assumir só para

si, nem jogar só para o jurídico, e entender que realmente é uma coisa que o seu board tem que estar completamente envolvido.

Cesar - E a gestão de dados está ficando cada vez mais importante.

Marcel - Exato.

Cesar - Você tem que começar a agir de uma forma muito mais eficaz do que fazia antes. Então, são necessárias novas estruturas, novos processos e a própria presença do DPO. E uma preocupação em relação às nossas adaptações é que várias informações irão permear os nossos clientes para dentro dos nossos sistemas. Então como é que a processadora vai estar em sintonia com o que está acontecendo do lado do cliente? Essa é uma das informações que a gente precisa estabelecer rapidamente, criar os processos. Depois trabalhar também sobre a questão da exclusão dos dados, que é uma parte que preocupa bastante devido à preparação dos sistemas para isso.

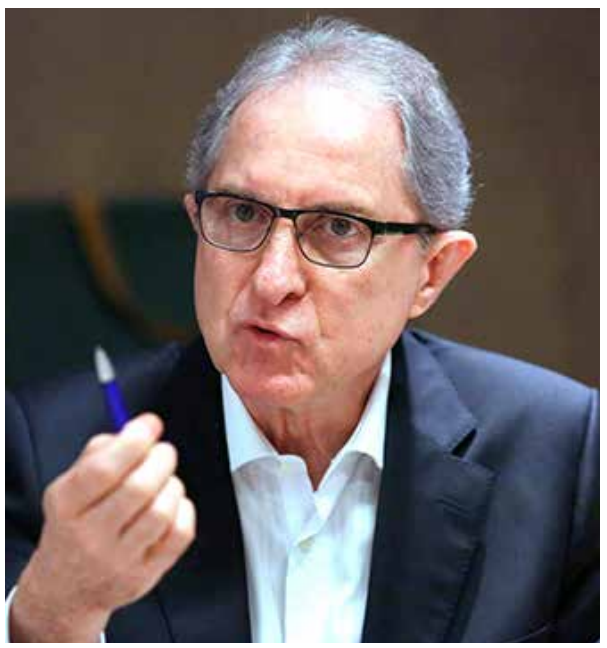
IH - Igohr, a Vivo é uma operadora e em tese não tem responsabilidade sobre os dados que são coletados por terceiros via dispositivos móveis. Mas vocês também coletam dados dos dispositivos móveis que vocês operam. Uma outra questão para você, mas que também serve para todo mundo, é que, pela lei, os clientes vão ter a possibilidade de editar os próprios cadastros dentro das empresas. Certo, Marcel?

Marcel - Há uma série de direitos conhecida como direitos de retificação, acesso, oposição.

IH - A Vivo está preparada para isso?

Igohr - Ainda estamos em uma fase inicial. A gente tem o comitê montado e estamos fazendo a análise diagnóstica para poder entender o tamanho do impacto. Porque se a gente vai para um lado paranoico, vai custar dezenas de milhões de reais para adequar os sistemas e garantir que tudo se adapte à lei. Por exemplo, eu tenho sete sistemas de billing de faturamento. Se eu tenho que pagar a informação, como vou fazer? É uma quantidade tal de sistemas na empresa, são mais de 600, então a gente precisa entender fazer um bom diagnóstico. E mesmo compartilhando um pouco da experiência que está sendo adotada na Telefónica da Europa, não são todas as diretrizes da lei que foram aplicadas. Mas um tema que me deixa muito preocupado é o fato de que o mundo das operadoras de telecom, como ele é, vai deixar de existir: cada vez, mais elas terão que se reinventar sobre como ofertar e manter o nível. Hoje, informações que não eram usadas no passado começaram a ser usadas. Hoje, se você vai a um show alguém pode lhe oferecer um produto relacionado àquele show. Hoje, isso não é considerado um dado do cliente. Hoje eu consigo saber quantas vezes você acessa os aplicativos do Bradesco e do Itaú. A gente consegue ter informação sobre praticamente toda a vida do cliente. Quando começarmos a usar isso em prol do negócio, como isso vai ser encarado? Vai ser tratado sob demanda ou já tem que partir do princípio de que eu tenho que ter a autorização do cliente para poder trabalhar com alguma informação que hoje não é considerada um dado livre?

Hamilton Penna



“A lei é uma iniciativa correta, de nos proteger como cidadãos, e que certamente vai exigir uma importante mudança cultural”.

