Novo marco regulatório para market places no Brasil: o que é importante saber

Gastão Mattos (*)

A Câmara Brasileira de Comércio Eletrônico (câmara-e.net) e a Gmattos organizaram em julho um evento para discutir o impacto do novo marco regulatório sobre liquidação de pagamentos em market places no Brasil

A relevância das vendas online via market places é expressiva, alcançando 25% do total vendido no comércio eletrônico no país, com viés de alta. Segundo o Internet Retailer Conference + Exhibition (IRCE), metade do faturamento global do e-commerce refere-se vendas por market places. No Brasil, estimo que também chegaremos a 50% do total das vendas no horizonte máximo de 3 anos. Os grandes players do mercado como B2W, Via Varejo, Walmart, Máquina de Vendas, Magazine Luiza, Dafiti, Netshoes, entre outros, ou mesmo novos como o iFood já operam na modalidade de Market Place, em muitos casos, atuando como liquidantes dos pagamentos ao receberem o valor integral pago, para posterior repasse aos Sellers (lojas que usam o market place para vender suas mercadorias). Nesta operação, caracteriza-se o papel de subcredenciador para a loja âncora ou market place.

No evento, especialistas da Câmara Interbancária de Pagamentos (CIP), Visa e Moip compartilharam sua visão a respeito do novo marco definido pelo BACEN através da Circular 3886 e Carta Circular 3872.

Em resumo, o BACEN definiu que qualquer operação que realize intermediação de pagamentos, participando da sua liquidação, precisa estar enquadrada neste regulatório. Isso significa que subcredenciadores (subadquirentes ou facilitadores) que recebam o pagamento, criando uma nova agenda para dividir o recebível em partes entre sellers e market places, estão sujeitos à regulação.

Dentre outras obrigações, a mais relevante é a necessidade de uso da Câmara Interbancária de Pagamentos (CIP) para liquidação de todos os pagamentos em cartões de crédito a partir de 28 de setembro próximo, para aqueles subcredenciadores que movimentaram mais de R$ 500 milhões em transações de crédito nos últimos 12 meses. Esta obrigação se refere aos pagamentos feitos no papel de subcredenciador apenas. A medida tem caráter de proteção ao ecossistema de pagamento, pelo eventual risco sistêmico, na falha de algum agente liquidante quanto às suas obrigações.

Mesmo para aqueles subcredenciadores que não tenham atingido este limite, é necessária adequação à normas, dentre as quais ter sua operação homologada pelos "arranjos de pagamentos". Entenda-se "arranjos" como as bandeiras aceitas pelo subcredenciador (Visa, MasterCard, Amex, Diners, Elo, Hipercar etc). As bandeiras ou arranjos funcionarão como controladores desta nova norma, aprovando ou impedindo a operação de subcredenciadores.

Este papel a ser assumido pela Visa e outras bandeiras globais é inédito. Em nenhum outro mercado as bandeiras de aceitação têm esta responsabilidade.

Já a integração obrigatória na CIP para a liquidação de pagamentos é algo bastante complexo, pois implica em desenvolver e manter um novo fluxo para o processo mais sensível de um market place, ou seja, organizar a agenda de recebimento e divisão de valores com a efetiva liquidação dos pagamentos.

O tempo mínimo estimado para integração técnica é de 6 semanas. Contudo, o caminho crítico para sua efetivação pode ser bem mais longo, porque a CIP somente inicia seu processo após assinatura de contrato, que exige a apresentação de documentação de aprovação do subcredenciador pelos arranjos de pagamento a serem utilizados. Aqueles subcredenciadores ou postulantes a este papel que, neste momento, estiverem ainda nesta fase (contrato com a CIP) não terão mais tempo hábil de se enquadrar até a data estipulada pelo BACEN (28 de setembro de 2018).

Isso gera uma situação de atenção, porque segundo a CIP menos de 10 subcredenciadores estão em processo de integração (nenhum ainda concluído), o que leva a crer que uma grande parte da demanda dos market places será atendida via a contratação de processadores homologados (subadquirentes estabelecidos), que se encarreguem da liquidação na CIP, ao menos para adequação inicial ao regulatório.

Uma fase instável de adequação é esperada para que todos os agentes envolvidos possam se adequar, mas como quase sempre, momentos de ruptura como este podem revelar oportunidades para surgimento de novos players ou expansão de serviços para players existentes, como, por exemplo, empresas adquirentes. Não por acaso, as principais adquirentes como Cielo, Rede e Getnet Santander estão disponibilizando plataformas de serviço para o subcredenciamento. Outros players independentes como Moip também são uma alternativa para este serviço.

