

A SEGURANÇA DA INFORMAÇÃO NO PROCESSO ELETRÔNICO E A NECESSIDADE DE REGULAMENTAÇÃO DA PRIVACIDADE DE DADOS

Comunicação científica a ser apresentada no XIII World Congress of procedure law

José Carlos de Araújo Almeida Filho¹

INTRODUÇÃO. I. NECESSIDADE DE PROTEÇÃO DE DADOS. II. RELATIVIZAÇÃO DO PRINCÍPIO DA PUBLICIDADE. III. SISTEMAS INFORMÁTICOS SEGUROS E DIREITO PROCESSUAL. IV. NORMA ABNT 27001/2006. V. CONCLUSÃO. REFERÊNCIAS BIBLIOGRÁFICAS

INTRODUÇÃO

Analisamos, no presente texto, a necessidade da proteção de dados no sistema da informatização judicial do processo, recém implantada pela Lei no. 11.419/2006. A partir do momento em que se visualiza um sistema totalmente informático e com transmissão de peças processuais através de meios eletrônicos, estamos tratando, efetivamente, de dados.

A ciência Processual deverá caminhar *pari passu* com as novas tecnologias e, diante da crescente preocupação com sistemas de gerenciamento de documentos, encontramos a NORMA ABNT 27001/2006, tradução da ISO/IEC 27001, cuja primeira edição data de março de 2006.

Antes de adentrarmos na questão puramente informática, relativa à segurança da informação, analisamos a necessidade da proteção de dados, a possibilidade de relativizar o princípio da publicidade e a integração entre sistemas informáticos e Direito Processual.

¹ Professor de Direito Processual Civil da EMERJ, na Universidade Católica de Petrópolis e professor convidado na pós-graduação em processo civil da UERJ. Mestre em Direito pela UGF/RJ, Membro do Instituto Brasileiro de Direito Processual e advogado no Rio de Janeiro.

A questão do GED – gerenciamento eletrônico de documentos – é tratada neste texto, porque se apresenta, ao nosso sentir, a melhor política a ser adotada na tramitação dos feitos judiciais, devido a uma complexa *cadeia* sistêmica de proteção dos documentos que tramitarão. Aliado ao GED, temos a questão da segurança da informação, com a necessidade de normas previamente estipuladas e sempre de acordo com a ABNT 27001.

Finalizamos o texto com análise dos pontos mais relevante da norma ABNT, para, finalmente, concluirmos o texto com nosso pensamento acerca da informatização e sua política de proteção de dados.

I. NECESSIDADE DE PROTEÇÃO DE DADOS

No Brasil a privacidade de dados se encontra regulamentada pelo Decreto 3505/2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Em seu art. 1º observamos:

“Art. 1º Fica instituída a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, que tem como pressupostos básicos:

I - assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição;

II - proteção de assuntos que mereçam tratamento especial;

III - capacitação dos segmentos das tecnologias sensíveis;

IV - uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais;

V - criação, desenvolvimento e manutenção de mentalidade de segurança da informação;

VI - capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado; e

VII - conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade.”

Ainda que haja norma específica, tratando da proteção de dados, a mesma somente é aplicável à Administração Pública Federal, não atingindo outras esferas do sistema federativo e, com isto, causando uma enorme preocupação quando se está diante do processamento dos feitos por meio eletrônico (a informatização judicial).

Assim se admite porque as peças contidas nos autos de qualquer processo, não importando a mídia que os suporte, são dados, e, como tal, diante da crescente tecnologia da informação, aliada à promulgação da Lei nº. 11.419/2006, merecem ampla proteção. No denominado *e-Gov*, ainda que os sistemas informáticos necessitem de certificação digital, e, com isto, gozando de certa confidencialidade, não se apresenta impossível a divulgação ou *vazamento* de informações existentes no processo eletrônico.

O inciso VII da referida norma destaca a preocupação do *vazamento* de informação, ainda que se adotem chaves criptográficas para a garantia da guarda de dados dos indivíduos. O texto legal em referência demonstra a preocupação de conscientizar a administração pública de ser possível que dados telemáticos sejam disponibilizados na Internet.

A Profa. Catarina Sarmiento e Castro, da Universidade de Coimbra, ao tratar da privacidade de dados², assevera:

“(...) as ameaças à privacidade advêm também da revolução provocada pelas possibilidades abertas através do tratamento automatizado dos dados pessoais, que permite que sejamos “perseguidos” durante todo o dia, e nos transformou em “pessoas electrónicas”, encerradas num mundo de vidro...”

...

“Direito ao esquecimento

O **Direito ao esquecimento** (*the right to be let alone* ou *droit a l’oublie*) obriga a que os dados apenas possam ser conservados de forma a permitir a identificação dos seus titulares durante o período

² SARMENTO E CASTRO, Catarina. *Direito da Informática, privacidade e dados pessoais*. Almedina, 2005: Coimbra (Portugal).

necessário para a prossecução das finalidades da recolha ou do posterior.”

