Entenda o que é o assinador Shodô do PJe, novo e-SAJ e o que mudará no peticionamento eletrônico brasileiro.

José Antonio Milagre – 14/02/2017

Inscreva-se no meu canal no Youtube. Vídeos semanais sobre Direito Digital e Informática Juridica!

Os militantes da Justiça do trabalho estão se deparando recentemente com avisos sobre uma nova forma de assinar documentos no PJe, de nome "Shodô" ("a arte da caligrafia", em japonês). Mas afinal, o que é este aplicativo e no que ele é diferenciado?

O Shodô é uma aplicativo de assinatura para Justiça do Trabalho que nasceu considerando a descontinuidade e necessidade de substituir a tecnologia mais antiga usada para assinatura digital, denominada Applet. Os Applets fazem a interface do usuário para a digitação do PIN e reconhecimento do certificado digital.

Ocorre que, no caso específico, os navegadores estão descontinuando (alguns já descontinuaram) o suporte a Applets e o que restava ao usuário era a troca de navegador. Um exemplo é o Firefox que só pode ser usado no PJe, para quem usa assinador com base no Java, até a versão 41. Ou seja, advogados tinham que ficar desatualizando seus sistemas ou

baixar o navegador PJe feito pelo CNJ em http://www.pje.jus.br/wiki/index.php/Navegador_PJe.

A diferença é que ao contrario da validação do certificado em Java ou Applet, a validação agora passa a ser feita por aplicativo desenvolvido pelo próprio Conselho Superior da Justiça do Trabalho.

O aplicativo pode validar documentos por exemplo, com o PJeOffice, desenvolvido pelo CNJ (disponível na tela de login do PJe). Com o Shodô, espera-se que o usuário possa voltar a usar navegadores até então considerados incompatíveis e até mesmo versões mais novas de navegadores como Firefox, que muitas vezes, se atualizados, tornavam o peticionamento inviável. É possível assinar documentos pelo Shodô diretamente ou pelo PJe Office.

A expectativa é que em 2017 grande parte do PJe migre para nova versão, 1.14. Uma das novidades previstas para o Shodô, é a possibilidade, na versão 15, de uso de certificados modelo A1, ou seja, arquivos de computador que não precisam ser gravados em token ou carteira criptográfica. Hoje a plataforma 2adv (http://trend2adv.com.br/) já permite esta funcionalidade.

O que é interessante é que embora venha para substituir o Applet, o fato é que é necessário o Java para instalar o executável Shodô no computador do Advogado, o que fez com que muitos colegas indagassem se não está-se trocando seis por meia dúzia.

Nesta esteira, sabe-se também quem na Justiça Estadual, alguns sistemas já caminham para substituição de autenticadores de assinatura baseados em Java para aplicações plug-ins próprios, como é o caso do e-SAJ (Usado em vários Estados), cuja empresa anunciou em alguns Estados o Web Signer (anunciado no TJ/SC http://www.sajdigital.com.br/saj-na-midia/web-signer-do-portal-e-saj/) e que permite ressuscitar até mesmo a utilização do

Internet Explorer, do mesmo modo, substituindo a leitura de tokens feita em Java, permitindo qualquer versão de outros navegadores. A modificação vem recebendo o nome de “novo e-saj”. Embora a Softplan informe que se trata de um “plug-ins nativo” dos navegadores, não é o que parece das pesquisas que realizamos.

Em São Paulo, a possível mudança chamou a atenção da Comissão de Informática da OAB/SP, que de forma proativa já se manifestou no sentido de requerer um prazo mais confortável para os Advogados. Sob o prisma da segurança, não há duvidas que as medidas de certo modo permitem que Advogados voltem a atualizar seus aplicativos, consequentemente mantendo-se com paths de segurança ativados. Já quanto à segurança das novas aplicações, caberá análises mais aprofundadas.

Se haverá melhorias em termos de funcionalidades, agilidade, acessibilidade e redução de falhas, só o tempo, ou melhor, a Advocacia, é que poderá dizer. Por hora, cabe a nós nos preparar para as mudanças anunciadas.

Referências

Saiba mais sobre a configuração do Shodô para PJe, acessando http://www.trt15.jus.br/programas/pdf/PJE15-ConfiguracaoAssinadorShodo.pdf

Assista um vídeo sobre o Shodô feito pelo CSJT em: https://www.youtube.com/watch?v=nc7v09RP6cU

Acesse: Facebook.com/professormilagre

José Antonio Milagre é Advogado, Mestre e Doutorando em Ciencia da Informação pela UNESP, MBA em Tecnologia da Informação e Presidente da Comissão de Direito Digital e Processo Eletrônico da OAB/SP Regional da Lapa.

Inscreva-se no meu canal no Youtube. Vídeos semanais sobre Direito Digital e Informática Juridica!

O que fazer em caso de crime na Internet ou contra a privacidade cometido pelo WhatsApp?

O WhatsApp é um dos mais populares aplicativos no Brasil, cresceu pois integrou número de telefone celular a comunicação via Internet, de forma gratuita. Não se justifica mais o envio de torpedos SMS pagos se é possível se comunicar com maior eficiência em uma interface gratuita. Além disso, o aplicativo permite o envio de conteúdo multimídia, áudio e vídeo e a criação de grupos. A aplicação diz ter 38 milhões de usuários no Brasil. 430 milhões de usuário no mundo.

