Três motivos para que os CIOs considerem o GDPR enquanto o prazo se aproxima

Aruna Ravichandran (*)

Com o prazo de adaptação ao Regulamento Geral de Proteção de Dados (GDPR – General Data Protection Regulation) da União Europeia chegando ao fim, os CIOs estão correndo para mitigar riscos de multa por não cumprirem com as exigências

GDPR é uma regulamentação que exige que as empresas protegam os dados pessoais e a privacidade dos cidadão europeus para todas as transações realizadas entre membros da União Europeia.

Este é um exercício tático necessário, mas os CIOs não devem pensar sobre o GDPR apenas por este viés. Na verdade, existem três razões importantes para que todos os CIOs vejam o GDPR também de forma estratégica.

Razão nº 1: A responsabilidade futura pelo uso de dados pessoais irá além do GDPR

O prazo final para adaptação ao GDPR (25 de maio de 2018) é uma data importante. Porém, não será a última.

À medida que as organizações acumulam mais dados do cliente, exploram e monetizam esses dados das mais diversas formas, e considerando possíveis usos inadequados dessas informações que expõe os clientes a maiores riscos, é importante que as agências reguladoras e os formuladores de políticas tomem medidas apropriadas.

O GDPR pode ser a resposta atual de maior destaque às preocupações relacionadas aos dados dos clientes, mas é apenas um indicativo das mudanças que estão por vir. Uma nova evolução da economia digital global inevitavelmente levará a outras regulamentações relacionadas à gestão de dados, e não apenas na União Europeia e nos Estados Unidos, mas em todo o mundo. Na verdade, o GDPR foi amplamente discutido em vários fóruns legislativos e regulatórios em Washington DC, inclusive quando Julie Brill, da Comissão Federal de Comércio dos Estados Unidos, escreveu: "O GDPR terá efeitos abrangentes sobre todos nós... [e] parte do seu objetivo foi definir um padrão global."

Esta é uma mudança estratégica, não apenas tática. Historicamente, os CIOs consideravam os dados armazenados na infraestrutura corporativa como propriedade corporativa. O modelo tradicional considera os dados como uma propriedade de quem os coleta.

O GDPR sinaliza uma mudança radical neste modelo. No futuro, as empresas apenas pegarão "emprestado" os dados dos seus proprietários (leia-se, dos cidadãos), que terão os direitos específicos relacionados ao ciclo de vida dos mesmos. Os CIOs devem repensar todos os aspectos da empresa digital neste contexto.

Razão nº 2: A conformidade com o GDPR é mais do que apenas a governança de dados

A visão simplista do GDPR é a de que você estará em conformidade se gastar dinheiro com ferramentas de governança de dados e encontrar um agente de dados suficientemente engajado para impor as políticas internas de governança de dados de uma organização.

Mas isso é apenas parcialmente correto. Para cumprir com o GDPR e outros regulamentos relacionados, você precisa da tecnologia certa e das pessoas certas para ficarem de olho nos dados em toda a empresa.

Mas existem muitas outras fontes de dados na empresa digital atual além dos aplicativos e bancos de dados em produção. A pressão para colocar rapidamente novos recursos digitais inovadores no mercado, por exemplo, está fazendo com que muitas equipes de DevOps acelerem e não analisem bem os dados de teste que elas usam para realizar o trabalho. Às vezes, esses dados são enviados para fora da empresa para contratar desenvolvedores e QA shops sem qualquer mascaramento.

Por outro lado, muitas empresas recebem dados de terceiros sem investigar suficientemente as práticas de limpeza dessas informações. Essas ações podem expor uma companhia a responsabilidades graves relacionadas a dados, independente de se achar segura ou em conformidade.

Os CIOs devem considerar a conformidade como uma regra empresarial estratégica. São necessárias políticas fortes, transparentes e eficazes de descoberta, de coleta, de teste, de gerenciamento e remoção de dados, não apenas para garantir o cumprimento, mas também como parte integral da construção de relações digitais confiáveis e duradouras com os clientes.

Razão nº 3: O GDPR é uma oportunidade para a marca, não apenas uma carga imposta externamente.

Quando surge um regulamento complexo e de alto impacto, como o GDPR, é comum vê-lo um fardo. Afinal, para se adaptar ao GDPR, as organizações geralmente usam recursos de outras iniciativas e a atenção do CIO é desviada de outros assuntos urgentes.