A preocupação quanto à necessidade de uma regulamentação mais abrangente para a proteção de dados telemáticos diz respeito à possibilidade que as pessoas têm, nos dias de hoje, de consultar a Internet, e, com isto, *vasculharem* a vida íntima do cidadão. Se uma destas pessoas solicitar, v.g., emprego em uma empresa, poderá o empregador fazer uma busca na Internet, identificando se ele possui ações cíveis, como uma execução, de Direito de Família etc³. Sendo o direito de ação garantido a todos, pode até mesmo ocorrer a possibilidade de ajuizamento de demanda totalmente inapropriada, a fim de prejudicar uma determinada pessoa. Ainda que no futuro seja julgado improcedente pedido infundado e o abuso do Direito Processual seja devidamente repugnado pelo Judiciário, a parte em questão já se encontra em prejuízo moral e material, porque não almejou um emprego ou mesmo uma promoção.

E, como nas lições da Profa. Catarina Sarmiento e Castro, a Internet e os demais meios informáticos não permitem ao cidadão o direito ao esquecimento, estando este incluindo como especialidade do direito à privacidade. Se é certo que a mídia convencional (rádio, TV e imprensa escrita) já causa enormes danos à imagem das pessoas, por possíveis matérias de cunho sensacionalista, ainda há a possibilidade das informações se perderem com o tempo e serem relegadas ao esquecimento. Contudo, na Internet, esta prática não é possível. Os dados ficam, permanentemente, alocados nos servidores e possíveis de serem analisados a qualquer momento.

Uma política de proteção de dados, a ser aplicada no Brasil e tendo como parâmetro a Diretiva 95/46 da Comunidade Européia, se apresenta oportuna e necessária.

³ No caso das consultas pelo nome de empregado (reclamante) na Justiça do Trabalho, TRT da 1ª Região, a página apresenta o seguinte alerta: “Atendendo recomendação do Presidente do TST, Ministro Francisco Fausto, fica extinta a possibilidade de consulta a andamento processual por meio do nome do trabalhador (reclamante) nesta página.”

Muito se tem discutido sobre temas afeitos ao processamento eletrônico, mas sem a devida preocupação quanto aos bancos de dados. Os autos no formato eletrônico serão alocados em servidores e estes podem estar fisicamente nos Tribunais ou alocados por empresas privadas, nos termos da norma ABNT/ISO 27001/2006. E serão considerados *dados*, para os fins de tratamento informático.

Mas o Processo moderno não deve se intimidar diante das novas tecnologias, ao mesmo passo em que as novas tecnologias não podem suplantar princípios seculares consagrados. Desde a Proclamação da Revolução Francesa e seguindo a linha histórica, com a Declaração dos Direitos do Homem, o direito da personalidade sempre foi – e deverá continuar sendo – um princípio sagrado, que poderá sobrepor-se a outros de inferioridade hierárquica no sistema constitucional pátrio.

Antes de analisarmos a nossa idéia de uma relativização do princípio da publicidade, é importante destacar que os dados poderão ser protegidos pela administração pública, mas ainda assim haverá riscos de divulgação do conteúdo dos autos de um processo eletrônico através da Internet.

Adotamos como exemplo de invasão de privacidade as *comunidades* de natureza *virtual*, como o *Orkut* e, agora, o *Youtube*, que violam, diariamente, os direitos mais sagrados do ser humano. Na obra cuja introdução é realizada pelo jornalista Heródoto Barbeiro⁴, tratando-se do relatório da *Central Intelligence Agency* (CIA), chama-nos a atenção o capítulo intitulado “*A pressão da alta tecnologia sobre a governabilidade*”:

“Hoje, usuários de microcomputador têm mais capacidade na ponta de seus dedos do que a NASA tinha como os computadores que usou na primeira viagem do homem à Lua. A tendência de uma capacidade, velocidade, redução de preços e mobilidade cada vez maior terá enorme implicação política: milhares de pessoas e de pequenos grupos – muitos dos quais nunca tiveram tanta capacidade – não apenas de conectarão com os outros, mas também planejarão, mobilizarão e cumprirão tarefas com resultados potencialmente mais satisfatórios e eficientes do que

⁴ BARBEIRO, Heródoto. *O Relatório da CIA. Como será o mundo em 2020. Economia, religião, guerras, tecnologia*. EDIOURO, SP:2006

seus governos poderiam imaginar. Isso certamente afetará o relacionamento entre indivíduos, seus governos e diretrizes governamentais, bem como gerará pressão em alguns governos para que respondam de maneira mais ágil.”

(...)

A crescente conectividade também será acompanhada pela proliferação de comunidades virtuais transnacionais, tendência que pode complicar a capacidade dos países e das instituições globais de gerar consenso e de pôr em prática as decisões tomadas, podendo até mesmo ver desafiadas as sua legitimidade e autoridade.”

O relatório da CIA aponta um cenário antes inimaginável, mas já podemos constatar o poder que a Internet vem provocando no mundo, porque as comunidades virtuais existem. A adoção de políticas públicas e a necessidade de que estas sejam de natureza transnacional não está mais distante de uma realidade. A proteção de dados telemáticos no processo eletrônico é de tal forma imperiosa, como o próprio *desafogo* do sistema judicial.

Por enquanto, diante da lentidão de nosso sistema legislativo, passamos a adotar a teoria da relativização do princípio da publicidade, mas com mecanismos de proteção de dados que seja o mais seguro possível.