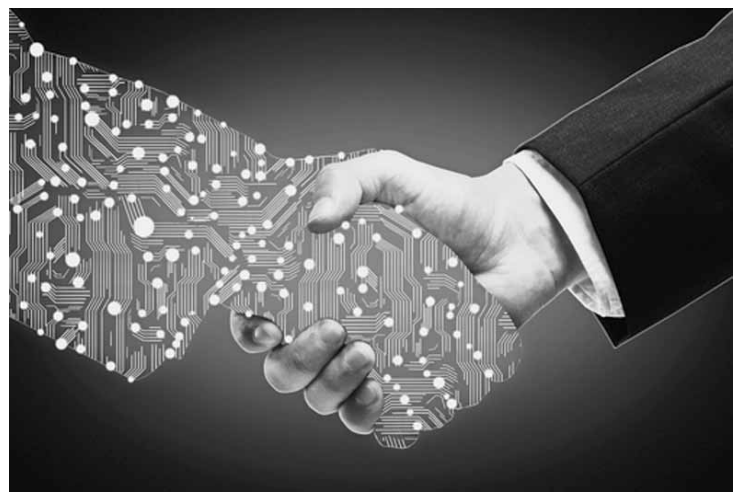
Embora exista uma tendência entre grandes varejistas pela internalização do subcredenciamento da modalidade market places buscando melhores margens, não está claro se este será o modelo preponderante, dada a dificuldade e complexidade deste papel. O que me parece certo, é que boa parte dos players vai terceirizar o serviço inicialmente, seja com os grandes adquirentes ou com subadquirentes independentes, ganhando tempo para validar a hipótese de subcredenciamento próprio.

(*) É sócio fundador da Gmattos, empresa especializada no mundo online, com foco em Pagamentos. Uma de suas competências é interpretar tecnologias emergentes e indicar o caminho viável para sua proliferação no mercado digital.

Como se preparar para a transformação digital do Direito

A hora para adquirir as competências necessárias para lidar com as tendências digitais do direito é agora

Daniel de Lima Cabrera (*)



No início de julho uma polêmica envolvendo o uso de robôs para consulta jurídica mobilizou os advogados. Esta polêmica envolve apenas o começo de uma profunda transformação digital que já começa a atingir todo o universo do Direito. Big data, inteligência artificial e contratos digitais são apenas algumas tendências que estão moldando a advocacia do futuro.

Estudo realizado pela American Bar Association mostra que 90% dos advogados norte-americanos já utilizam ativamente soluções digitais móveis específicas para o trabalho jurídico. Outro estudo, da LexisNexis, mostra que as soluções de inteligência artificial existentes já podem tornar o trabalho do advogado até 90% mais rápido. É uma transformação profunda na forma como estamos habituados a trabalhar.

Por isso, o principal desafio dos advogados é se preparar. Com base nas tendências que estão norteando o processo de transformação digital, seguem algumas ações que podem empoderar o jurista diante dos desafios da tecnologia:

Direito baseado em dados

Algoritmos de inteligência artificial conseguem analisar microdados e mapear tendências contraintuitivas de conflitos judiciais. Saber aplicar a ciência de dados na análise destes microdados, usando se possível machine learnings, pode permitir ao advogado analisar qual a melhor estratégia de defesa, quais os riscos que estão expondo mais as empresas e como decidem determinados juízes diante de determinados temas.

Contratos em forma de software

Se um advogado ainda não ouviu falar na Solidity, linguagem de programação elaborada para smart contracts que rodam na blockchain da Ethereum, é hora de ouvir falar. A Solidity é a primeira linguagem de programação que consegue traduzir cláusulas contratuais em código fonte de software, transformando o contrato em um aplicativo.

Outras plataformas similares devem surgir, permitindo que, por exemplo, um termo de confissão de dívida esteja integrado ao banco para monitorar se a dívida foi paga e, caso contrário, faça automaticamente a negativação do cliente, o protesto da dívida, a notificação extrajudicial ou mesmo a execução judicial da dívida. Cartórios, bancos e tribunais já contam com digitalização suficiente para isso.

