Leis de Segurança da Informação

Denilson Aparecido Agostinho
Universidade Federal de Santa Catarina
denilson@inf.ufsc.br

RESUMO

Na sociedade em que o bem mais valioso é o conhecimento humano, a discussão acerca da segurança da informação, ganha contornos de extrema relevância. A influência, o impacto e as soluções que o direito, em conjunto com outros campos inter-relacionados da atuação humana, busca para disciplinar as relações daí oriundas constituem o tema deste trabalho. Aborda-se o estudo de aspectos como legislação para segurança da informação, políticas nacionais e internacionais relativas ao tema em questão,infra-estrutura de chaves-públicas,e direito penal voltado a crimes contra a segurança da informação.

Palavras-Chave

Segurança, informação, legislação, políticas.

1. INTRODUÇÃO

A legislação competente à segurança da informação desenvolveu-se tendo como base os textos modelos e padrões normatizadores. Adotou-se as referências de normas já instituídas por Órgãos Oficiais, as quais criam o ambiente pertinente a aplicação da legislação, desta maneira há a possibilidade de adequação mais afinada dos modelos jurídicos à realidade do campo virtual. A Internet trouxe uma novo pensamento, um novo comportamento no cenário mundial. É o que alguns juristas denominam de sociedade da informação, na qual existe reflexão da necessidade da existência de um marco jurídico que permita a livre circulação de bens e serviços, além de garantir a liberdade dos cidadãos. Na União Européia (UE) várias batalhas estão sendo travadas para se atingir um denominador comum nas políticas de novas tecnologias de informação, a qual só pode ser assegurada por leis que permitam a regulamentação de cada país, a regulamentação entre empresas privadas e públicas e inclusive a regulamentação entre as pessoas físicas. A título de exemplo, o Conselho da Europa apresentou a última versão de um documento sobre crimes virtuais. Trata-se de um inventário com sansões penais e um dispositivo inspirado na legislação francesa. Existe uma diretiva européia sobre o comércio eletrônico, a qual reconhece a assinatura digital que, além da proteção de dados pessoais, está ganhando dimensão internacional num esforço para proteger o indivíduo. Foi criada uma certificação digital comprovando que o usuário estava realmente praticando determinado ato com sua própria identidade. Trata-se de uma verificação feita em um banco de dados específico, com a aplicação da Public Key Infrastructure (PKI). Teve início em 1997 com conferências e iniciativas no comércio eletrônico através da Organization for Economic Co-operation and Development (OECD – Organização para Cooperação e Desenvolvimento Econômico e da General Usage for International Digitally Ensured Commerce (GUIDEC).A utilização da chave pública obedece aos seguintes padrões internacionais: ISO 9796, ANSIX9.31, ITU-T x509, PACS, SWIFT. Países que ainda estão criando as normatizações e legislações tendem a exigir tipos específicos de tecnologias para seguirem padrões já existente, desta maneira alcançam uma homogeneidade e compatibilidade com os demais países. Tomando-se tais atitudes, cria-se um ambiente propicio a eliminação de obstáculos para que os certificados sejam reconhecidos em outras nações e as negociações possam ter realmente amparo judicial legal perante o comércio internacional .De forma geral o mundo está consciente da real importância da elaboração de legislações específicas a tais ambientes e encontram-se tramites de projetos em diversos países, havendo de tal forma uma perspectiva altamente positiva para que num futuro breve o Brasil também tenha um sistema legislador especifico e eficiente.

2. POLÍTICA NACIONAL DE SEGURANÇA DAS INFORMAÇÕES

Consciente da importância das informações processadas nos órgãos e entidades da administração, o Presidente da República editou recentemente o Decreto 3.505, de 13 de junho de 2000, por meio do qual foi instituída a política nacional de segurança das informações. Com esse ato normativo, o governo brasileiro despertou de vez para a necessidade de proteção de assuntos que mereçam tratamento especial, adotando medidas para prevenir o risco de sua vulnerabilidade. A administração pública, em todos os seus níveis e órgãos, processa informações consideradas "sensíveis", que requerem a proteção contra a intrusão e modificação desautorizadas. Assim, o estabelecimento de uma política de segurança do material informativo que é armazenado e documentado em seus sistemas de computação é de extrema importância.

A política (de segurança) da informação nos órgãos e entidades da Administração Pública Federal tem, nos termos definidos no Decreto, os seguintes objetivos (art. 3º):

a) dotá-los de instrumentos e recursos tecnológicos que os capacitem a assegurar a confidencialidade, a integridade e a autenticidade dos dados e informações classificadas como "sensíveis";
b) eliminar a dependência externa em relação a sistemas e equipamentos relacionados à segurança da informação;

c) promover a capacitação dos recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação;
d) promover a capacitação industrial do país com vistas à sua autonomia no desenvolvimento e na fabricação de produtos e serviços relacionados com a segurança da informação.

O uso e desenvolvimento de equipamentos dotados de recursos criptográficos também é a tônica das diretrizes da política nacional de segurança da informação. No inc. VII do art. 4º o Decreto chega a indicar que poderão ser estabelecidos padrões, níveis e tipos de métodos criptográficos a serem adotados pelos órgãos da administração, de modo a assegurar a confidencialidade e integridade dos documentos neles processados e arquivados. Já no inc. XIV, está indicada como meta a implementação de uma infra-estrutura de "chaves públicas" para serem utilizadas por todos eles. Além de estar regulamentada a realização de auditorias para aferir o nível de segurança dos respectivos sistemas de informação, também é previsto a emissão de "certificados de conformidade" (art. 2º, I, e 4º, XI), que representam a garantia formal de adequação dos equipamentos informáticos à política de segurança.