II. RELATIVIZAÇÃO DO PRINCÍPIO DA PUBLICIDADE

O relatório da CIA apresenta-se preocupante e como vimos não está distante da realidade. As comunidades virtuais existem, mas, por enquanto, não chegam ao ponto de tomarem decisões e provocarem um caos na governabilidade.

No atual período do conhecimento em que vivemos, estamos na era da sociedade da informação tecnológica, com adoção de enciclopédias livres⁵, podendo ser editadas e transmitir *informação* “confiável” instantaneamente. Vivenciamos a idéia da desterritorialização, apregoada por Pierre Lévy. Em sua obra *Cibercultura*⁶, questiona a idéia de uma descentralização dos grandes centros urbanos. Ao contrário das perspectivas negativas elencadas no relatório

⁵ WIKIPEDIA – www.wikipedia.org

⁶ LÉVY, Pierre. *Cibercultura*. Editora 34, SP:2005

da CIA, Lévy aponta a possibilidade de uma integração tecnológica, com a possibilidade de eliminar a exclusão digital.

Mas não descarta o filósofo da Universidade de Paris a idéia de inserção da *cibercultura* no sistema governamental. E acrescenta em sua obra “*As tecnologias da inteligência*”⁷ o conceito de *esquecimento*:

“Por mais que elas sejam consubstanciadas à inteligência dos homens, as tecnologias intelectuais não substituem o pensamento vivo. O enorme estoque de imagens e palavras ressoando ao longo das conexões, cintilando sobre as telas, repousando em massas compactas nos discos, esperando apenas um sinal para levantar-se, metamorfosear-se, combinar entre si e propagar-se pelo mundo em ondas inesgotáveis, esta profusão de signos, de programas, esta gigantesca biblioteca de modelos em via de construção, toda esta imensa reserva não constitui ainda uma memória.

Porque a operação da memória não pode ser concebida sem as aparições e supressões que a desagregam, que a moldem de seu interior. Debruçado sobre seus projetos, o ser vivo destrói, transforma, reinterpreta as imagens e as palavras daquilo que se torna, através desta atividade, o passado. A subjetividade da memória, seu ponto essencial e vital, consiste em rejeitar a pista ou o armazenamento no passado a fim de inaugurar um novo tempo.

Ainda é necessária, portanto, uma memória humana singular para *esquecer* os dados dos bancos, as simulações, os discursos entrelaçados dos hipertextos e o balé multicolorido que o sol frio dos microprocessadores irradia sobre as telas. Para inventar a cultura do amanhã, será preciso que nos apropriemos das interfaces digitais. Depois disso, será preciso esquecer-las”.

A questão da governabilidade, aliada à filosofia das novas tecnologias alcançam o Direito Processual, porque se não houver uma política pública efetiva de proteção dos bancos de dados na informatização judicial, ou, pelo menos por enquanto, a idéia de relativização do princípio da publicidade, tanto o relatório da CIA, quanto a idéia de *sistemas a serem esquecidos*, poderão causar problemas derivados.

É certo que a idéia de um processo eletrônico tem por objetivo a aceleração da prestação à tutela jurisdicional e esta se configura, pela pacificação imposta pelo Direito Processual, na maior garantia de cidadania, como

⁷ LÉVY, Pierre. *As tecnologias da inteligência*. Editora 34, SP: 2006

exposto no art. 1º da Constituição da República Federativa do Brasil. Anteriormente à cidadania, inserida no inciso II, o inciso I do referido artigo consagra a soberania.

Diante das idéias filosóficas expostas, podemos conceber uma possibilidade de *quebra da segurança jurídica do Estado Democrático de Direito*.

Quando admitimos a idéia de relativização do princípio da publicidade, estamos tratando apenas do processo, mas a idéia poderá servir de base para toda uma construção em termos de *e-Gov*, a fim de preservar a soberania do Estado. Políticas transnacionais são de relevante importância neste cenário, tomando-se por base as diretivas da Comunidade Européia.

Mas relativizar um princípio constitucional nos obriga a avaliar a ponderação destes princípios. Isto porque encontramos hierarquicamente ligados os princípios da dignidade da pessoa humana, da liberdade de expressão, da honra, da privacidade, da publicidade dos atos judiciais e da impossibilidade de tribunais de exceção.

Trata-se de direitos fundamentais, mas não absolutos!

A Profa. Ada Pellegrini Grinover⁸ trata, no capítulo I de sua obra, sobre a *colisão de princípios constitucionais* e admite ser “um dos maiores desafios postos ao jurista contemporâneo”.

Ao tratar do princípio da proporcionalidade, que nos parece a melhor solução para discorrermos sobre a necessidade de relativização de um princípio constitucional, a ilustre e consagrada jurista adverte:

“A referida proporcionalidade deve ser entendida como *justo equilíbrio entre os meios empregados e os fins a serem alcançados*. Assim, segundo a doutrina, a proporcionalidade deve levar em conta os seguintes dados: (i) *adequação*, ou seja, a aptidão da medida para atingir os objetivos pretendidos; (ii) *necessidade*, como exigência de

⁸ GRINOVER, Ada Pellegrini. *O Processo. Estudos e pareceres*. DPJ, SP:2006

limitar um direito para proteger outro, igualmente relevante; (iii) *proporcionalidade estrita*, como ponderação da relação existente entre os meios e os fins, ou seja, restrição imposta (que não deve aniquilar o direito) e a vantagem conseguida⁹, o que importa na (iv) *não-excessividade*¹⁰”.

