



Advogados americanos discutem implicações éticas da computação em nuvem

No *Techshow* da ABA (*American Bar Association*) deste ano, foram apresentadas novas regras do código de ética dos advogados, para adaptá-lo à era digital. De uma maneira geral, o advogado tem o dever de ser competente tecnologicamente e estar consciente das implicações éticas da computação em nuvem.

Em uma discussão sobre “Ética, Segurança e Computação em Nuvem”, representantes da ABA disseram que, “de acordo com as novas regras de conduta profissional, os advogados devem se manter atualizados sobre os benefícios e os riscos das tecnologias relevantes para a prática, da mesma forma que devem se atualizar frequentemente sobre as mudanças nas leis”.

A palavra mais usada em toda a discussão é o adjetivo “razoável” — isto é, advogados não precisam ser gênios em tecnologia, mas devem fazer “esforços razoáveis” para preservar a confidencialidade dos dados ou informações do cliente, mantidas na nuvem. Devem impedir qualquer divulgação não autorizada, mesmo que isso ocorra de forma inadvertida.

“Os advogados devem fazer esforços razoáveis para manter a confidencialidade, incluindo a sensibilidade das informações, as probabilidades de vazamento na ausência de salvaguardas e os custos e as dificuldades de implementar salvaguardas adicionais”, dizem as regras.

Até o momento, seccionais da ABA em 14 estados apresentaram propostas sobre as responsabilidades éticas dos advogados em relação à computação em nuvem (ver abaixo). Os representantes da ABA apresentaram cinco recomendações:

- Mantenha-se atualizado;
- Aprenda o que não sabe;
- Lembre-se de que você não está garantindo a segurança das informações do cliente contra acesso não autorizado [*isso fica a cargo da empresa provedora do serviço de computação em nuvem*];
- Reveja, periodicamente, as medidas de segurança adotadas pela provedora do serviço de computação em nuvem;
- Não se esqueça de que circunstâncias especiais exigem precauções especiais.

As propostas das seccionais da ABA procuram conciliar a computação em nuvem às obrigações éticas dos advogados. Algumas podem ser adotadas por qualquer escritório de advocacia, outras podem ser discutidas. Uma proposta interessante é a de estabelecer no contrato de serviço a responsabilização civil da provedora por qualquer vazamento de dados dos clientes.



Conheça as propostas que as seccionais da ABA apresentaram, até agora:

ESTADO	Propostas
ALABAMA	<ul style="list-style-type: none">· Saiba como a fornecedora lida com armazenamento e segurança de dados.· Assegure-se razoavelmente de que o acordo de confidencialidade seja obedecido.· Conheça as melhores práticas sobre salvaguardas de dados.
ARIZONA	<ul style="list-style-type: none">· Tome precauções razoáveis de segurança, incluindo proteção de senha, criptografia, etc.· Desenvolva ou consulte alguém com competência em segurança de computação <i>online</i>.· Reveja periodicamente as medidas de segurança.
CALIFÓRNIA	<ul style="list-style-type: none">· Avalie a natureza da tecnologia, precauções de segurança disponíveis e limitações ao acesso de terceiros.· Consulte um especialista na ausência de <i>expertise</i> dos advogados.· Avalie a sensibilidade dos dados, o impacto de um vazamento para o cliente, a urgência da situação e as instruções do cliente.
IOWA	<ul style="list-style-type: none">· Assegure-se de que terá acesso irrestrito a seus dados, quando necessário, incluindo a remoção deles na terminação do serviço.· Determine o grau de proteção assegurado aos dados armazenados em um serviço de computação em nuvem.



MAINE	<ul style="list-style-type: none">· A fornecedora do serviço e possivelmente seus funcionários devem ter uma obrigação executável de manter a confidencialidade.· A fornecedora deve notificar o escritório sobre qualquer caso de vazamento.· Os dados devem ser transferidos à fornecedora de uma maneira segura.
MASSACHUSETTS	<ul style="list-style-type: none">· Reveja (e examine periodicamente) os termos do serviço, restrições ao acesso a dados, portabilidade dos dados e práticas de segurança da fornecedora do serviço.· Siga expressamente as instruções do cliente em relação ao uso de tecnologia de nuvem para armazenar e transmitir dados.· No caso de informações particularmente sensíveis do cliente, obtenha a sua aprovação antes de armazenar ou transmitir informações pela internet.
NOVA HAMPSHIRE	<ul style="list-style-type: none">· Tenha um entendimento básico da tecnologia e conheça as mudanças nas leis e regulamentos sobre privacidade.· Considere obter o consentimento informado do cliente, antes de armazenar na nuvem informações altamente confidenciais.· Remova os dados do cliente da nuvem e os dê a ele à conclusão da representação ou quando o arquivo não precisa mais ser preservado.· Faça um esforço razoável para assegurar que as provedoras de serviço na nuvem entendam e ajam de uma maneira compatível com as responsabilidades profissionais dos advogados.
NOVA JERSEY	<ul style="list-style-type: none">· A provedora do serviço deve ter uma obrigação executável de preservar a confidencialidade e a segurança.· Use tecnologia disponível para proteger as informações contra tentativas previsíveis de bisbilhotagem dos dados.



NOVA YORK	<ul style="list-style-type: none">· A provedora deve ter uma obrigação executável de preservar a confidencialidade e a segurança dos dados e deve notificar o advogado se for citada por dados do cliente.· Use tecnologia disponível para proteger as informações contra tentativas previsíveis de bisbilhotagem dos dados.· Examine as práticas de segurança da provedora do serviço e reveja periodicamente para se certificar de que estão atualizadas.· Investigue qualquer quebra potencial de segurança ou lapsos da provedora para se certificar de que os dados do cliente não sejam comprometidos.
NEVADA	<ul style="list-style-type: none">· Escolha uma provedora de serviço na qual possa confiar razoavelmente, no que se refere à preservação das informações confidenciais do cliente.· Instrua e exija que a provedora mantenha a confidencialidade das informações do cliente.
CAROLINA DO NORTE	<ul style="list-style-type: none">· Examine os termos e as políticas e, se necessário, renegocie, para se certificar de que sejam consistentes com suas obrigações éticas.· Avalie as medidas de segurança da provedora e sua estratégia de <i>back-up</i>.· Assegure-se de que os dados poderão ser recuperados se a provedora interromper suas atividades ou se os advogados quiserem cancelar o serviço.
OREGON	<ul style="list-style-type: none">· Assegure-se que o acordo de serviço exija que o vendedor preserve a confidencialidade e a segurança.· Exija o envio de uma notificação no caso de os dados serem acessados por uma parte não autorizada.· Certifique-se de que o serviço de <i>back-up</i> seja adequado.· Reavalie passos preventivos periodicamente, à luz dos avanços da tecnologia.



PENSILVÂNIA	<ul style="list-style-type: none">· Tome medidas razoáveis para se certificar de que todo material armazenado na nuvem permaneça confidencial.· Empregue salvaguardas razoáveis para proteger os dados contra vazamentos, perdas de dados e outros riscos.· Conheça todas as propostas de possíveis salvaguardas.
VERMONT	<ul style="list-style-type: none">· Tome precauções razoáveis para assegurar que os dados do cliente permaneçam seguros e acessíveis.· Considere se certos tipos de dados (como, por exemplo, testamentos) devam ser guardados no formato original em papel.· Discuta a adequabilidade do armazenamento em nuvem com o cliente, se os dados forem especialmente sensíveis (por exemplo, segredos comerciais).

Date Created

04/04/2014