O Decreto atribui à Secretaria-Executiva do Conselho de Defesa Nacional a execução das diretrizes da política de segurança das informações, e inclusive cria um órgão especialmente encarregado de assessorá-la na consecução desse objetivo - o Comitê Gestor de Segurança da Informação, integrado por representantes de vários ministérios e do Gabinete de Segurança Institucional da Presidência da República.

Política de segurança das informações talvez seja hoje o principal ponto de preocupação dos governos nacionais. O Congresso dos EUA, por exemplo, editou uma lei proibindo as empresas privadas de comercializar tecnologia de criptografia sem prévia autorização. O setor privado hoje em dia, principalmente as grandes empresas nacionais e multinacionais, já adotaram sistemas criptográficos para garantir a segurança na transmissão e processamento das informações. Faltava no Brasil o estabelecimento de uma política global de informação, que impulsionasse a implementação da infra-estrutura de segurança nos órgãos públicos e a interoperabilidade entre os diversos sistemas informáticos.

3. INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA

O Instituto Nacional de Tecnologia da Informação ofertou ao Parlamento nacional, ao relator do Projeto Lei 7316/2002, deputado Jorge Bittar (PT/RJ), um substitutivo que será efetivamente uma Lei para o sistema nacional de certificação digital, a Infra-estrutura de chaves públicas do Brasil, a ICP-Brasil.

A ICP-Brasil implica o conjunto de técnicas, práticas e procedimentos, a ser implementado pelas organizações governamentais e privadas brasileiras, com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado na criptografia assimétrica (par de chaves pública e privada). A Medida Provisória 2.200/01 (1a. edição: 28/06/2001; 2a. edição: 27/07/2001 e 3a. edição: 24/08/2001) cria a "AC-Raiz" – Autoridade Certificadora Central, submetida ao Comitê Gestor da ICP-Brasil, com poderes para credenciar entidades certificadoras. Embora não seja negada validade a certificados emitidos por entidades não credenciadas, assinaturas eletrônicas produzidas sob a égide da ICP-Brasil terão presunção de veracidade com relação aos signatários, possibilitando plena atribuição de validade jurídica a documentos eletrônicos.

O sistema ICP-Brasil que hoje se encontra operacional e pronto para seu uso em nosso país é um sistema jurídico, econômico e tecnológico dependente de um cenário estável e de credibilidade.

Com certeza, o modelo jurídico-tecnológico presente neste Substitutivo não elide os debates que são tradicionais no tema da certificação digital. Apesar de seu caráter forçosamente técnico, ele sempre se mostrou repleto de polêmicas: a validade jurídica de documentos eletrônicos, identidade digital do ciber-cidadão, o "modelo de negócio" da certificação digital, o par assinatura digital versus assinatura tradicional, o tema do não-repúdio na vida jurídica, são alguns deles. Mas a publicação de uma Medida Provisória deu lugar a uma conjuntura ainda mais polêmica, pois desconsiderou o debate que então acontecia no Congresso Nacional e em geral na sociedade. Com uma Lei para a o sistema ICP-Brasil a sociedade poderá ajustar o modelo sob o impacto da evolução das técnicas, da descoberta de novas tecnologias e da evolução da própria sociedade brasileira. O jusfilósofo italiano Norberto Bobbio, após investigar com precisão o dogma do desejo de completude de um ordenamento jurídico, onde um Corpus juris é concebido sem lacunas. Termina por salientar: asseverar que "existem lacunas ideológicas em cada sistema jurídico é tão óbvio que não precisamos nem insistir. Nenhum ordenamento jurídico é perfeito, pelo menos nenhum ordenamento jurídico positivo" (Teoria do Ordenamento Jurídico, cap. IV, 6). O modelo que atualmente apresentdado não tem em absoluto a pretensão absurda de ser sem lacunas, mas, isto sim, reflete a situação concreta de um sistema preparado para ser o sistema nacional de certificação digital. Com a fusão da estabilidade jurídica e sua operação concreta em nosso país dará a tal sistema as condições institucionais para necessários acordos internacionais de certificação digital, principalmente com as nações do Mercosul e da Comunidade européia, já em curso de debate e negociação.

O eixo fundamental do Substitutivo em análise é: definição de assinatura eletrônica e certificados digitais, definição da infra-estrutura de chaves públicas brasileira, definição da prestação de serviços de certificação e, por fim, revoga a Medida Provisória 2.200, convalidando os atos praticados com base neste diploma legal.

Na definição de assinatura eletrônica e certificados digitais o Substitutivo produz definições em sintonia com as legislações internacionais, tal como a diretriz da Comunidade Européia, abandonando a expressão "autoridade certificadora" e adotando a nomenclatura "prestador de serviços de certificação". O Substitutivo também garante o mesmo valor probante e jurídico das assinaturas manuscritas à assinatura digital. Garantindo

expressamente a posse da chave criptográfica ao seu possuidor (art. 8ª, §2º), - é ele que irá gerar seu par de chaves e que ficará em sua posse.

Na definição da infra-estrutura de chaves públicas brasileira, o sistema ICP-Brasil, assegura-se um novo modelo para o Comitê Gestor da ICP-Brasil, definindo suas competências e sua governança. Redesenhando, por outro lado, o papel do Instituto Nacional de Tecnologia da Informação, sedimentando sua presença na política tecnológica do governo. O Substitutivo reconhece, no âmbito do sistema nacional de certificação digital, o papel de destaque do Observatório Nacional – órgão do Ministério da Ciência e Tecnologia, que mantém a hora legal brasileira, a sua importância na confiabilidade no sistema ICP-Brasil. Exigindo, posteriormente, no quadro das Resoluções da ICP-Brasil, o uso de protocolos abertos e universais nos serviços de sincronismo e carimbo de tempo.