A idéia da teoria da proporcionalidade pode ser bem aplicada a uma teorização da relativização do princípio da publicidade, diante da inexistência de uma norma regulamentadora que garanta a efetiva proteção de dados no processo eletrônico.

Os quatro pontos destacados pela Profa. Ada Pellegrini Grinover irão justificar a idéia, porque a *adequação* consiste em promover um processo justo e rápido, mas sem a possibilidade de invasão de privacidade; a *necessidade* de limitar um direito ao outro, igualmente relevante, se justifica com mais propriedade no Processo Penal, porque a intimidade do réu, enquanto não transitada em julgado a sentença penal condenatória, não justifica que ele seja execrado pela opinião pública; a *proporcionalidade estrita* necessita impor limites a um novo sistema processual que se encontra em vigor, e finalmente, a *não-excessividade* dos meios, sob pena de transformarmos o processo eletrônico em tribunal de exceção.

A apresentação realizada até o presente momento aponta para a necessidade de uma estruturação jurídica com fundamentos sociológicos e filosóficos. E não existe no direito uma ciência que mais se coadune com a sociologia e a filosofia que o Processo.

Na obra *Direitos Fundamentais*¹¹ os autores Vicente Paulo e Marcelo Alexandrino tratam das restrições aos direitos fundamentais e ao narrarem sobre a proporcionalidade, advertem que são, em verdade, relativização de princípios. Avançam, entretanto, com a *teoria dos limites dos limites*. Segundo os autores trata-se do limite à possibilidade de limitação dos direitos fundamentais.

⁹ Cf. no texto original: Cf. Luiz Roberto Barroso, *Interpretação e aplicação da Constituição*, São Paulo, Saraiva, 1996, p. 209.

¹⁰ Cf. no texto original: Cf. Humberto Bergmann Ávila, op. cit. p. 159.

¹¹ PAULO. Vicente. ALEXANDRINO, Marcelo. *Direitos Fundamentais*. 2ed. Impetus, 2003:RJ

Mas diante de tudo quanto exposto, como conciliar princípios e direitos fundamentais? A proporcionalidade, sem dúvida, é a melhor saída, baseada em uma teoria argumentativa própria para o processo. Não se pode violar o princípio da publicidade, sob pena de termos sistemas autoritários, como também não podemos ampliar o princípio de tal maneira a violem-se os princípios da intimidade, da dignidade da pessoa humana e, como consequência destes, o direito ao esquecimento.

Casuisticamente, ainda que de forma hipotética, podemos admitir que um determinado feito tramitou do início ao fim através do procedimento eletrônico. Se as bases de dados do Tribunal admitem o acesso irrestrito, garantido pela Constituição, ressalvados os casos de segredo de justiça, a qualquer cidadão, diante do princípio da publicidade, após o trânsito em julgado e cumprimento da sentença um indivíduo poderia lançar todo o processado na Internet. E de forma anônima, porque os sistemas informáticos modernos assim o permitem.

Diante dos problemas advindos com a informatização judicial do processo, a existência de comunidades virtuais transnacionais e a possibilidade de dados telemáticos no processamento judicial serem violados, alavancamos a teoria da necessidade de relativização do princípio da publicidade, a fim de impedir livre acesso aos autos na forma eletrônica.

Com isto não se impede que as certidões sejam emitidas, mas até que uma política pública de segurança de dados seja implantada, é primordial a restrição dos atos às partes e seus procuradores.

Comumente perguntam-nos acerca do direito do advogado de analisar qualquer feito, ainda que não munido de procuração. Em todos os eventos dos quais participamos, a nossa resposta é simples: basta peticionar, eletronicamente, com utilização de certificação digital, requerendo ao juiz vista dos autos. O princípio da publicidade e o direito do advogado de ter acesso aos autos não será violado, mas a partir do momento em que qualquer pessoa alheia ao feito dele tiver conhecimento, passa a ser co-responsável por qualquer violação a outros direitos fundamentais.

A relativização do princípio da publicidade não implica em tribunal de exceção, mas garantia a outros princípios de relevante importância.

III. SISTEMAS INFORMÁTICOS SEGUROS E DIREITO PROCESSUAL

Por sistemas informáticos seguros devemos ter em mente a idéia fixa de certificação digital. E a certificação digital não é apenas para assinatura de documentos eletrônicos, mas dos próprios sistemas dos Tribunais.

Os portais aonde se alocação as informações processuais devem ser criptografados e com a adoção do denominado GED (gerenciamento eletrônico de documentos).

Entendemos que de nada adianta a *febre* da informatização judicial sem que requisitos mínimos de segurança sejam adotados, como: (i) adoção de portais com criptografia e sistema ssl; (ii) adoção de *string*¹² a fim de restringir a busca através dos motores na Internet, como *Google*, *Yahoo!*, dentre outros; (iii) a necessidade de adoção de certificação digital, dentro da hierarquia ICP-Brasil, nos termos da Medida Provisória 2.200-2/2001; (iv) adoção das normas ABNT 27001/2006; (v) adoção do GED com filtros informáticos que impeçam a visualização do documento a não ser através de pessoas cadastradas.