A qualquer cidadão, com um pacote mínimo de dados é permitido se valer dos benefícios do mensageiro. Porém, tal aplicação, hoje de responsabilidade do provedor de serviços Facebook, vem sendo utilizada como plataforma para a pratica de crimes eletrônicos, nomeadamente, compartilhamento de conteúdo ofensivo, ameaçador, difamatório e envolvendo crimes de intolerância e pornografia infantil.

Graças a possibilidade de criação de grupos, usuários podem criar “grupos fechados” e adicionar somente quem desejar. Quem

é adicionado não recebe um convite mas entra de imediato, devendo deixar o grupo caso não se sinta confortável. E se o grupo compartilhava conteúdo ilegal? Seu nome pode ser listado como um participante, mesmo não tendo aceitado convite algum.

Diante da vingança pornô, ou da cópia indevida de fotos e vídeos íntimos, privados ou de cunho sexual envolvendo uma pessoa, era comum a criação de blogs anônimos, perfis ou páginas em redes sociais divulgando o conteúdo "caiu na rede". De posse da "URL" ou do link específico da postagem (com a numeração do usuário (id), página ou postagem) era possível mover ação para identificação da pessoa por trás da ofensa, bem como para remoção do conteúdo.

Porém, no Whatsapp, vítimas de crimes na Internet sofrem com uma agravante: A mensagem com conteúdo inverídico corre de celular para celular, ponto a ponto, ou mesmo é postada em grupo que sequer a vitima faz parte ou conhece, sendo que muitas vezes não tem como especificar o "local", dentro do serviço, em que o conteúdo fora compartilhado, quanto mais precisar "qual" telefone realizou a postagem inicial.

Os tempos são outros. Se antes a vítima comparecia à polícia ou a um escritório de advocacia com cópias das postagens, hoje comparece informando que "ouviu dizer" que em algum no lugar no WhatsApp suas fotos ou vídeos em situação íntima estão circulando.

E o cenário se ultraja, pois com a Lei 12.965/2014, o Marco Civil da Internet, nos termos do seu art. 21, o provedor deverá indisponibilizar, tão logo notificado extrajudicialmente, o conteúdo envolvendo imagens, vídeos ou outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado em relação a vítima, sob pena de ser responsabilizado. Por outro lado, esta notificação deverá ter elementos que permitam a identificação específica do material apontado como violador da intimidade. Mas como identificar?

Neste contexto, algumas orientações e procedimentos simples podem auxiliar aqueles que tiveram problemas com o uso indevido do WhatsApp para a divulgação de conteúdo íntimo:

1. *Converse com quem viu a mensagem ou que participa do grupo referido e verifique se podem lhe transmitir o conteúdo ou pelo menos indicar os nomes dos grupos, nomes ou números telefônicos das pessoas responsáveis pelo conteúdo ofensivo; Lembrando que se conseguir entrar no grupo, só verá as mensagens posteriores ao ingresso;*

2. *Tenha em mente que o nome que aparece em um contato pode ser fantasiado, então, busque pelo número de telefone utilizado pelas mensagens; Embora com certeza usuários e grupos tenham um "ID" na aplicação, ao contrário de outras redes sociais, tal dado não é exibível ao público;*

3. *Se algum amigo recebeu o conteúdo, ele pode fazer um backup da conversa e remeter para um e-mail ou mesmo lhe remeter o conteúdo; Se algum conhecido é participante do grupo, ele pode extrair uma lista de todos os participantes;*

4. *Você não vai conseguir pesquisar por repositório de grupos na Internet e só consegue entrar em um grupo se te adicionarem – O que é bem diferente das redes sociais convencionais; Por outro lado, considere o Google na busca por pessoas mencionando o grupo no Whatsapp;*

5. *Uma pessoa pode estar cadastrada no Whatsapp com um numero que não mais detém ou (em casos específicos) de terceiros; Cuidado em tomar conclusões precipitadas. Converse com um perito digital; Jamais processe alguém por achismo ou presunção;*

6. *Registre todo o material envolvendo o conteúdo ofensivo, se necessário lavre uma ata notarial, onde um cartório irá constatar que acessando a aplicação pelo usuário x, na data e hora y, obteve acesso ao conteúdo ilegal;*

7. É um erro processar a operadora de telefonia ou provedor de Internet para que forneça dados de um usuário do Whatsapp; Embora o WhatsApp atue com números telefônicos (como ID na aplicação), cada usuário faz um cadastro independente no sistema. O provedor de conexão deverá ser acionado após a vitima descobrir o Ip ou os dados do telefone do responsável;

8. No pedido de dados de acesso a aplicação, solicite também os números telefônicos cadastrados e o IMEI (número de série do equipamento) (O WhatsApp registra esta informação);

9. De posse dos dados cadastrais do responsável pela publicação do conteúdo (após fornecimento dos dados pelo provedor de conexão ou telefonia), pode ser o caso da determinação judicial de uma busca e apreensão do equipamento celular para verificar se o conteúdo lá se encontra, podendo os chats serem recuperados mesmo após a exclusão;

10. Ordem judicial específica poderá requerer o extrato das comunicações feitas de um usuário WhatsApp para outro.

Com estas orientações e medidas a vítima minimizará a dificuldade de apuração da autoria de um crime virtual cometido na plataforma, lembrando que, embora o WhatsApp declare em seus termos que está sob a Lei da Califórnia, ao tratar informações de brasileiros, deve oferecer foro no Brasil para resolução de litígios e principalmente, está obrigado, pelo Marco Civil da Internet, a guardar os registros de acesso a aplicação por 6 (seis) meses. Portanto, a vitima deve agir rapidamente.