Célio, da Prodesp

Marcel - Você pode trabalhar com múltiplos cenários. Pode pedir o consentimento nesse caso, quando o cliente, por exemplo, assina o contrato padrão. Você vai deixar claro que, por exemplo, ele consente com certas atividades e certos hábitos, relativos à utilização do telefone e da própria linha, dos dados, mas aí corre os riscos do consentimento que a gente falou. Se o cliente revoga o consentimento, você tem que descartar esse dado. Você também pode se basear no interesse legítimo e dizer: minha intenção é melhorar o meu produto, o meu serviço. Na verdade, tudo depende das finalidades para as quais você vai usar essa informação. Se é para uma questão comercial, você sempre deverá perguntar: será que isso vai frustrar a expectativa desse titular de dados?

André - Quem vai ser o responsável por conferir se a lei está sendo ou não cumprida? Porque hoje temos que atender às auditorias externas, todas elas independentes, e isso é um mindset já estabelecido. Quem teria essa abordagem legal para fazer essa verificação se você está compliant? E a quem eu poderia recorrer para me garantir, antes de esse sujeito chegar?

Marcel - Quem vai definir tudo isso é a autoridade, que ainda não foi criada. A autoridade pode sim fazer auditoria. A lei exige que toda operação de tratamento de dados seja documentada. Não quer dizer que cada vez que alguém se cadastra no seu sistema você precise ter um registro. Você precisa ter um raciocínio em que documenta, com uma descrição de como acontece o processo interno. Feito isso, você tem que aguardar alguém questionar e nesse caso é a autoridade. Agora, a autoridade não vai fazer auditoria a todo momento, não há um intervencionismo tão grande. Como você

evita isso? Ainda não existe esse mercado no Brasil, mas provavelmente ele vai existir: é o mercado das certificadoras. É exatamente a mesma lógica de Sarbannes-Oxley e a mesma lógica de compliance. Vão aparecer empresas que teoricamente serão homologadas ou aprovadas por essa autoridade.

Carlos Augusto - Na prática, todo mundo aqui tem área de compliance e eu imagino que as áreas de compliance estejam analisando o assunto e vão remeter para as auditorias que de alguma maneira vão verificar essas práticas. O quanto elas estão capacitadas e qualificadas deve ser uma preocupação delas, porque evidentemente isso vai ser incluído nos planos das nossas auditorias internas e eventualmente externas também, porque essa autoridade não vai ter capacidade de olhar para tudo, para o Brasil do tamanho que é e no volume que é. O que a gente espera é que essa autoridade exista para dar algumas regras, para criar uma jurisprudência, no sentido de dirimir algumas dúvidas e orientar alguns padrões e o limite do interesse legítimo e etc. Mas na prática isso tem que ser resolvido dentro da governança da própria empresa

IH - Célio a estrutura de governança e de compliance da Prodesp, uma empresa pública, está em condições de se adequar à nova lei?

Célio - Em 2016, quando o governo editou e sancionou a lei das estatais, a 13.303, na época deu dois anos para as empresas se adaptarem. Venceu em 31 de junho de 2018. Na época, nós criamos um grupo para adaptar a empresa a todas as novas exigências da 13.303. Qual é o princípio da 13.303? É melhorar a governança das empresas estatais, tipo Sarbannes-Oxley. Então fizemos um planejamento com umas 20 grandes ações e a gente executou todas, porque era tudo basicamente voltado para dentro. Assim, a Prodesp evoluiu muito na sua governança. Criamos inclusive uma área de conformidade, gestão de risco, controle interno, etc.

Em relação à lei de proteção de dados, é uma iniciativa correta, de nos proteger como cidadãos, e que certamente vai exigir uma importante mudança cultural. Só acho que 18 meses é um prazo muito curto, em comparação com os 24 meses da 13.303, a lei das estatais, que é só voltada para o setor interno. A Prodesp, como vocês sabem, é uma integradora e processadora de sistemas principalmente para o governo do estado de São Paulo. Mas quase 20% do nosso faturamento não vem do governo do estado de São Paulo, mas de outros milhares de clientes. A gente processa, por exemplo, automação hospitalar. Nós temos sistemas com muitas informações de cidadãos, inclusive prontuários eletrônicos, que são de alta criticidade. Temos muitas informações das polícias. Por isso, nós criamos um grupo de trabalho com o mesmo espírito da lei 13.303, mas já chegamos à conclusão de que não vai dar para fazer só um plano de 20 grandes ações, porque a coisa é muito mais ampla e envolve essa mudança cultural. E nós temos um papel importantíssimo, que é o de disseminar essa cultura nas secretarias e demais órgãos do governo. E para isso, temos que começar executando coisas mais óbvias, como olhar o nosso código de conduta, treinar as pessoas, contratar consultorias, mudar os nossos contratos. E no nosso caso, tem mais um aspecto relevante: quem vai pagar a conta dessa transformação? Vamos ter que mexer em inúmeros sistemas. Se bem que a lei tem dispositivos específicos para governo, como no caso da segurança pública. Tem algumas salvaguardas.