A adoção do GED, aliada às demais necessidades, nos parece de grande utilidade para uma política de segurança da informação. Pelo sistema adotado pela Lei 11.419/2006, o uso do *software livre* terá preferência sobre os demais, o que não significa dizer não ser possível a adoção de *software proprietário* para a tramitação dos atos processuais.

A política de *software livre* se apresenta importante, porque há relatos de poucos ataques e diminutos contágios por vírus. Desta

¹² Cf. Enciclopédia Livre Wikipedia: “Em informática uma **String** é uma seqüência de vários caracteres simples. Esta expressão é normalmente utilizada em Linguagens de programação.”

forma, aplicando-se o GED ao sistema, poderemos pensar em um sistema informatizado confiável.

O GED, segundo Baldan, Valle e Cavalcanti¹³ “é a tecnologia que provê um meio de facilmente armazenar, localizar e recuperar informações existentes em documentos e dados eletrônicos durante todo o seu “Ciclo de Vida””.

Na Enciclopédia Livre Wikipedia¹⁴, GED é definido:

“Gerenciamento eletrônico de documentos ou Gestão electrónica de documentos (GED) é uma tecnologia que provê um meio de facilmente gerar, controlar, armazenar, compartilhar e recuperar informações existentes em documentos. Os sistemas GED permitem aos usuários acessar os documentos de forma ágil e segura, normalmente via navegador Web por meio de uma intranet corporativa, a capacidade de gerenciar documentos é uma ferramenta indispensável para a Gestão do Conhecimento.

Documentos formam a grande massa de conhecimentos de uma empresa. O GED permite preservar esse patrimônio e organizar eletronicamente a documentação, para assegurar a informação necessária, na hora exata, para a pessoa certa. O GED lida com qualquer tipo de documentação.

Qualquer tipo de empresa, pequena, média ou grande, pode usar o GED, entre: escolas; empresas de advocacia; hospitais; administradoras de condomínios; empresas de recrutamento; escritórios de arquitetura, design e engenharia; assessorias de imprensa e de comunicação; e consultorias. Nas médias e grandes empresas, o GED poderá ser aplicado para setores específicos (RH, Treinamento, Contabilidade, Marketing, Informática). Este serviço avalia as necessidades específicas do cliente e oferece um sistema modular, o que possibilita a implantação gradativa do Gerenciamento Eletrônico de Documentos.”

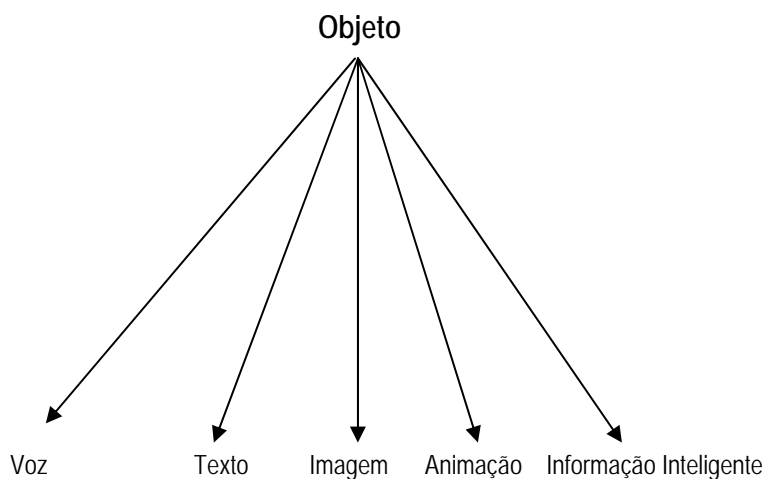
Para que o GED seja considerado como tal, somente documentos eletrônicos podem ser processados através do sistema, ou seja, acaso haja *papel*, não estaremos diante de um *Gerenciamento Eletrônico de Documentos*. A adoção de um computador, segundo os autores supra citados, é indispensável.

¹³ BALDAN, Roquemar. VALLE, Rogério. CAVALCANTI, Marcos. *GED. Gerenciamento eletrônico de documentos*. Érica, 9ed., SP: 2005

¹⁴ http://pt.wikipedia.org/wiki/Gerenciamento_eletr%C3%B4nico_de_documentos

Mas o GED pode gerenciar diversos tipos de arquivos, incluindo textos. Admitimos, contudo, que a adoção do GED em textos com o processador *Word*, por exemplo, não seja uma saída ou alternativa viável para a segurança do processo eletrônico, assim como não admitimos tão seguro o formato criado pela empresa *Adobe*, o .pdf, pela possibilidade de captura de hipertextos na Internet. A idéia de um gerenciamento passaria por programas que ocultariam o documento e, este, deveria ser processado como imagem.

E o GED possui diversas outras formas de garantia e segurança para o processamento eletrônico dos autos. No caso, por exemplo, de um interrogatório, o sistema armazena, cronologicamente, os dados, conforme se visualiza na imagem abaixo, extraída da obra dos autores citados



Não basta, para a sistemática processual, que o sistema se utilize do GED para o processamento, armazenamento e captura dos dados informáticos. Será necessária a segurança dos sistemas de informação e a possibilidade de menor erro possível na transmissão dos dados.