Na definição da prestação de serviços de certificação o Substitutivo ao Projeto Lei torna o credenciamento à ICP-Brasil facultativo (Art. 25), tornando a prestação de serviço de certificação fora da ICP-Brasil sem a necessidade de "prévia autorização do Poder Público". Define com rigor os critérios de credenciamento na ICP-Brasil, assim como os critérios técnicos de segurança física e lógica vigentes no sistema. Assegura, por conseguinte, práticas eficazes de informação ao usuário do sistema sobre os efeitos da certificação na vida do cidadão, assim como cria todo um capítulo contemplando o "dever da informação". Outra urgente medida é uma gradação de penas para o sistema ICP- Brasil, criando diversas categorias de infração e penalidades no âmbito do sistema.

Enfim, revoga a Medida Provisória 2.200, convalidando os atos praticados com base neste diploma legal. O Substitutivo também normatizará o uso de certificados digitais da ICP-Brasil no âmbito da Administração Pública Federal.

O Projeto Lei, sobretudo, ao ser construído a partir de um modelo em pleno funcionamento em nosso país, tem como seu objetivo expresso a eficácia de seu modelo jurídico e tecnológico. Tal é agora o desafio que nos provoca: a eficácia de todo um sistema e sua formulação. Kelsen já ligara a eficácia do Direito ao "domínio da realidade"; Husserl, matemático e fenomenólogo, em sua obra póstuma, fundamentara a Ciência, assim como "todas as suas questões práticas e teóricas", no mundo-da-vida.

Nos últimos anos temos cada vez mais confiado em redes de informática, dispositivos digitais e seus bits. Confiança deverá ser no sistema ICP-Brasil entendido mais do que nunca como um valor objetivo, ou de possível objetivação, e não como algo psicológico ou meramente subjetivo. Fundamentando a ICP-Brasil em rigoroso processo de auditoria, baseando-a em regramento claro e tornado público, e decidido por um Conselho geral, o Comitê Gestor da ICP-Brasil. Sem nos esquecermos jamais na manutenção da interoperabilidade do sistema nacional de certificação digital e uso rigoroso de protocolos abertos e mantidos por consórcios abertos de empresas, comunidades ou governos.

Resumindo, a Política de Segurança Geral da ICP-Brasil tem como objetivos:

- Definir o escopo da segurança das entidades;
- Orientar, por meio de suas diretrizes, todas as ações de segurança das entidades, para
- reduzir riscos e garantir a integridade, sigilo e disponibilidade das informações dos
- sistemas de informação e recursos;
- Permitir a adoção de soluções de segurança integradas;
- Servir de referência para auditoria, apuração e avaliação de responsabilidades.

A Política de Segurança tem ainda como abrangência os aspectos de Requisitos de Segurança Humana, Requisitos de Segurança Física ,Requisitos de Segurança Lógica e Requisitos de Segurança dos Recursos Criptográficos.

3.1. O ITI - Instituto Nacional de Tecnologia da Informação

O Instituto Nacional de Tecnologia da Informação – ITI, autarquia federal vinculada à Casa Civil da Presidência da República, é a Autoridade Certificadora Raiz – AC Raiz da Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil.

Como tal é a primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, e tem por competências emitir, expedir, distribuir, revogar e gerenciar os certificados das Autoridades Certificadoras - AC de nível imediatamente subseqüente ao seu; gerenciar a lista de certificados emitidos, revogados e vencidos; executar atividades de fiscalização e auditoria das AC, das Autoridades de Registro - AR e dos prestadores de serviço habilitados na ICP-Brasil.

Compete ainda ao ITI estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico voltados à ampliação da cidadania digital. Neste vetor, o ITI tem como sua principal linha de ação a popularização da certificação digital e a inclusão digital, atuando sobre questões como sistemas criptográficos, software livre, hardware compatíveis com padrões abertos e universais, convergência digital de mídias, entre outras.

3.2. Algumas Legislações Importantes para ICP

Segue abaixo algumas resoluções, leis e decretos pertinentes à Insfra-estrutura de Chaves Públicas, e importantes para a questão de segurança da informação,

- Resolução Nº 31, de 29 de janeiro de 2004: Altera os Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil e os Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil;
- Resolução Nº 29, de 29 de janeiro de 2004: Designa Comissão para realizar auditoria pré-operacional da AC Raiz;
- Resolução Nº 28, de 11 de novembro de 2003: Altera a Resolução nº 7, de 12 de dezembro de 2001, que aprova os requisitos mínimos para políticas de certificado da ICP-Brasil;