Marcel - Na verdade, a lei tem um dispositivo muito importante para o setor público: ela autoriza, como uma das bases legais de tratamento, a execução de políticas públicas que sejam respaldadas por lei, contratos, normas, etc. Então, de certa maneira o setor governamental tem uma ampla possibilidade de tratar dados com base no argumento de execução de política pública, que é quase como funcionaria o legítimo interesse para o setor privado. Só que todos os princípios e todas as finalidades da legislação têm que ser observados da mesma maneira. Acho que esse trabalho de educação vai ser enorme. Qual vai ser a tentação do setor público? Jogar tudo na ideia de que o tratamento é baseado na execução de políticas públicas. Essa é uma crítica que os críticos da Europa sempre fizeram: mas o governo vai ter que se automultar? O governo vai colocar R$ 50 milhões de multa para a Prodesp?

IH - Daniel, pelo fato de ter ações em bolsa, a Sabesp está mais preparada para a implementação da lei?

Daniel - A Sabesp desenvolve um trabalho intenso de governança, por ser uma empresa regulada e ter ações nas Bolsas de Nova York e de São Paulo.

Hamilton Penna

“A gente consegue ter informação sobre praticamente toda a vida do cliente. Quando começarmos a usar isso em prol do negócio, como isso vai ser encarado?”

Igohr, da Vivo

Nós passamos por todos os modelos possíveis de compliance. Essa discussão começou na área de TI da Sabesp e já estamos tomando algumas iniciativas. Em uma empresa pública, é preciso respeitar uma quantidade enorme de leis e regulamentações, mas a questão é que a lei foi criada para conter abusos, como o uso descontrolado e interessado dos dados. Mas, como nós não compartilhamos dados, a primeira reação do corpo executivo foi: "Por que precisamos nos adequar a essa lei?" Na verdade, um ponto muito crítico para nós, que somos empresa pública, é a Lei de Acesso à Informação, que demanda interesse específico e muitas vezes com interesse político em informações estratégicas da empresa. Pelo menos como custodiante dos dados – e o dado da Sabesp é muito bem definido como sendo do negócio –, a Sabesp evoluiu para ter a governança de dados, que fica estrategicamente em outra área. Então isso está sendo um trabalho recente e muito alinhado à área de risco do negócio. Temos um plano de ação a curto prazo. Recentemente, a Sabesp fez uma licitação para contratar uma empresa especializada em direito digital para nos orientar. A particularidade da Sabesp é a questão da distribuição das informações com terceiros, desde os leituristas aos escritórios de cobrança. Os dados dos nossos clientes estão lá. Já o dado do empregado, como o Célio muito bem disse, é público. Esse é o ônus de se trabalhar em uma empresa pública.

Qual é o ponto na questão de segurança da informação em um mundo de tecnologia? É aumentar o interesse pela base de dados. Se eu não compartilho, se reservo ou se estou em tudo aderente à lei, certamente vai haver um interesse maior por essa base. De meu ponto de vista, a lei acaba incentivando esse mercado negro. A Sabesp tem 28 milhões de pessoas atendidas, temos 9 milhões de clientes cadastrados.

IH – Vocês têm ideia de como devem lidar com o legado de dados anteriores à lei?