Então, por que não considerar transformar os custos que você não pode evitar em investimentos que compensam no longo prazo? Uma boa administração de dados não deve ser apenas algo que fazemos porque somos obrigados. Deve ser algo que fazemos porque é ético e de valor para nossos clientes. Além disso, o GDPR oferece um campo de atuação igual entre as empresas internacionais, incentivando o desenvolvimento de tecnologias inovadoras que podem beneficiar a todos.

Muitas empresas usam a responsabilidade corporativa a seu favor. A rede varejista Whole Foods e a fabricante de roupas e acessórios esportivos Patagonia são exemplos clássicos de empresas que elevam suas marcas e o envolvimento de clientes ao contextualizar as compras como mais do que meras transações financeiras. Quem pode dizer que a administração de dados não pode se tornar um equivalente digital da proteção ambiental ou impacto social do tipo "na compra de um produto, doamos outro para caridade"?

Além disso, a administração insuficiente pode trazer consequências estratégicas além das multas por descumprimento. Se os clientes não acham que podem confiar em você com seus dados, eles provavelmente não confiarão em você com seu dinheiro.

Mas isso sugere que os CIOs que consideram a administração de dados de forma estratégica serão superiores aos que não colocam isso em prática. Então, por que não se juntar a eles?

(*) É VP de Product Marketing da CA Technologies.

Blockchain, a verdade e a era da Confiança 3.0

Assim como a definição da 'verdade' mudou radicalmente com o advento da Internet e das redes sociais, a definição de 'confiança' no século XXI será reescrita por novas tecnologias como o Blockchain

Omarson Costa (*)

Fonte da imagem: Collaberex

Estava começando a escrever este artigo quando o senhor Mark Zuckerberg declarou guerra contra as "fake news", anunciando que o Facebook passará a dar prioridade aos posts dos seus amigos no feed em detrimento aos posts de notícias. Mas será que ele conseguirá vencer esta batalha? Seu "mea culpa" irá evitar que mentiras (ou falsas verdades) sejam espalhadas pela Internet?

Acho difícil. Depois da era digital, uma coisa é a verdade; outra é em quem você confia.

Quando as redes sociais deram vez e voz aos usuários, a verdade entrou em cheque e gerou uma crise de confiança, abrindo um terreno fértil para infestar nossas timelines com 'verdades' das mais variadas.

Mudar os algoritmos do Facebook não deve exterminar a boataria nociva pelo simples fato de que sempre haverá outros canais para viralizar posts sensacionalistas e, principalmente, por conta de uma mudança no comportamento da humanidade pós-Internet que me inspirou neste texto: o digital mudou nossa relação com a verdade, nos levando a estabelecer novas relações de confiança e a acreditar mais nas pessoas e menos nas instituições, como a própria mídia, os bancos, o governo e outras que, mesmo com os dois pés atrás, fomos obrigados até hoje, por falta de opção, a ter fé.

Quem imaginava que entraríamos no carro de um desconhecido ao invés de chamar um táxi (Uber) confiando em um ranking? Ou que aceitaríamos receber ou nos hospedar na casa de alguém que nunca vimos na vida no lugar de escolher um hotel (Airbnb)? E o que leva milhões de investidores a acreditar em uma moeda virtual sem lastro com nenhum ativo financeiro tradicional? Resposta: Confiança.

Em entrevista ao blog Futurism, a escritora Rachel Botsman, autora do livro "Who Can you Trust? How Techonology Brought Us Together – and Why It Could Drive Us Apart", pontua: "A confiança está mudando das instituições para os indivíduos... e ainda estamos vendo as profundas consequências desta mudança, da influência na eleição presidencial ao Brexit, os algorismos e os bots".

E continua: "estamos vivendo um vácuo de confiança que surge quando nossa crença em fatos e na verdade é continuamente questionada... Neste vácuo nos tornamos mais suscetíveis e vulneráveis a teorias da conspiração, a diferentes vozes que sabem falar com os sentimentos da pessoa acima dos fatos. É uma nova forma tóxica de transparência".