- Resolução Nº 26, de 24 de outubro de 2003: Altera os Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil, os Requisitos Mínimos para as Políticas de Certificado na ICP - Brasil e os Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP – Brasil;
- Resolução Nº 25, de 24 de outubro de 2003: Aprova os procedimentos a serem adotados pelo Instituto Nacional de Tecnologia da Informação - ITI na sua atividade de fiscalização;
- Resolução Nº 24, de 29 de agosto de 2003: Estabelece critérios para cadastramento e autorização de empresas de auditoria especializada e independente no âmbito da InfraEstrutura de Chaves Públicas Brasileira - ICP-Brasil
- Resolução Nº 21, de 29 de agosto de 2003: Altera a Declaração de Práticas de Certificação da AC - Raiz da ICP - Brasil, os Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP - Brasil, os Requisitos Mínimos para as Políticas de Certificado na ICP - Brasil e os Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP – Brasil;
- Resolução Nº 20, de 08 de maio de 2003: Determina o desenvolvimento de uma plataforma criptográfica aberta, voltada à operação da AC Raiz;
- Resolução Nº 16, de 10 de junho de 2002: Estabelece as diretrizes para sincronização de freqüência e de tempo na Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil;
- Resolução Nº 13, de 26 de Abril de 2002: Altera a declaração de práticas de certificação da AC Raiz da ICP-Brasil, os critérios e procedimentos de credenciamento das entidades integrantes da ICP-Brasil, os requisitos mínimos para as declarações de práticas de certificação das autoridades certificadoras da ICP-Brasil, os requisitos mínimos para as políticas de certificado na ICP-Brasil, e dá outras providências;
- Resolução Nº 10, de 14 de Fevereiro de 2002: Estabelece as diretrizes da política tarifária da Autoridade Cerificadora Raiz - AC Raiz da ICP-Brasil;
- Resolução Nº 8, de 12 de Dezembro de 2001: Aprova os requisitos mínimos para as declarações de práticas de certificação das autoridades certificadoras da ICP-Brasil;
- Resolução Nº 7, de 12 de Dezembro de 2001:Aprova os requisitos mínimos para políticas de certificado na ICP-Brasil;
- Resolução Nº 6, de 22 de Novembro de 2001: Aprova os critérios e procedimentos de credenciamento das entidades integrantes da ICP-Brasil;
- Decreto Nº 4.414, de 07 de outubro de 2002: Altera o Decreto no 3.996, de 31 de outubro de 2001, que dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal;
- Decreto Nº 3.996, de 31 de outubro de 2001: Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal;
- Decreto Nº 3.505, de 13 de junho de 2000: Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;
- Medida Provisória Nº 2.200-2, de 24 de Agosto de 2001:Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências.

4. O GRUPO DE SEGURANÇA DA INFORMAÇÃO

A Câmara Técnica dos Serviços de Rede do Poder Executivo Federal, órgão colegiado, diretamente subordinado ao Secretário de Logística e Tecnologia da Informação do Ministério de Planejamento, Orçamento e Gestão criou o Grupo de Segurança da Informação. No Ano 2000, esse grupo foi consolidado no Comitê Gestor de Segurança da Informação, CGSI.

O Grupo de Segurança da Informação, GSI, foi criado com os seguintes objetivos:

a)Apresentar um conjunto de recomendações mínimas para a implementação, no âmbito da Rede Governo, de uma Política de Segurança; – essa proposta foi apresentada e já publicada no Diário Oficial da União (Decreto No 3.505, de 13 de Junho de 2000), que instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

b) Apresentar uma proposta para adoção de Infra estrutura de Chave Pública (ICP-GOV ou PKI), com seus mecanismos, ferramentas e aplicações associadas; Esse proposta consistiu no DECRETO Nº 3.587, DE 5 DE SETEMBRO DE 2000, que estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal - ICP-Gov. O prazo para apresentação da proposta de regulamentação da ICP-GOV, previsto nesse decreto, foi cumprido.

A Infra-estrutura de Chaves Públicas do Poder Executivo Federal - ICP-Gov é constituída de um conjunto de regras de segurança para a tramitação, certificação e autenticação de documentos eletrônicos. Esse conjunto de regras estabelece, entre outras coisas, os critérios padrões para a classificação das informações em cinco níveis de segurança, do ultra-secreto ao ostensivo. Para a especificação e aplicação desses padrões, estão sendo implantados os diversos componentes da ICP-Gov: a política de certificação, a arquitetura das chaves públicas, as atribuições e estrutura da autoridade gerenciadora e das autoridades certificadoras, os protocolos de segurança e padrões técnicos a serem adotados.

A implantação dessa infra-estrutura deverá permitir aos órgãos públicos ampliar a prestação de serviços e garantir a segurança da circulação de informações e documentos em meio eletrônico. Não há custos diretos envolvidos. A futura implantação das estruturas das Autoridades Certificadoras dependerá de recursos orçamentários e financeiros específicos. A ICP-Gov implantada inicialmente no âmbito do Governo Federal, futuramente deverá

interagir com outras infra-estruturas de chaves públicas, dos Poderes Judiciário e Legislativo, além de outros níveis de Governo.

O Comitê Gestor de Segurança da Informação, CGSI, vinculado ao Conselho de Defesa Nacional, é o encarregado de coordenar os trabalhos de concepção, especificação e implementação da ICP-Gov. Essa proposta está em conformidade com os padrões internacionais, o que garante amplas possibilidades de interação com as soluções adotadas por outros países, tendo em vista a perspectiva de expansão das atividades de e-business.

As medidas representam impulso significativo ao estabelecimento da base legal necessária à regulamentação do uso da tecnologia da informação. A ativa participação do Governo Federal nessa questão representa também um grande incentivo aos negócios e transações eletrônicas e à própria Administração Pública, na prestação de serviços ao cidadão.

5. A INTERNET E OS TRIBUNAIS

O Brasil já conta com aproximadamente 15 milhões de internautas e previsões de movimentar bilhões no comércio eletrônico. Estudos concluem que a presença virtual pode significar a sobrevivência do próprio negócio. Para o consumidor estima-se que as compras pela internet chegam a ser 15% mais baratas que as demais. Para o fornecedor, a redução dos custos associados à estrutura de vendas podem ser até 80% menores. Além disso, surge uma nova modalidade de transações, as chamadas business to business (b2b), possivelmente o carro chefe do comércio eletrônico, principalmente se considerarmos os valores envolvidos. É de suma importância ressaltar a aplicação das disposições do Código de Proteção e Defesa do Consumidor (Lei 8078/90), inclusive nas operações b2b, desde que o adquirente seja o destinatário final do produto ou do serviço.