Marcel – No finalzinho da lei, tem um dispositivo que fala que a autoridade é que vai fixar as regras para a adequação das bases antigas à nova lei. Quando teve o GDPR entrando em vigor na Europa, todo mundo pediu o consentimento de novo. Era preciso fazer isso? Não. As autoridades europeias inclusive falaram: se você tem a prova do consentimento, não é porque o GDPR entrou em vigor que você precisa pedir um novo consentimento. A prova do consentimento anterior basta. O que as empresas constataram? "Eu lá tenho essa prova em algum lugar? Não tenho como provar isso, vou ter que fazer isso do zero". Aqui é mais ou menos a mesma coisa: não adianta imaginar que a lei só se aplica para as bases novas criadas a partir de fevereiro. Não tem jeito. A base que já existe está sujeita à lei também. Se a autoridade nacional for criada nesse meio tempo, talvez dê algumas diretrizes de como isso vai ser implementado. Vamos pensar no pior cenário: a autoridade não é criada, não existem diretrizes, não tem orientação nenhuma de mercado. O que vocês devem fazer? Devem olhar de novo para esse mapeamento das bases legais, e entender onde cada um se enquadra. Vão precisar realmente ter um novo momento de consentimento e disparar mensagens para milhões de clientes, para ter certeza de quem vai consentir e quem não vai. E como é que se gerencia tudo isso? Aí sim, do ponto de vista de TI, você tem que ter um sistema que saiba gerenciar isso. Acho que a grande complexidade é essa. Por isso que de certo modo todo mundo vai tentar recorrer ao interesse legítimo

Igohr – Na Espanha, para cada acesso que você faz no Wi-Fi, público ou corporativo, aparece um documento para você aprovar. Por quê? Porque a cada acesso você tem um IP dinâmico e então você é um cliente novo.

Rogério – Não acredito que vamos ter mais dificuldades com o legado do que com os sistemas novos. Do meu ponto de vista, mesmo o nosso banco digital Next já é legado para o conceito da lei. Quer dizer, ele não pressupôs uma construção baseada nessas características de que estamos falando aqui. No fundo, a mudança estrutural é da indústria inteira. Na minha opinião, o trabalho é quase igual para o novo quanto para o legado, porque nada foi construído com essa premissa. O seu ponto é importante porque se juridicamente não acharmos uma fórmula de usar como interesse legítimo e o consentimento for a bola da vez, nós vamos ter que mudar os processos de coleta e de manutenção dos dados. A complexidade maior não está no armazenamento e na proteção do dado ou em evitar o vazamento do dado**,** mas está no negócio, na maneira como o negócio está estruturado, se tenho justificativa para ele.

Marcel – Tem um elemento adicional, que tem a ver diretamente com TI, que é o seguinte: a lei também fala que é um direito do titular de dados, independentemente se é público, privado ou de qual ramo de negócio, questionar e pedir

Hamilton Penna

"Um ponto muito crítico para nós, que somos empresa pública, é a Lei de Acesso à Informação, que demanda interesse específico".

Daniel, da Sabesp

a revisão manualmente, por uma pessoa física, de decisões tomadas de maneira automatizada. Isso é muito importante porque estamos falando de cenários como, por exemplo, o da pessoa que teve um crédito automaticamente negado porque os algoritmos e os modelos decidiram. Ele tem o direito de exigir que alguém explique para ele os motivos, pessoalmente inclusive, da recusa. Eu desconheço, do ponto de vista de sistemas, se isso é algo que está no radar de vocês.

Carlos Augusto - Tem o direito ao esquecimento também, que é totalmente TI, de se conseguir apagar os dados de todas as bases. Isso é altamente complexo.

IH - O Waldir pode falar, porque isso pode acontecer também com o cadastro positivo.

Waldir - Uma das coisas que me preocupa muito, porque temos um birô com muitos dados do mercado, dados de pessoas. São 207 milhões de pessoas e 32 milhões de empresas na minha base. Portanto, fazem parte do core da nossa empresa os dados pessoais, os dados de negativação, os dados de ações e protestos dentro do nosso portfólio de dados. A lei permeia desde o core da empresa, o board da empresa, passando pelo jurídico, passando pelas áreas de produtos. Vamos ter que rever todos os produtos, olhar de modo diferente algumas coisas, ainda que a gente possa estar sob a proteção do legítimo interesse, para crédito, fraude, cobrança. Mas nós temos também o que chamamos de marketing service, em que podemos oferecer os dados para empresas buscarem novos clientes. Será que vamos poder fazer isso? Como é dado sensível, e, em tese pelo menos, de legítimo interesse, tradicionalmente não precisávamos de autorizações. Mas para o cadastro positivo, por exemplo, vai entrar toda essa história do opt out e opt in. Será que na hora em que a lei entrar em vigor, teremos que avisar 120 milhões que são o mercado alvo desse cadastro? Imaginem o dinheiro que isso vai consumir. Para mim, as áreas de TI e de segurança são meras facilitadoras de uma regra de negócio da empresa. O foco são os modelos de negócio e isso vai nos impactar bastante.