Acaso não percebamos estas nuances próprias da informatização judicial, os críticos e retrógrados se vangloriarão do insucesso na implantação do sistema no Brasil.

William Stallings, ph.D em Ciência da Computação, na sua obra sobre redes e sistemas¹⁵ alerta para um dado que nos é de suma importância, ou seja, a possibilidade de erros no sistema. Há previsão na Lei 11.419/2006¹⁶, quanto ao sistema do Tribunal se encontrar inoperante, mas esta questão passa pela segurança na transmissão de dados.

Se um sistema se torna instável, duas hipóteses podem ocorrer: o envio duplicado de peças processuais ou a insegurança em sua remessa. Políticas de Tecnologia da Informação, com adoção de sistemas seguros e “*necessidade de controle de erros*”, como ressaltado por Stallings são necessários e a ciência processual passa a conviver com questões complexas de Informática.

Para Stallings, “a capacidade de controlar esses erros é cada vez mais importante em sistema de comunicação de dados.”

A implementação do procedimento eletrônico em nosso sistema processual é um grande avanço, mas barreiras deverão ser rompidas. A primeira delas diz respeito à rejeição da Informática no cenário jurídico.

A questão da segurança da informação não vem sendo debatida quando se discute a informatização judicial, a não ser quanto à integridade do uso de chaves públicas e privadas e a adoção da ICP-Brasil. Ocorre, entretanto, que o Processo possui em si a missão de pacificação da sociedade e por esta razão deve estar *pari-passu* aliado às novas tecnologias da informação.

Estudos realizados pela *Loudhouse Research*¹⁷, revelam que dois terços (2/3) das empresas não se preocupam com segurança da informação. Diante de nossa atual realidade, identificamos, sem uma pesquisa

¹⁵ STALLINGS, William. *Redes e sistemas de comunicação de dados*. 5ed. Campus, RJ:2005

¹⁶ Art. 10. A distribuição da petição inicial e a juntada da contestação, dos recursos e das petições em geral, todos em formato digital, nos autos de processo eletrônico, podem ser feitas diretamente pelos advogados públicos e privados, sem necessidade de intervenção do cartório ou secretaria judicial, situação em que a autuação deverá se dar de forma automática, fornecendo-se recibo eletrônico de protocolo.

§ 2º No caso do § 1º deste artigo, se o Sistema do Poder Judiciário se tornar indisponível por motivo técnico, o prazo fica automaticamente prorrogado para o primeiro dia útil seguinte à resolução do problema.

¹⁷ <http://www.geek.com.br/modules/noticias/ver.php?id=5323&sec=5>

aprofundada, que a questão da segurança na transmissão das informações inseridas no processo não vêm sendo discutidas pelos especialistas, seja na área do Direito, seja na área da Informática.

É preciso uma política de segurança, com árduo treinamento de todos os que participam do processo, para que sistemas informáticos sejam plenamente adotados no Brasil.

Por esta razão, defendemos a idéia de controle dos atos processuais, através de relativização do princípio da publicidade e a inserção de políticas de segurança, nos termos da NORMA ABNT 27001/2006.

IV. NORMA ABNT 27001/2006

A norma ABNT NBR ISO/IEC 27001, trata, especificamente, de tecnologia da informação e segurança. Para uma perfeita aplicação do procedimento eletrônico junto aos Tribunais, não bastará a adoção de certificação digital, mas a análise da referida norma.

Um fator que provoca o afastamento do profissional do Direito da Informática é a máquina e a constante idéia de os sistemas não serem seguros. Uma pequena digressão se apresenta importante, comparando o que vivenciamos hoje, com o advento do CPC de 1939, quando, no mesmo, passou a ser adotada a datilografia como forma de materializar os atos processuais. A afirmação de que seria possível adulterar o feito parece-nos a mesma que ouvimos hoje.

A diferença é que nos sistemas informáticos é possível identificar uma alteração em qualquer documento.

A questão da segurança e dos sistemas deve competir a profissionais da área da Informática, com ampla especialização em segurança da informação.

Nos termos da Norma ABNT 27001, em sua p. 4, “a política de SGSI é considerada um documento maior da política de segurança da informação. Estas políticas devem estar descritas em um documento.”

Entendemos que não bastam os parâmetros da Lei 11.419/2006, da Medida Provisória 2.200-2/2001, se normas internas dos Tribunais não especificarem a sua política de segurança da informação. O monitoramento constante do servidor e análise crítica dos procedimentos (item 4.1 da ABNT 27001) devem ser implementadas. Os riscos no momento da transmissão de dados devem ser bem analisados, sob pena de vulnerabilidade e, com isto, enormes prejuízos causarem aos usuários do sistema.

Sabemos ser possível inserir vírus em documentos e, diante desta possibilidade, qualquer pessoa que tenha acesso a um processo no formato eletrônico, poderá causar grandes danos se políticas de segurança não forem implantadas. Uma sugestão, muito simples, é a *varredura* do documento antes de ser inserido no sistema.