A dependência do mundo virtual é inevitável. Grande parte das tarefas do nosso dia a dia são transportadas para a rede mundial de computadores, ocasionando fatos e suas conseqüências, jurídicas e econômicas, assim como ocorre no mundo físico. A questão que surge é relacionada aos efeitos dessa transposição de fatos, basicamente a sua interpretação jurídica. Como exemplo, podemos citar a aplicação das normas comerciais e de consumo nas transações via internet (responsabilidade perante o Código do Consumidor), a questão do recebimento indesejado de mensagens por e-mail (spam), a validade jurídica do documento eletrônico, o conflito de marcas com os nomes de domínio, a propriedade intelectual e industrial, a privacidade, a responsabilidade dos provedores de acesso, de conteúdo e de terceiros na web e os crimes de informática.

A legislação brasileira pode e vem sendo aplicada na maioria dos problemas relacionados à rede. Para questões específicas e controvertidas, como aquelas citadas, existem projetos de lei em tramitação, os quais devem objetivar a complementação e adequação como princípios fundamentais, sob pena de uma inflação legislativa desnecessária. Acrescente-se que diversas nações possuem regulamentação sobre os temas, destacando-se os Estados Unidos, membros da União Européia, Canadá, Colômbia, Itália, Alemanha e Portugal. No Brasil, ainda que de forma embrionária, destacamos a recente Lei nº 9.800/99 permite o envio de petições via e-mail ao Poder Judiciário, observados certos requisitos e a Lei nº 9983/00, que tipifica condutas criminosas quanto à prejuízos aos sistemas informatizados da Administração Pública.

Questão de extrema relevância é a da validade do documento eletrônico. Basta afirmar que uma simples mensagem enviada por e-mail dificilmente tem plena validade jurídica, equiparando-se a prova oral. Isso porque, em tese, por meio de recursos técnicos, é possível alterar documentos digitais sem deixar vestígios. Por outro lado, através da técnica da certificação eletrônica, é possível garantir a autenticidade e a veracidade de um documento eletrônico e, por conseqüência, atribuir validade jurídica ao mesmo. A certificação eletrônica mais comum é aquela por meio da utilização de chaves públicas (assinatura digital por criptografia assimétrica) é, em síntese, uma codificação, garantida e atribuída por uma terceira pessoa (certificador), representada por um certificado (software) que identifica a origem e protege o documento de qualquer alteração sem vestígios. Por isso, aqueles que dispõem da assinatura digital já podem efetuar troca de documentos e informações pela rede com a devida segurança física e jurídica.

Outro assunto interessante é o recebimento de mensagens indesejadas ou não solicitadas, mais conhecido como "spam". O Projeto de Lei nº 1589/99 eo 2358/00 tratam do assunto, dispondo que aqueles que praticarem essa conduta deverão informar o caráter da mensagem, sob pena de multa (PL 2358). Os países da União Européia deverão ter registros específicos para esse tipo de correspondência. Nos Estados Unidos, aquele que proceder como "spamer" poderá ser condenado civil (multas de US$ 500 a 25,0000) e criminalmente. Independentemente de normas especiais, no Brasil, aquele que enviar "spam" poderá ser responsabilizado nos termos das leis em vigor, desde que haja a efetiva demonstração do prejuízo causado.

No tocante as marcas registradas, notórias, nomes comerciais ou próprios que conflitam com nomes de domínios de sites na internet, a questão é controvertida, porém a tendência é a proteção ao detentor da marca. Deve-se destacar que, em 1995, a International Trade Mark Association reconheceu a identidade da marca ao nome de domínio. Além disso, jurisprudência francesa e americana tendem nesse entendimento. Merecem destaque, também, as primeiras decisões judiciais brasileiras nesse contexto: a 14ª Câmara do Tribunal de Justiça do Rio Grande do Sul concedeu o direito de uso do domínio "rider.com.br" ao detentor da respectiva marca; no mesmo entendimento foi a decisão da 2ª Câmara do Tribunal de Justiça do Paraná quanto ao domínio "ayrtonsenna.com.br". Para litígios decorrentes de domínios de primeiro nível ".com", várias são as decisões arbitrais proferidas pela WIPO Arbitration Center, também, em sua maioria, favoráveis aos respectivos proprietários das marcas.

Outro fator que não pode ser deixado de lado é a problemática da segurança no mundo virtual, que merece atenção destacada. Aproximadamente 1/3 das empresas brasileiras já foram atacadas por hackers. Os efeitos decorrentes desse aspecto ensejam a busca pela responsabilidade do ato danoso, seja na esfera criminal ou na cível, justificando, também, a preocupação com a discussão e debate do assunto, propondo, inclusive, a necessidade de regulamentação complementar.

As relações virtuais e seus efeitos são realidade. A tendência é a substituição gradativa do meio físico pelo virtual ou eletrônico, o que já ocorre e justifica a adequação, adaptação e interpretação das normas jurídicas nesse novo ambiente. Na grande maioria dos casos é possível a aplicação das leis existentes o que gera direitos e deveres que deverão ser exercidos e respeitados. Assim, de rigor e imprescindível o estudo, orientação e aplicação da internet como ambiente de resultados legais sérios e com enorme potencial de efeitos jurídicos, como, por exemplo, a possibilidade, desde já, da assinatura digital de contratos eletrônicos entre as partes com segurança muitas vezes superior àquela utilizada no meio físico.

6. CONTRATOS ELETRÔNICOS

Empresários que desejam realizar contratos de alto valor por meio eletrônico devem aguardar a edição final da regulamentação da Medida Provisória n° 2.200, de acordo com o advogado Renato Opice Blum, presidente do Comitê de Direito de Tecnologia, para garantir a validade jurídica de documentos eletrônicos.
A MP n° 2.200 foi publicada, entrou em vigor no mesmo dia e está aberta a consulta pública até 23 de julho. Pela MP, um documento só terá sua validade jurídica comprovada se possuir assinatura digital certificada por uma autoridade que, por sua vez, deve ser licenciada pelo Comitê Gestor da ICP-Brasil. “Essa estrutura ainda não existe e não há como se precaver em caso de problemas na Justiça”, disse Blum. Antes da MP, as empresas podiam apresentar documentos eletrônicos simples ou contratar uma certificadora privada.