A lei rege a guarda e rege também a exposição do dado, e nisso é diferente da lei europeia, que faz a regra da gestão do dado e não da exposição. Então há uma série de nuances aí que é diferente tanto na lei europeia quanto na nossa lei.

Uma das questões que mais me preocupam é o fato de que, hoje, uma negativação tem a validade de cinco anos. Se de repente tenho que excluir a pessoa, como é que fica essa negativação? Como é que se trabalha esse processo? É uma questão de negócio, em que vamos ter que trabalhar com os bancos, que é quem consome informação de crédito?

Olhando do ponto de vista tecnológico, há algumas coisas que podem ser feitas para melhorar o nosso processo. Como birô, nós temos uma preocupação muito grande quanto à rastreabilidade do dado, de onde ele veio. Nós temos esse compromisso, somos o fiel depositário dos dados dos nossos clientes e precisamos evitar vazamentos de informações para o mercado.

Marcel - A lei também fala que não é aplicável quando o dado é considerado anonimizado. Ou seja, se de fato o sistema não permite que se saiba a quem o dado pertence, nem quando combinado com outras informações de quem receber esse dado. O problema é que aí você vai ter uma discussão muito grande de quão anonimizado esse dado estava. Tem um caso concreto que ajuda a ilustrar isso. Uma empresa europeia fazia o seguinte: justificando que estava anonimizando o dado, ela eliminava o último octeto do endereço IP dos usuários. Como vocês sabem melhor que eu, isso permite você saber a origem geográfica, o país ou às vezes, até dependendo da precisão, outras coisas. Eles disseram que anonimizavam os dados. Como os dados foram considerados não suficientemente anonimizados, ela foi multada. Acho que todo mundo entendeu que não tem um único caminho. O caminho correto é fazer a coisa certa, que é realmente buscar o compliance com a legislação. É doloroso e complicado, porque estamos importando uma cultura legislativa que nunca tivemos. Mas acho que os benefícios aí de médio e longo prazo serão grandes.

Rogério - O grande problema dessa história é como se operacionaliza a lei.

Marcel - É isso mesmo.

Rogério - Hoje, para abrir uma conta, a gente pede lá 100 dados. Será que esses 100 dados são necessários? Eu preciso de raça? Vou justificar que a raça interessa? Se vou fazer uma seleção de candidatos para o banco, preciso saber o sexo? Por causa daquele cadastro de seleção de funcionários, vou ter que pegar o consentimento? Então, essa revisão de todos os cadastros, para eliminar coisas que não necessita é fundamental para, depois, no ambiente de TI, a gente deixá-lo menos complexo.

Marcel - Tem um elemento adicional que eu agregaria que o fato de que as multas e outras possíveis penalidades podem ser muito atenuadas, se fica claro que a empresa ao menos tentou cumprir a lei, implementou mecanismos de governança, etc. Ainda que tenha tomado todas as de cisões catastroficamente erradas, como se basear em interesse legítimo quando não podia, os europeus têm considerado esse esforço. Eles punem também, pois foram cometidos alguns erros, mas em patamar infinitamente mais bando. Ou seja, não podemos pensar no compliance como uma coisa absoluta de tudo ou nada, mas como jornada mesmo.

Rogério - Outro tema que estamos discutindo é o dos dados dos colaboradores. Temos mais de 100 mil colaboradores. Como garantir que os dados deles estão protegidos por essa lei, de tal forma que na hora em que saírem não vão exigir algum dado que não estaria em compliance?

Curt - E como é que fica o mercado de seguros, com apólices que devem ser guardadas por 20 anos?

Marcel - Mas aí tem a obrigação legal. A questão é que você não pode usar esses dados de 20 anos para marketing. Aí se trata do atrelamento com a finalidade.

Curt - Há ainda a questão das novas tecnologias, como o blockchain, que tem alguns outros princípios, ou o open banking. O problema com o blockchain é que você não apaga, não opera. Fora o controle dessa informação na rede. Quer dizer, uma vez que participo dela, é meio que premissa que os participantes tenham acesso aos dados que estão trafegando. Quer dizer, nós temos algumas tecnologias que resolvem alguns problemas, mas que vão ser limitadas de alguma forma com isso.