Pela análise que fizemos de diversos sistemas informáticos, que permitem o envio de peças aos Tribunais, incluindo-se o Supremo Tribunal Federal, não observamos, em qualquer deles, um sistema de *varredura* dos textos a serem enviados. Os denominados *cavalos de tróia*, que são programas do tipo espião, se instalam nos servidores, e, com isto, uma enorme possibilidade de prejudicialidade de todo o sistema informático processual.

Os investimentos em TI devem ser analisados, compartilhados e integrados entre si, para que não fiquem expostos a danos. Com políticas de TI e SGSI, podemos afirmar que o sistema eletrônico é mais seguro do que o convencional, que resolverem denominar *processo físico*, em comparação com o *processo eletrônico*.

A norma ABNT 27001, em seu item 4.3.1., trata da documentação e da necessidade de rastreamento das ações inseridas no sistema. Como a

norma é abrangente, para qualquer sistema, apresenta-se com mais propriedade para grandes organizações.

Quanto a este aspecto, é de bom alvitre que passemos a analisar todo o sistema processual como uma grande organização, a fim de atribuir a cada membro a sua verdadeira função, como, por exemplo, entregar a um administrador o controle do serviço cartorário. E, dentro desta política de segurança, a partir do momento em que decisões são tomadas (aqui, na espécie, podemos inserir as judiciais, as promoções do MP e as petições, a fim de adaptar a norma geral ao sistema processual), o sistema deverá identificar através de rastreamento quem efetivamente produziu determinada peça. O primeiro passo que vislumbramos é a adoção de certificação digital nos moldes da Medida Provisória 2.200-2/2001.

Os documentos devem ser controlados e não basta a sua inserção no sistema do processo de informatização judicial (item 4.3.2.). A norma em análise aponta os seguintes requisitos:

“4.3.2. Controle de documentos

Os documentos requeridos pelo SGSI devem ser protegidos e controlados. Um procedimento documentado deve ser estabelecido para definir as ações de gestão necessárias para:

- a) aprovar documentos quanto à sua adequação antes de sua emissão¹⁸;
- b) analisar criticamente e atualizar, quando necessário, e reaprovar documentos¹⁹;
- c) assegurar que as alterações e a situação de revisão atual dos documentos sejam identificados²⁰;

¹⁸ **N.A.** Este procedimento pode ser adotado na informatização judicial, mesmo diante dos termos do art. 10 da Lei 11.419/2006, que dispõe: “A distribuição da petição inicial e a juntada da contestação, dos recursos e das petições em geral, todos em formato digital, nos autos de processo eletrônico, podem ser feitas diretamente pelos advogados públicos e privados, sem necessidade da intervenção do cartório ou secretaria judicial, situação em que a autuação deverá se dar de forma automática, fornecendo-se recibo eletrônico de protocolo.” Isto porque o documento é considerado adequado à sua inserção pela natureza do procedimento judicial. Em caso de impertinência da peça, compete ao juiz determinar a sua apensação *por linha* (o que pode soar estranho em procedimento eletrônico, mas perfeitamente cabível), ou mesmo sua desapensação.

¹⁹ Observe-se que a norma não permite adulteração, substituição ou troca do documento. Analisando a norma ABNT 27001, concluímos que a mesma trabalha com o sistema workflow, através de GED. Acaso haja alteração, por reaprovação no documento, ele perderá a assinatura digital original e incidentes de falsidade poderão ser argüidos – o que não nos parece uma política interessante. Competirá aos Tribunais, sempre atentos às normas em vigor, adaptarem a ABNT 27001 ao procedimento eletrônico, com manuais e capacitação de todos os seus servidores.

²⁰ Entendemos que o item *c* não pode ser aplicado ao processamento eletrônico, sob pena de inutilização dos atos processuais.

- d) assegurar que as versões pertinentes de documentos aplicáveis estejam disponíveis nos locais de uso;
- e) assegurar que os documentos estejam legíveis e prontamente identificáveis
- f) assegurar que os documentos permaneçam disponíveis àqueles que deles precisam e sejam transferidos, armazenados e finalmente descartados conforme os procedimentos aplicáveis à sua classificação;
- g) assegurar que documentos de origem externa sejam identificáveis;
- h) assegurar que a distribuição de documentos seja controlada;
- i) prevenir o uso não intencional de documentos obsoletos; e
- j) aplicar identificação adequada nos casos em que sejam retidos para qualquer propósito.”

A ABNT 27001, sem dúvida alguma, é aplicável ao processamento eletrônico, diante de sua especificidade. Certo, contudo, como ressaltado nas notas de rodapé, que alguns itens deverão ser adaptados ao processamento eletrônico.

Diante destas considerações, entendemos que os Tribunais devessem implantar a norma ABNT 27001 e requerer certificado ISO 27001. Todos os incidentes de segurança deverão ser previamente identificados e aplicados para que o processamento eletrônico seja adotado no Brasil como padrão mundial.

Quanto à letra *j*, é importante destacar a necessidade de aplicação da ICP-Brasil, sob pena de não se identificar o usuário e a inserção do documento nos autos do processo eletrônico²¹.