A publicação da medida provisória se sobrepôs ao trabalho da comissão da Câmara dos Deputados que discutia o substitutivo ao projeto de lei n° 1.483, sobre a validade jurídica do documento eletrônico e da assinatura digital. Para Blum, o substitutivo elaborado pelo deputado Julio Semeghinié melhor do que a MP. “O texto não exclui a validade de documentos eletrônicos que sem assinatura digital e não determina uma centralização das operações no governo federal, como faz a MP, ato que considero arriscado.”

Caso não haja acordo para fundir os termos de cada texto e aprovar uma lei só, espera-se que o substitutivo continue em tramitação e, quando aprovado, revogue a medida provisória nos itens que forem conflitantes.

7. CARTÓRIO ELETRÔNICO

A advogada Mariza Delavieve Rossi, do escritório Ulhôa Canto, Rezende e Guerra Advogados, apresentou o projeto de lei 1.589, do deputado Luciano Pizzatto (PFL-PR) e chamou a atenção para o fato de ele prever a criação da atividade cartorial eletrônica – sistema de autenticação de documentos que transitam via web, a ser feita por tabeliães previamente certificados e com atividade regulada pelo Poder Judiciário. O projeto de lei tem nove capítulos e 52 artigos e seu propósito é instituir a fatura e a assinatura digital nas transações eletrônica.

8. ASPECTOS DA RESPONSABILIDADE CIVIL PELA GUARDA DA INFORMAÇÃO

Não é pelo fato de estarem relacionadas ao ambiente dito virtual, que a segurança, a guarda, o uso e a manutenção da informação são obrigações de menor poder coercitivo, na forma da lei Ao contrário, estão sujeitas, inclusive, às sanções cabíveis, caso haja descumprimento. Muito embora o tema reclame e justifique exaustivo trabalho específico, não se pode deixar de traçar algumas considerações fundamentais.

Como já dito, alguns países já decidiram definir tipos penais a partir dos quais pretendem punir as práticas infracionais consideradas mais danosas. O Brasil ainda não dispõe de tal texto legal. O crime aqui praticado só poderá encontrar óbice e sanção jurídica se já estiver definido como tipo penal, sendo a tecnologia apenas o meio mediato – e ainda assim se o tipo não previr, expressamente, um outro meio – utilizado para a consecução do resultado.

Ainda assim, a responsabilidade civil pelo fato ou pelo dano causado à informação é imputável ao causador do resultado maligno, em virtude da possibilidade da aplicação analógica da lei cível, desde que obedeça aos pressupostos caracterizadores já familiares ao instituto: uma ação, ou uma omissão, que, mediante um liame ou nexo de causalidade, importe em um resultado danoso, mediante culpa do agente.

Todas as relações jurídicas, e, por conseqüência, todos os agentes envolvidos e relacionados à guarda e à manipulação da informação estão sujeitos a responder civilmente por suas ações ou omissões. O incipiente estado de definições técnico-jurídicas, no entanto, restringe sensivelmente a chegada da tal matéria às cortes do país, à exceção de alguns poucos leading cases, que começam a escrever a história jurisprudencial da matéria.

Os ataques e invasões a sistemas de informação, segundo observação anterior, são passíveis de responsabilização no plano cível, à medida em que causem dano efetivo, assegurada a reparação do dano moral, e desde que o invasor ou agressor possa ser individualizado. Ora, não é necessário muita reflexão para entender que, com a garantia do direito à privacidade, aliada às limitações técnicas existentes, o rastreamento efetivo do responsável por um ataque é tarefa extremamente árdua, embora não impossível. Técnicas de tracking estão sendo desenvolvidas e grupos especiais do órgão competente, neste caso, a polícia, estão sendo treinados para lidar com a nova realidade que se lhes apresenta. Divisões de Alta Tecnologia já são uma realidade em muitas forças policiais no país e no exterior.

Em relação a serviços prestados pelas empresas, a responsabilização civil é tarefa menos abstrata. Isto porque os sujeitos da relação estão claramente definidos, dependendo o surgimento da obrigação de composição do dano apenas da prova do resultado daninho, do nexo de causa e da culpa.

Provedores de acesso, são agentes diretamente expostos a estas questões. Na maior parte das situações, suas ações estão relacionadas à aplicação da teoria da culpa, sendo essencial que se

demonstre, efetivamente, a existência de imprudência, negligência ou imperícia para a responsabilização civil.

Quanto à divulgação de conteúdo, cabe deliberar a respeito da responsabilidade civil do provedor de acesso. A ser obedecido o direito estrito à privacidade, nenhuma atitude pode tomar o provedor com relação à informação que trafega pelo seu domínio, quando for apenas o intermediário, o meio técnico. Assim sendo, existe vedação inclusive constitucional à sua intervenção na esfera privada do sujeito.

Outro norte toma a discussão quando o provedor edita o dito conteúdo. Neste caso, há responsabilidade direta pela informação veiculada ou produzida. Analogamente, pode-se dizer que, ao tomar conhecimento de transmissão ou divulgação de informação manifestamente indevida ou imprópria, o provedor torna-se solidariamente responsável, devendo adotar as providências técnicas cabíveis para fazer cessar a irregularidade.

Havendo a presença do consumidor em um dos pólos da relação jurídica, desaparece, por comando legal do Código Brasileiro de Defesa do Consumidor, a necessidade de caracterização da culpa, surgindo a chamada responsabilidade objetiva ou sem culpa.

