# E-mails exigem cuidados específicos para servirem como prova


Já é comum que processos jurídicos utilizem uma mensagem de correio eletrônico como meio de prova. Seja sobre um contrato trocado pelo e-mail e as manifestações expressas de vontade entre as partes nas mensagens que o discutem ou como elemento cabal da existência de uma fraude interna em uma empresa ou uma licitação, o e-mail é sem dúvida um instrumento de prova.

Então basta salvar o e-mail como PDF e dar *upload* no processo eletrônico e tudo certo? Com a devida ressalva aos especialistas por deixar de lado procedimentos mais aprofundados, algumas considerações gerais são necessárias antes de simplesmente responder não a esta pergunta.

Assim como um papel impresso pode ser válido como documento apenas após uma perícia, a validação de um e-mail como prova não pode ser feita pela análise de um papel com a mensagem impressa. Uma mensagem de e-mail não serve como prova válida antes de uma perícia que garanta algumas características mínimas de sua validade.

Um e-mail somente será uma prova documental, com validade intrínseca, se atender as seguintes características:

- Autenticidade. Possibilidade de validação da chave geradora com base em uma chave pública;
- Confidencialidade. O emissor possui chave pessoal e registrada em uma cadeia de autenticação;
- Integridade. A alteração de um bit sequer na mensagem resulta em uma incompatibilidade com as chaves;
- Irretratabilidade. O emissor não pode negar que aplicou a assinatura à mensagem.

Ou seja, um e-mail é uma prova inerentemente considerável somente se for assinado eletronicamente, a exemplo da assinatura do magistrado em um processo eletrônico conferindo características de documento eletrônico para o despacho.

Quando este não for o caso, as mensagens devem ser periciadas para atestarem suas características de prova jurídica. Em princípio a perícia deve validar:

- O arquivo da mensagem em si, verificando origem, destino, data, hora e conteúdo;
- A cadeia de custódia da mensagem, validando a não contaminação do valor jurídico da prova, verificando especialmente autorizações e garantia de integridade das informações custodiadas.

A cadeia de custódia é especialmente relevante para os casos de informações em meio digital, dada a facilidade de alteração dos conteúdos sem rastros aferíveis.

Somente será possível equacionar a validade da mensagem se, além do acesso ao arquivo da mensagem que foi impressa, for seguida a sequência de atos que levaram à aquisição da informação. Desde a coleta na máquina, no servidor ou no provedor até a posse do arquivo pela parte.

Quando se trata de mensagem originada diretamente de provedores de aplicação na Internet (*webmail*), a exemplo do Gmail do Google ou Hotmail da Microsoft e dos nacionais Terra ou UOL, conseguidas por meio de quebras judiciais de sigilo telemático, tem-se que cada mensagem pode estar dentro de um conjunto de mensagens.

Os conjuntos de mensagens podem ser enviados pelo próprio provedor de aplicação responsável pelo domínio do e-mail, colhendo a caixa de e-mails por completo. Os provedores de aplicação de e-mails na Internet são acostumados a este procedimento, nos EUA a Microsoft até cobra para fornecer estes dados aos investigadores, conforme indicado nos vazamentos da NSA efetuados pelo ex-agente Snowden.