IH - Parece claro que há aqui um consenso de que a aplicação da lei não é uma questão do jurídico nem da TI das empresas, mas é uma questão de negócio. De toda forma, acho que seria interessante uma última reflexão sobre a questão da tecnologia, porque se falou aqui em automatizar alguns procedimentos para a melhor adequação à lei.

Waldir - Não sei se a gente já tem essa visão clara. Agora, todo fornecedor diz que está compliant com a lei. Isso me faz lembrar da época de cloud, quando todo mundo tinha hardware e solução para cloud. Não sei se hoje temos isso. Porque ferramenta para mim é aquilo que você usa após a definição daquilo que tem que fazer. Então a complicação maior acho que é essa: é o entendimento da tecnologia de acordo com a nossa necessidade. E a necessidade ainda não está clara.

Igohr - Como hoje ainda não há uma definição sobre se determinado dado cadastral do cliente é sensível ou não, ou se é público ou não, embora existam e muitos pacotes de mercado, acho que não existe sistema que controle isso.

Rogério - Com relação à proteção de dados, você tem.

Igohr - Isso sim.

Rogério - Quando você vai compartilhar, acho que o segredo está em saber que tipo de informação você pode enviar. Então na hora de transmitir o arquivo, hoje você já tem ferramentas que possibilitam que você, em um cadastro que tem 30 campos, selecione cinco e só compartilhe aqueles outros cinco. E você fica com os 30 protegidos do seu lado.

Igohr - Isso sim. Mas o cliente pode decidir o que ele quer ou não e eu vou ter que ter isso armazenado em algum lugar.

Rogério - Aqui a gente volta àquela história do consentimento, que considero o mais crítico. Na tecnologia o mais difícil para nós, que ainda não encontramos no Bradesco, é a milha final, que é a exclusão. Como garanto que de fato eu excluí aquilo, de tal forma que um perito, se vier fazer uma auditoria, vai confirma que aquele dado foi realmente excluído? Do ponto de vista da tecnologia, estamos nos debruçando bastante para ver que ferramentas de fato vão garantir que o dado foi excluído e que se tiver uma perícia, seja qual for, de fato aquele dado não apareça mais.

André - Quero dar um exemplo da complexidade desse tema. Digamos que você tenha a retenção por cinco anos do backup. Você nunca vai conseguir excluir os dados de backup até a retenção morrer. Ou seja, no final do dia, o dado do cliente sempre vai continuar existindo. Pode ser que no seu sistema de front end ele não exista, mas se você tem retenção de cinco anos, se excluir seu front end, ele vai demorar cinco anos para sair do seu backup. Não existe uma tecnologia que permita que você exclua dados do backup.

Célio - Hoje, você não armazena o backup quando chega de manhã e resolve armazenar. Isso custaria muito dinheiro e tem toda uma administração por trás. Você é obrigado a armazenar. Na minha visão, ainda não está no momento das ferramentas. Acho que essa vai ser uma trajetória longa, certamente muito mais longa do que o período que vai até a entrada da lei em vigor.

Curt - Tenho notado, neste curto espaço de tempo, e a gente já recebeu lá diversos especialistas, que nenhum deles está sentado aqui e pilotando o que estamos pilotando.

Carlos Augusto - Nesse ponto, acho que a questão da arquitetura ajuda muito a ter uma gestão melhor. Trabalhei em vários bancos e sempre brinquei que tinha dezenas de cadastros únicos. Mas consegui uma arquitetura em que realmente tenho o cadastro único, então os meus dados de clientes estão em um lugar só. Todo o meu analitycs está em um lugar, um data lake só, então a gestão fica muito mais fácil. É claro que depende da complexidade e do porte da empresa, mas há uma jornada que facilita, no sentido de garantir a integridade dos dados.

Hamilton Penna

“Vamos ter que rever todos os produtos, olhar de modo diferente algumas coisas, ainda que a gente possa estar sob a proteção do legítimo interesse, para crédito, fraude, cobrança”.

Waldir, da Boa Vista

A Micro Focus ajuda as empresas a se adequarem a nova Lei Geral de Proteção de Dados por meio da utilização de produtos inovadores e processos confiáveis. Conheça a nossa metodologia e casos de sucesso dos nossos principais clientes acessando o nosso site :
www.microfocus.com/en-us/marketing/gdpr
E assista ao webinar *WEBINAR - LGPD (Lei Geral de Proteção de Dados)* no nosso canal do YouTube:
www.youtube.com/Microfocusbrasil

MICRO FOCUS