Há histórias inacreditáveis de como um falsário pode influenciar a opinião de um desavisado que bota a maior fé nas redes sociais. No final do ano passado correu o mundo a saga do escritor londrino Oobah Butler, que enganou o TripAdvisor montando um grupo de amigos para regidir reviews positivos para um restaurante fake que criou no quintal de casa com o garboso nome The Shed at Dulwich. O site do restaurante está até hoje no ar e, acreditem, continua atraindo clientes.

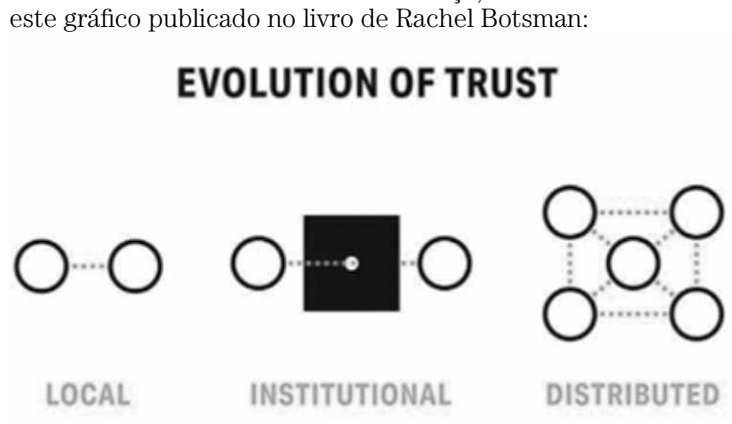
A coisa foi tão longe que o restaurante ficou cotado como o melhor de Londres sem nunca ter de fato existido! Para desfazer a mentira, Butler chegou a chamar alguns dos clientes que fizeram reserva no restaurante e serviu marmitas compradas no mercado. O curioso, mas não totalmente inesperado, é que muitos clientes elogiaram a comida e disseram que gostariam de voltar!

Da mesma maneira que dão cada vez menos ouvido à mídia, os 'millenials' mostram estar mais dispostos a depositar confiança em fintechs ou no bitcoin do que nos bancos e nas moedas cunhadas pelos reis, que mereciam reverência por terem sido indicados por Deus.

Um sistema monetário tem um dos seus pilares sustentado pela confiança. Possivelmente, como já aconteceu em vários episódios na história (a quebra da Bolsa de Nova York ou a Black Monday, para citar alguns dos mais emblemáticos), o fim da confiança irá aniquilar muitas moedas virtuais, mas isso não quer dizer que elas deixarão de existir.

O grande benefício do bitcoin, além de se tornar uma alternativa (de alto risco) aos investidores, foi o desenvolvimento da tecnologia que está por trás das moedas de bites: o blockchain, um sistema distribuído que não é de propriedade de ninguém; é um ativo da Internet disponível a todos os seus usuários e que estabeleceu um novo padrão de confiança para transação de dados confidenciais e recursos financeiros.

A confiança tem um custo. E o blockchain irá ajudar a derrubar este custo. Ele é a versão 3.0 da confiança, como bem demonstra este gráfico publicado no livro de Rachel Botsman:



Na sua versão 1.0 a confiança era estabelecida no caderninho de fiado do quitandeiro ou nas moedas emitidas por reis. Era uma confiança local, peer to peer. Na 2.0 passamos a confiar nas instituições e, ao invés do olho no olho, começamos a emitir boletos e acreditar nos recebíveis carimbados pelos bancos.

Chegamos na 3.0 voltando para uma descentralização em que a segurança é garantida por um sistema em cloud, distribuído, que permitirá não apenas a transação de moedas, eliminado a necessidade de acreditar cegamente no sistema financeiro e no Banco Central, mas a construção de novos modelos de negócios baseados em relações de confiança – não serão os bancos os únicos a ser impactados pelo blockchain; muitas indústrias serão transformadas pela tecnologia.

Em resumo, qualquer negócio que for sustentado por relações de confiança e precisar de um contrato para validar uma transação entre duas ou mais partes poderá ser viabilizado pela tecnologia blockchain. Um fundo de crowdfunding, uma empresa de crédito, um banco de dados, um sistema de armazenamento e compartilhamento de documentos digitais, um sistema de logística, uma empresa de seguros.