Segurança de dados

Há muito mais informação circulando, e os termos de confidencialidade tradicionais não são mais suficientes para proteger as informações sigilosas de uma corporação. Há apenas dez anos bastava um non-disclosure agreement (NDA) para assegurar a confidencialidade dos dados. Hoje torna-se fundamental compreender algoritmos de criptografia como a SHA-256, criada pela Agência Nacional de Segurança (NSA) para proteger os documentos confidenciais do governo norte-americano. Em um ambiente de negócios cada vez mais dominado pela computação em nuvem, soluções móveis e internet das coisas, este tipo de conhecimento precisará ser dominado pelo advogado para proteger o sigilo das informações.

Olhe para o Reino Unido

O maior mercado de trabalho para advogados no mundo é o Reino Unido, e é lá que as tendências de transformação digital do direito estão mais desenvolvidas. A PwC acredita que "o trabalho do advogado será liderado pelas pessoas, mas ele será cada vez mais acelerado pela tecnologia". Pesquisa com as 100 maiores bancas de advocacia do Reino Unido, mostra que 80% delas já conta com uma estratégia digital clara, e o custo com TI já responde pela maior parte do orçamento de atividades de suporte dos escritórios.

Ainda que a definição de estratégias complexas e a relação humana com os interlocutores da atividade jurídica sejam atribuições dos operadores do Direito que, por ora, não estão ameaçadas pelos robôs, a hora de começar a buscar essas competências é agora. O profissional de direito, como qualquer outro, terá que ser cada vez mais multidisciplinar, incorporando conhecimentos e pessoas de exatas ao seu trabalho diário. A mudança que a carreira de Direito está vivendo neste momento é equivalente à gerada pela fundação da Faculdade de Direito Civil na Universidade de Bolonha em 1088.

(*) É sócio da Cabrera Advogados Associados. É graduado em Direito pela Faculdade de Direito de São Bernardo do Campo, pós graduado em Direito Civil e Processo Civil pela Escola Paulista de Direito (EPD); especialista em Recursos no Código de Processo Civil pela Faculdade Autônoma de Direito (Fadisp), pós graduado em Direito Tributário pela Faculdade de Direito de São Bernardo do Campo, e concluiu MBA em Gestão Estratégica e Econômica de Negócios na FGV.

Brasil tem mais de 7,2 milhões de sites desprotegidos

Mapeamento da internet brasileira feito pela BigData Corp a pedido da Serasa Experian em junho deste ano aponta que 40,10% dos sites do país não estão seguros, o que representa um total de 7,2 milhões de endereços. Estes sites não possuem o certificado de segurança (SSL – Secure Socket Layer), que promove uma conexão segura utilizando a criptografia entre o servidor e os dados trafegados, o que evita o roubo de dados durante a transação.

O estudo também mostra que no mesmo período de 2016 o percentual de sites sem a proteção era ainda maior: 62,42%. Ainda que o país tenha assistido um rápido avanço na adoção do SSL no período, o volume de sites sem os certificados de segurança ainda é considerado alto. Outro aspecto que chama a atenção no estudo é o fato de que, mesmo entre os que possuem os sites que possuem certificados de segurança, perto de um quarto (24.97% ou 2,73 milhões) estão expirados e precisam ser renovados. E outros 3,7 milhões, ou 34,07% dos que possuem o certificado, terão suas licenças expiradas em até três meses.

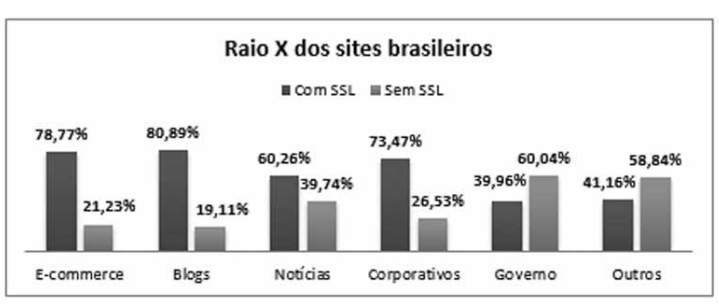
"É bom lembrarmos que no restante do mundo, no entanto, em média, apenas 8,57% dos sites não possuem essa proteção. E a questão ganha uma relevância ainda maior no momento em que sites sem certificados de SSL são expostos pelo Google com avisos de "não seguros" e deixam de aparecer nos primeiros lugares nas buscas feitas pelo Google", comenta Thoran Rodrigues, CEO e fundador da BigData Corp. Ou seja, segundo Rodrigues, empresas que mantêm sites sem a camada de SSL poderão ser prejudicadas pois terão seus sites nas últimas páginas de resultados nos sites de busca.