A segurança da continuidade de acesso, por exemplo, assemelha-se ao serviço prestado pela concessionária de serviços públicos, sendo o provedor responsável pela estrutura externa e o consumidor pela interna. Aplicável a teoria do risco, através da qual o provedor, razoavelmente observado o estágio de desenvolvimento da tecnologia disponível, assume o risco de sua atividade econômica, obrigando-se a ressarcir o eventual prejuízo direto daí advindo, bem como a reparar o dano decorrente.

As demais empresas que operam na Internet também estão sujeitas a estabelecer relações de consumo, no que devem obedecer às mesmas regras. Os procedimentos utilizados no comércio pela Internet são exatamente os mesmos verificados no comércio tradicional, verificando-se tão somente alteração na forma e nos mecanismos de contratação, através do desenvolvimento de novas tecnologias.

Uma última observação cabe a respeito da diferenciação entre os danos oriundos das falhas de segurança em sistemas de informação desenvolvidos sob medida e em aplicativos denominados de prateleira, de consumo de massa. Há que se observar que, enquanto estes estão diretamente relacionados ao consumidor final, aqueles podem ser caracterizados como insumos de produção, vez que sua destinação final, não raro, é a utilização comercial, empresarial do software. Daí decorre que o tratamento e as soluções legais devem ser diferenciadas, valendo, em regra, as normas de defesa do consumidor para o software de massa e as eventuais cláusulas contratuais para produtos on demand.

9. CRIMES VIRTUAIS – ASPECTOS JURÍDICOS

Assim como o direito, a nossa língua sofre uma influência natural das transformações atuais, bastanto para comprovar, perguntar a alguém se já tomou conhecimento do que venha a ser um Hackers, ou seja, indivíduos que possuem conhecimentos específicos e aprimorados no setor informático, cuja essência de vida deste indivíduo é vagar pela internet "invadindo" computadores alheios, tanto o é, que consta no Dicionário Aurélio a definição do que seja hackers dispondo que é o "Indivíduo hábil em enganar os mecanismos de segurança de sistemas de computação e conseguir acesso não autorizado aos recursos destes, ger. a partir de uma conexão remota em uma rede de computadores; violador de um sistema de computação".
Dentre os delitos perpetrados por estes, podemos citar as constantes investidas as contas bancárias alheias, desviando seus valores para contas fantasmas de amigos ou próprias e, nessa mesma linha de delitos um dos mais usuais delitos dessa natureza que é a "invasão" de computadores particulares com o intuito de ler os chamados e-mails.

Diante da popularização e do fácil acesso ao microcomputador, é que muitos indivíduos utilizam a INTERNET (jovens na sua maioria, entre 15 e 20 anos) como meio para praticar delitos das mais variadas espécies, causando enormes prejuízos a Bancos ou Instituições financeiras através de desvios em seu erário, bem como divulgando material pornográfico ou de caráter discriminatório.

Destaca-se, então, com grande importância, a necessidade de discussões sobre o ajustamento da norma penal em face dos crimes virtuais e sua repercussão em âmbito jurídico.
Para se aplicar a devida sanção penal, deve se ter fixo um sujeito infrator, um dos elementos intrínsecos da ação. O direito penal não pode alcançar pessoas abstratas, virtuais. Não podemos, na sanha de condenar, aplicar a sanção penal aquele que pela sua conduta não concorreu de qualquer modo para a caracterização do evento criminoso.
Diante deste fato é que os crimes perpetrados neste ambiente se caracterizam pala ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas.

Não basta, para a aplicação da sanção penal, o conhecimento superficial sobre a identidade do acusado, não se trata de homonímia, mas da comprovação de que aquele que se figura como imputado realmente praticou o que lhe é imputado. Tendo como norte o caráter virtual deste meio, as transações e ingressos na internet são realizados por meios de chaves, códigos formulados através da criptografia.

Nem sempre o Direito acompanha a evolução da sociedade e à medida que esta evolui, reclama por parte deste, novas formas de procedimentos e novos tipos legais que ampare e, resguarde os frutos oriundos desta evolução.

O direito, apesar de esforça-se para acompanhar a evolução da sociedade, carece de meios que ilida condutas atentatórias contra as normas penais constantes do nosso modelo legal atual.

O cerne da questão se prende ao fato de que é princípio penal básico que não há crime sem lei anterior que assim o defina. Tal principio encontra-se esculpido no art. 5.°, inc. XXXIX, da Constituição Federal de 1988 nestes termos:

“ Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade...”

É diante deste princípio que só há conduta considerada como criminosa para efeito penal, se a mesma vier expressamente definida neste sentido. Não se pode aplicar a norma penal por analogia, devendo este princípio ser observado friamente, sob pena de se praticar uma coação ou constrangimento ilegal.

Tramitam, no Congresso Nacional, vários projetos de lei no sentido de classificar as condutas consideradas criminosas por meio da INTERNET, bem como a sua correta utilização. Entre eles, destaca-se o Projeto de Lei n.º 64/99 de autoria do Deputado Federal Luiz Piauhylino, cujo trabalho fora herdado de seu antecessor o Deputado Federal da bancada paraibana Cássio Cunha Lima, pioneiro nesta preocupação, tal PL dispõe sobre a "cyber - criminalidade", ou seja, os crimes praticados na área da informática, disciplinando, discriminando e atribuindo penalidades a tais condutas.

Devido à ausência de tipificação legal, discriminante das condutas dos agentes que utilizam a INTERNET como instrumento na prática de delitos, tal vácuo legal, encoraja o surgimento de novos delitos neste meio tecnológico.