Com um olho no futuro, o que aterroriza é pensar que algoritmos e robôs poderão analisar dados sobre nós, humanos, e atribuir notas de confiança para que sejamos ou não considerados confiáveis. Se por acaso um robô disser que você não merece crédito o que irá fazer? Se acha ficção, saiba que a China já colocou em teste o Social Credit System (SCS), que irá ranquear os cidadãos de acordo com seu status econômico e social a partir de dados coletados pelo governo.

Debater a ética sobre o avanço dos sistemas de Inteligência Artificial e da robótica se torna cada vez mais necessário, como propôs a primeira-ministra britânica em seu discurso em Davos. Ninguém vai querer deixar a decisão de julgamento moral para uma máquina ou ter interpretações de éticas que dependem do programador, da empresa ou do país de origem do sistema criado. Mas não se espante se dia desses encontrar em algum tribunal qualquer um robô-advogado.

(*) É formado em Análise de Sistemas e Marketing, tem MBA e especialização em Direito em Telecomunicações. Em sua carreira, registra passagens em empresas de telecom, meios de pagamento e Internet.

News @TI

Wappa lança serviço FastPass para pagamento automático de corridas de táxi

@Pensando em facilitar ainda mais a vida dos profissionais que precisam cumprir compromissos externos, a Wappa, pioneira e líder no setor de táxi corporativo e presente no mercado há mais de 15 anos, lança a função FastPass em seu app. A nova funcionalidade permitirá o pagamento automático das corridas, em alguns segundos, direto no aplicativo, eliminando completamente o uso de senhas. O diferencial do negócio é que todo processo será feito no app do taxista. O usuário precisa apenas confirmar o valor da corrida e, na sequência, recebe uma notificação em seu celular com a confirmação de pagamento e os dados da corrida.

Indicada como líder para plataformas de proteção endpoint

@A Sophos (LSE: SOPH), líder global em segurança de rede e endpoint, foi indicada pelo Gartner, Inc. como líder no Quadrante Mágico 2018 para Plataformas de Proteção de Endpoint[1]. A Sophos tem sido posicionada como líder nos 10 relatórios que foram publicados pela consultoria desde 2007. No relatório, o Gartner afirma que a definição de uma Plataforma de proteção de endpoint (PEP) foi atualizada: "Em setembro de 2017, em resposta à mudança da dinâmica do mercado e dos requisitos dos clientes, ajustamos nossa definição de um PEP. Um PEP é uma solução implantada em dispositivos de endpoint para evitar malwares baseados em arquivos, detectar e bloquear atividades mal-intencionadas de aplicativos confiáveis e não confiáveis, e fornecer recursos de investigação e remediação necessários para responder dinamicamente a incidentes e alertas de segurança" (www.sophos.com).

Novo canal no YouTube incentiva o brincar

O canal Toyzera vai inovar os conceitos de brincar dentro do YouTube. A linguagem divertida e leve dos episódios será criada pela Snack junto dos influenciadores Cauê Bueno (Baixa Memória) e Carolina Fernando (CajuTV), e o objetivo relaciona-se com momentos prazerosos de diversão, criatividade e muita brincadeira para as famílias.

"Vamos construir histórias e experiências usando formatos nativos da internet aliados a expertise da rede", afirma Vitor Knijnik, sócio fundador da Snack, maior rede multiplataforma brasileira de social video.

O canal estreiou na última quarta-feira (07/02) com o primeiro vídeo na parte da tarde. A princípio, serão duas temporadas (seis meses cada) com total de quarenta e oito episódios. O canal será dividido em quatro playlists: funboxing, mashup, top da galera e a ciência do brinquedo. Os temas estão relacionados com novidades, curiosidades e tutoriais sobre utilização de brinquedos.

Para a diretora de marketing da Ri Happy, Flávia Drummond, essa será mais uma plataforma que vai estimular o desenvolvimento através do brincar. "Continuamos nossa missão em levar o brincar por todo país e esse canal oferece diversas sugestões de brincadeiras, seja ao ar livre, entre amigos e toda família", esclarece a diretora.

Todos os vídeos serão gravados no estúdio localizado na loja Ri Happy da Av. Otto Baumgart, 800, em São Paulo. O espaço estará aberto todos os dias para os fãs conhecerem de perto a experiência fantástica do brincar. Para acessar o canal: https://www.youtube.com/channel/UCllVN3C7Cx_m9rdg9AcJYYw