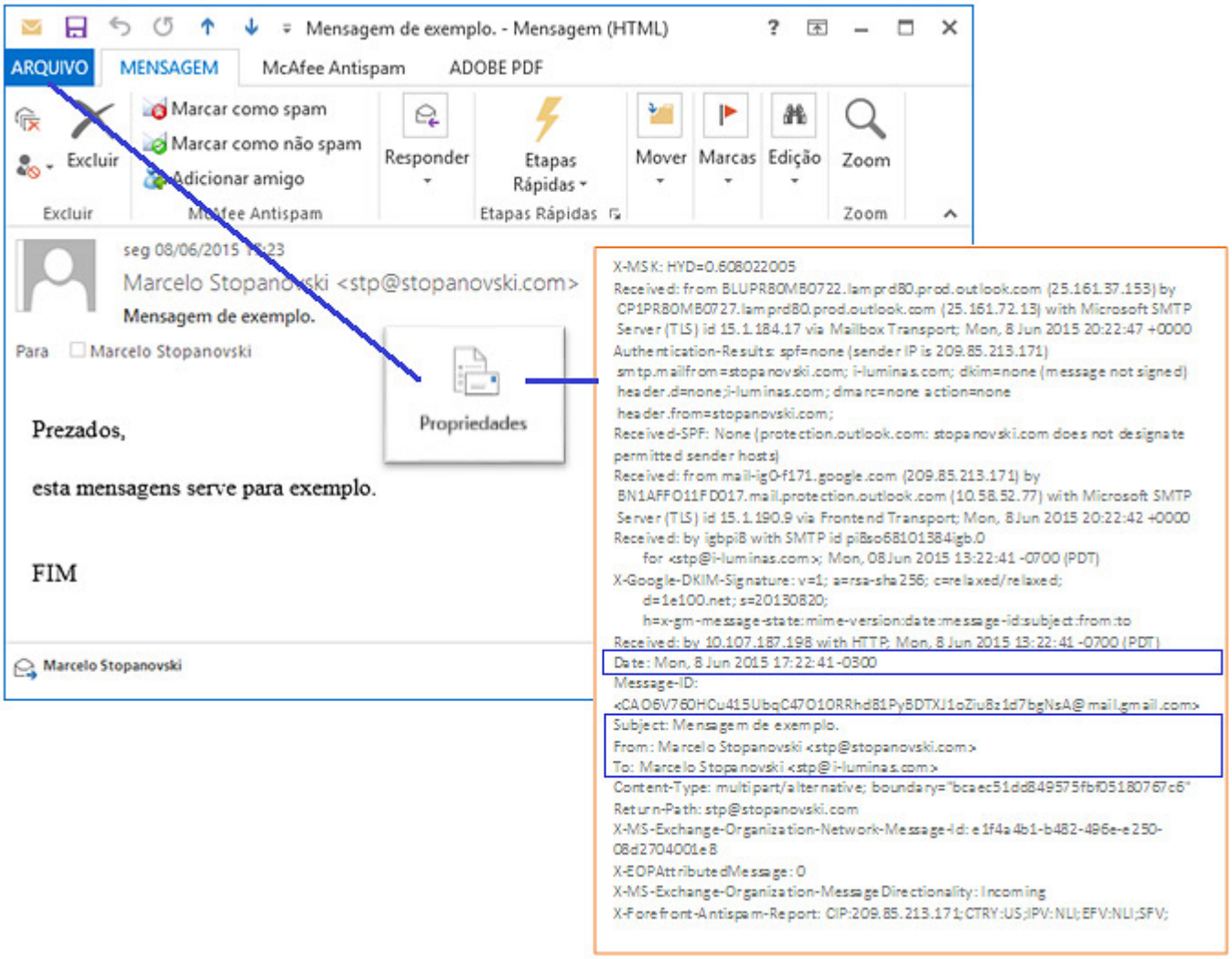
O conjunto pode também ser adquirido em uma busca e apreensão no servidor alvo ou pode ser providenciado pela própria parte interessada.

Em todos estes procedimentos para que cada conjunto adquira a segurança necessária visando sua utilidade como prova jurídica é necessário que seja garantido que o que foi colhido corresponda exatamente ao que está disponível para o juízo e as partes.

A tecnologia no estado da arte para que tal garantia seja dada é muito semelhante em funcionamento à própria assinatura eletrônica. No momento da coleta utiliza-se um algoritmo de *hash* (MD5, RDS por exemplo) para gerar uma chave de validação do conjunto de mensagens disponibilizadas. Esta chave é utilizada pelo juízo e pelas partes para conferir se as informações que estão sendo acessadas formam

Após a garantia da fonte íntegra, as mensagens podem ser submetidas à perícia de forma individual para validação de seus metadados e serem então discutidas como prova. Metadados são dos dados sobre os dados. São as informações que descrevem a estrutura, forma, tempo, origem e destino da mensagem.

Quando de posse de um arquivo no formato de uma mensagem de correio eletrônico é possível verificar seus metadados de plano, pois eles já estão dispostos geralmente no início da mensagem. Ocorre que estas informações podem não corresponder à informação real da mensagem, pois é possível alterá-las. Faz-se necessário verificar o que em termos um pouco mais técnicos chama-se cabeçalho do e-mail, e



Na mensagem aberta acessa-se "Arquivo" e depois "Propriedades", então o cabeçalho da mensagem exibe todas as transações entre os computadores servidores dos provedores de e-mail e as identificações de cada máquina (IP), sendo os reais metadados do e-mail. Aqui eles são apresentados de forma sintetizada.

Em conclusão, estas resumidas considerações servem para indicar que um e-mail sem assinatura eletrônica não é uma prova documental em si e precisa passar por perícia em sua cadeia de custódia e na mensagem propriamente dita para ser considerado como prova válida a ser discutida.

**Date Created**
02/09/2015