Enquanto houver por parte da legislação penal tal omissão, não serão considerados crimes, como de fato são. Destarte, seus agentes sempre serão agraciados com o benefício da impunidade, pois no direito penal não se pode atribuir uma pena, ou impor uma sanção, a uma conduta que o ordenamento penal não considere expressamente como criminosa, mesmo que tal conduta produza prejuízos financeiros ou atente contra a integridade humana, bens resguardados pelo direito penal.

9.1. Delegacias Virtuais

A Delegacia Virtual atua de duas formas. Na maioria dos casos, ela distribui, em tempo real, informações para as outras delegacias, segundo o tipo de delito ou o local em que este ocorreu. Desse modo, ela elimina o desconforto do cidadão, reduz a burocracia e aumenta a velocidade de resposta da Polícia.

Mas há uma circunstância em que a Delegacia Virtual tem uma função especializada. É o caso dos crimes cometidos por meio de computadores ligados à Internet - os chamados "delitos eletrônicos", muitos deles nem mesmo previsto na legislação. Estes incluem desde a simples "invasão" da privacidade de um microcomputador de uso pessoal até o acesso a informações sigilosas do Governo ou de empresas privadas e a transferência indevida de fundos bancários, passando pela clonagem de cartões de crédito, a divulgação de pornografia infantil e o incitamento à intolerância e ao ódio a determinados segmentos sociais. A Delegacia Virtual vai prevenir e combater esses crimes de várias maneiras. Uma delas é divulgando informações para que o próprio cidadão possa defender-se. Outra, é investigando e rastreando suspeitos para que sejam processados. E até apresentando propostas de legislação para que se possa enquadrar e punir esses criminosos.

Embora tenha como alvo principal o cidadão, a Delegacia Virtual possui também uma importante clientela "interna": a própria Polícia. Esta passa a contar com um poderoso instrumento para aumentar a sua agilidade e eficiência. E, ao melhorar o atendimento que presta ao cidadão, o policial vai aumentar o respeito que a sociedade tem por ele, e também a sua própria auto-estima. Tudo isso cria um círculo virtuoso, com o cidadão mais estimulado a colaborar com as autoridades na prevenção e no combate ao crime. Uma responsabilidade que, afinal, deve ser de toda a sociedade.

10. e-Direito

São tantas as formas de crimes virtuais que a Internet mais parece um território sem lei. Os juristas se mostram divididos. Há quem defenda a idéia de que a tecnologia não muda o Direito e por isso a Internet não precisa de uma legislação específica. Mas também existem os defensores do “e-Direito”, ou seja, da adaptação da lei para pôr ordem no ciberespaço.

Alguns juristas se enquadram no primeiro grupo. Para eles, todos os crimes cometidos através da Internet, ainda que transcendam a esfera do direito autoral, estão previstos nas leis do Brasil. Eles acham que as instituições do Direito são capazes de regular todo e qualquer avanço da tecnologia. Ainda acham que não faltam leis, mas sim meios de garantir seu cumprimento, como por exemplo: capacitação dos policiais e preparação das delegacias para lidar com novas tecnologias.

Uma das únicas alterações aceitas na lei por este grupo diz respeito ao conceito de furto presente no Código Penal. De acordo com a lei, o furto só se caracteriza se um objeto for removido, surrupiado. Mas, no caso de invasões de hackers a redes internas, os dados são roubados mesmo sem sair do HD das máquinas.

Já outro grupo de juristas discorda do exposto. Eles acreditam que para a punição dos crimes, é necessária certeza legal, ou seja, o crime deve estar previsto na lei. A legislação atual só se aplica para crimes virtuais se a Internet for usada apenas como meio. Mas quando a Internet também é o fim, então faz-se necessária uma regulamentação diferenciada. Eles defendem ainda que enquanto não houver crime específico que proteja o dado e a informação como um todo dentro de um sistema de informática, não se pode falar que tudo já é punível.

11. CONCLUSÃO

Sem dúvida, existe hoje uma quantidade considerável de ameaças à privacidade do indivíduo, ao intercâmbio eletrônico seguro e confiável de dados, e, por conseguinte, ao desenvolvimento eficiente das relações comerciais e empresariais.

Portanto, discussões devem ser realizadas a respeito dos efeitos jurídicos e da adequação das normas propostas à esta realidade, sendo absolutamente natural o aprimoramento e a atualização periódica da legislação que regulamenta a segurança da informação, instrumentos sem os quais a proteção à privacidade e à segurança dos dados e da informação corporativa será improdutiva.

O domínio da segurança da informação fatalmente se constituirá em instrumento de imensa vantagem política e econômica, cabendo certamente ao direito um papel fundamental no sentido de disciplinar e estabelecer limites a esta desmedida vantagem, de impedir desequilíbrios flagrantes e injustos e de dar contornos menos sombrios ao lema que acompanha a sociedade da informação.

12. BIBLIOGRAFIA

[1] CORRÊA, Gustavo Testa. Aspectos Jurídicos da Internet. São Paulo: Saraiva, 2000.

[2] GONÇALVES, Maria H. B. e outros. Ética e Trabalho, Ed. Senac Nacional, Rio de Janeiro, 1997.

[3] ELIAS, Paulo Sá. Alguns aspectos da informática e suas conseqüências no Direito. Jus Navigandi, Teresina, a. 4, n. 44, agosto/2000. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=1762>. Acesso em: 20/outubro/2004.

[4] GOUVEIA, Sandra. O Direito na era digital – Crimes Praticados por meio da Informática. Rio de Janeiro: Mauad, 1997.

[5] GRECO, Marco Aurélio. Internet e Direito. São Paulo: Dialética, 2000.

[6] REIS, Maria Helena Junqueira. Computer Crimes – A criminalidade na era dos computadores. Belo Horizonte: Del Rey, 1997.