A guisa de finalização do presente texto, entendemos que os procedimentos padrões da norma ABNT devam ser adotados pelos Tribunais, notadamente no que diz respeito a *responsabilidade da direção* (item 5), *auditorias internas* (item 6) e *análise crítica* (item 7).

Com sistemas seguros e adotando-se normas internacionais de segurança da informação, a idéia de insegurança no processamento eletrônico poderá ser eliminada, restando, apenas, eliminarmos a resistência dos usuários do computador, mas esta é uma questão de política cultural. As novas gerações não enfrentarão estes problemas.

²¹ Vide ADIn's 3869 e 3880, com petição de *amicus curiae* do Instituto Brasileiro de Direito Eletrônico, disponível em www.almeidafilho.adv.br

V. CONCLUSÃO

A informatização judicial não pode ser encarada como panacéia para os males do Judiciário, mas como uma grande ferramenta para sua celeridade. Inicialmente, gostaríamos de destacar que o procedimento eletrônico não eliminará, de imediato, com o *processo convencional*, em papel, mas poderá ser utilizado como *projeto piloto* para identificação dos *pontos mortos* e *gargalos* do processo.

A adoção da informatização judicial no Brasil se apresenta importante. Redução de custos, ampliação da política ambiental etc., são os argumentos mais palatáveis para que um sistema novo e moderno como o nosso seja adotado como modelo para o resto do mundo.

Ocorre, contudo, que a Internet é uma ferramenta poderosa e com diversos mecanismos que permitem a violação de dados. Como relatado no relatório da CIA, com simples comandos em nossos computadores portáteis temos mais poder que a NASA possuía quando levou o primeiro homem à Lua.

Diante deste enorme poder, admitindo que a informatização judicial não é panacéia para os males do Judiciário, temos a convicção que em muito contribuirá para a diminuição do risco Brasil (importante lembrar que as diversas demandas e o longo tempo de espera no processo interfere nos indicadores econômicos) e para a construção de um Poder aberto ao Séc. XXI.

Contudo, a informatização judicial não pode ser analisada apenas pela Lei 11.419/2006, nem tampouco, pela Medida Provisória no. 2.2000-2/2001. Os sistemas de processamento do sistema informático processual devem conter todos os requisitos de segurança adotados no mundo.

Fica certo que a norma ABNT 27001/2006 apenas trás alguns parâmetros de segurança, sendo certo que pela especificidade do

processamento eletrônico, diversas normas não poderão ser adotadas, como o controle de alteração de documentos – porque este, em nosso entendimento, não pode ocorrer.

Diante das questões expostas, deverão os Tribunais capacitarem seus funcionários para uma perfeita política de segurança da informação e impedir, através de programas de computador, que os dados não sejam alterados ou modificados.

A interação entre os mais diversos setores do conhecimento deverão estar integrados nesta política que se apresenta, a fim de eliminar um dos dois pontos de repulsa ao sistema: a segurança.

Quanto ao segundo ponto, somente com o tempo eliminaremos a aversão aos sistemas informáticos e nossa idéia é que os juristas se preocupem menos com o *informatiquês* e se dediquem à construção de teorias jurídicas capazes de tornar a informatização judicial no Brasil um modelo a ser seguido.

Temos capacidade para esta inserção e temos profissionais qualificados para tanto.

Resta-nos superar os preconceitos.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA FILHO, José Carlos de Araújo. *Processo Eletrônico e Teoria Geral do Processo Eletrônico. A informatização judicial no Brasil*. Forense, RJ: 2007

ALMEIDA FILHO, José Carlos de Araújo. CASTRO. Aldemario Araujo. *Manual de Informática Jurídica e Direito da Informática*. Forense, RJ: 2005

BALDAN, Roquemar. VALLE, Rogério. CAVALCANTI, Marcos. *GED. Gerenciamento eletrônico de documentos*. Érica, 9ed., SP: 2005

BARBEIRO, Heródoto. *O Relatório da CIA. Como será o mundo em 2020. Economia, religião, guerras, tecnologia*. EDIOURO, SP:2006

GRINOVER, Ada Pellegrini. *O Processo. Estudos e pareceres*. DPJ, SP:2006

LÉVY, Pierre. *Cibercultura*. Editora 34, SP:2005

_____. *As tecnologias da inteligência*. Editora 34, SP: 2006

PAULO, Vicente. ALEXANDRINO, Marcelo. *Direitos Fundamentais*. 2ed. Impetus, 2003:RJ

SARMENTO E CASTRO, Catarina. *Direito da Informática, privacidade e dados pessoais*. Almedina, 2005: Coimbra (Portugal)

STALLINGS, William. *Redes e sistemas de comunicação de dados*. 5ed. Campus, RJ:2005

WAMBIER, Luiz Rodrigues. WAMBIER, Teresa Arruda Alvim. MEDINA, José Miguel Garcia. *Breves Comentários à Nova Sistemática Processual Civil*. 3. RT, SP: 2007

SITES DE REFERÊNCIA

Enciclopédia Livre *Wikipedia* – www.wikipedia.com

Processo Eletrônico – www.processoeletronico.com.br

Tribunal Regional do Trabalho da 1ª Região – www.trtrio.gov.br

NORMAS

BRASIL, Lei 11.419/2006

ABNT 27001/2006