Maurício Balassiano, diretor de certificação digital da Serasa Experian, alerta que os consumidores devem ficar atentos para que seus dados, sejam bancários ou pessoais, não fiquem à mercê de possíveis golpistas. "Para isso, basta verificar se há cadeado na barra de endereço, ou se há um "s" após o http (https), indicando segurança, além da identificação de "seguro" e "não seguro" dada por alguns navegadores", ensina.

Os dois executivos apontam que o certificado expirado é algo ainda mais crítico para as empresas. Quando certificado está expirado e um usuário tenta acessar o site, seja por meio de uma busca ou quando o usuário digita direto o endereço, o navegador mostra uma página vermelha de erro, com um aviso informando que aquele endereço não é seguro, assustando o internauta. Dessa forma, ter o certificado expirado é, na verdade, pior do que não ter o certificado.

Um a cada cinco e-commerces não está seguro

Tendo em vista os vários tipos de sites, blogs são a categoria na qual os certificados SSL têm a maior penetração – 80,89% deles possuem essa proteção. "Isso se deve quase inteiramente ao fato de que boa parte deles está hospedada em grandes plataformas, que instalam o certificado automaticamente para eles", explica o CEO da BigData Corp. Naturalmente, e-commerces (78,77%) e sites corporativos (73,47%) vêm em seguida.



Mesmo que os e-commerces tenham um alto percentual de proteção em relação aos demais tipos de site, é importante ter-se em conta que, por se tratarem de sites que transacionam dados bancários, o percentual de 21,23% de sites inseguros é alto. Isso significa que aproximadamente um em cada cinco sites de comércio eletrônico não possui o certificado de segurança que criptografa os dados transacionados.

Percentual de grandes sites descobertos surpreende

Um dado do estudo que surpreende é o fato de que mais de um terço (37,36%) dos grandes sites com mais de meio milhão de visitas mensais não possuam certificados SSL. O índice é semelhante (37,51%) entre os sites médios – com mais de 10 mil e meio milhão de visitas mensais. Entre os pequenos – que recebem menos de 10 mil visitas mensais, o SSL está presente apenas em 41,98% deles.

Do ponto de vista da idade das empresas que mantêm sites com SSL, as mais antigas, com 20 anos ou mais, são a maioria – respondendo por uma participação 36,75%. Em segundo lugar, com 20,42% estão os sites entre 5 e 10 anos, e os de 10 a 15 anos (18,37%).

São Paulo lidera a participação dos sites que possuem SSL (33,77%), seguido por Minas Gerais (9%), Rio de Janeiro (8,8%) e Rio Grande do Sul (8,03%).

Ambientes inseguros

Uma prática muito utilizada pelos golpistas no ambiente online inseguro é a de phishing, na qual os criminosos copiam as informações trocadas durante uma transação. Dados pessoais roubados, como nome, endereço, CPF etc., podem ser coletados para fraude de identidade, que acontece quando dados pessoais de um consumidor são usados por terceiros para firmar negócios sob falsidade ideológica ou obter crédito sem a intenção de honrar os pagamentos.

Para verificar se o site possui o certificado SSL e, portanto, os dados trafegados estão sendo criptografados, sem risco de roubo, basta checar se há um cadeado na barra de status, ou se há um "s" após o http (https), indicando segurança. Em alguns casos, a barra de endereço do navegador fica verde. Atualmente alguns navegadores incluem para todos os sites a indicação de "Seguro" e "Não Seguro" também na barra de endereço. Normalmente também há um selo de segurança, atribuído pelo fornecedor do certificado, que pode ser encontrado no próprio site.

News @TI

Ferramenta de login online com certificado digital

@Chamado de Identific, o novo produto da Serasa Experian possibilita a identificação dos usuários (consumidores ou empresas) no ambiente digital por meio dos certificados digitais e-CPF, e-CNPJ e NF-e, apenas com a inclusão da senha "pin", que tem de 4 a 15 caracteres. A certificação digital é uma tecnologia que permite a identificação de pessoas físicas e jurídicas no ambiente eletrônico, regulamentada no país pela Infraestrutura de Chaves Pública Brasileira (ICP-Brasil), vinculada à Casa Civil da Presidência da República. Por isso, dá mais segurança aos processos de login na internet, diferente de outros métodos que utilizam apenas login e senha, ou logins de redes sociais (www.certificadodigital.com.br).