O Brasil contra o Cibercrime

(PLC 89 de 2003, PLS 76 de 2000, PLS 137 de 2000 – Crimes de Informática)

Começa comentando sobre a Lei do Software de 1987 e sua consolidação de 1998, descreve resumidamente os cinco projetos de lei mais característicos em andamento no Senado, descreve o PLC 89 de 2003, passa a descrever detalhadamente o PLS 76 de 200 que está apensado ao PLC89 de 2003 junto com o PLS 137 de 2000 e encerra comparando as disposições do PLS 76 de 2000 às recomendações da Convenção sobre o Cibercrime de 2001 do Conselho da Europa e a *Directiva* 2006/04 do Parlamento Europeu.

Quanto à tramitação, a Comissão de Educação (CE) do Senado Federal aprovou em 20 de junho de 2006 o Parecer do Senador Eduardo Azeredo ao Projeto de Lei do Senado (PLS) nº 76 de 2000 de autoria do Senador Renan Calheiros, apensado ao Projeto de Lei da Câmara (PLC) 89 de 2003 de autoria do Deputado Luiz Pihauylino e ao PLS 137 de 2000 do Senador Leomar Quintanilha.

O PLS 76, com as emendas propostas no Parecer à Comissão de Cosntituição e Justiça(CCJ), altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) e o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 9.296, de 24 de julho de 1996, o Decreto-Lei nº 3.689, de 3 de outubro de 1941, (Código do Processo Penal), a Lei nº 10.446, de 8 de maio de 2002 (Lei da Repressão Uniforme a Crimes Interestaduais e Internacionais) e a Lei 8.078 de 11 de setembro de 1990 (Código do Consumidor), para tipificar condutas realizadas mediante uso de rede de computadores ou internet, ou que sejam praticadas contra sistemas informatizados e similares, e dá outras providências.

O PLC 89 tem sua origem em 1996, dez anos atrás, foi aprovado na Câmara dos Deputados e depois na Comissão de Educação do Senado Federal. Iria à sanção presidencial mas como o PLS 76 era mais abrangente foi a ele apensado dentro dos procedimentos regimentais do Senado Federal.

O Senador Eduardo Azeredo, relator do PLC 89 e também do PLS 76 houve por bem aproveitar os três projetos de lei em um Substitutivo que foi aprovado na Comissão de Educação do Senado. O PLS está agora na Comissão de Constituição e Justiça (CCJ) e depois será apreciado em Plenário do Senado, daí seguindo à Câmara, caso aprovado.

BREVE RESUMO DO SUBSTITUITVO DO PLS À CCJ DO SENADO

O PLS define para efeito do Código Penal o que é dispositivo de comunicação, sistema informatizado, rede de computadores ou internet, identificação de usuário e autenticação de usuário e provedor de acesso e de serviço.

Altera o art. 2º da Lei nº 9.296, de 24 de julho de 1996, para determinar que a exigência de pena de reclusão não se aplica quando se tratar de interceptação do fluxo de comunicações em dispositivo de comunicação ou sistema informatizado ou rede de computadores ou internet.

Inclui o inciso IV ao art. 313 do Decreto-Lei nº 3.689, de 3 de outubro de 1941, Código do Processo Penal (CPP) que passa admitir a decretação da prisão preventiva nos crimes punidos com detenção, se tiverem sido praticados contra rede de computadores ou internet, dispositivo de comunicação ou sistema informatizado, ou se tiverem sido praticados mediante uso de rede de computadores ou internet, dispositivo de comunicação ou sistema informatizado.

Define que a pena de alguns crimes tipificados é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso. E ainda que a pena dos crimes de calunia, injúria e difamação aumentam-se de dois terços caso os crimes sejam cometidos por intermédio de dispositivo de comunicação ou sistema informatizado.

Os crimes tipificados são:

- Dano por difusão de vírus eletrônico ou digital;
- Acesso indevido a dispositivo de comunicação
- Obtenção, guarda, e fornecimento de informação eletrônica ou digital obtida indevidamente ou não autorizada
- Violação e divulgação não autorizada de informações depositadas em banco de dados
- Não guardar os dados de conexões realizadas em rede de computadores ou internet
- Permissão, com negligência ou dolo, do acesso a rede de computadores por usuário não identificado e não autenticado
- Atentado contra a segurança de serviço de utilidade pública
- Interrupção ou perturbação de serviço telegráfico, telefônico ou de rede de computadores ou internet
- Difusão maliciosa de código – (phishing)
- Falsificação de cartão de crédito ou débito ou qualquer dispositivo eletrônico ou digital portátil de armazenamento e processamento de informações
- Falsificação de telefone celular ou meio de acesso a sistema eletrônico ou digital
- Furto qualificado com uso de dispositivo de comunicação, sistema informatizado ou rede de computadores ou internet

O PLS equipara à "coisa" o dado ou informação em meio eletrônico ou digital, a menor quantidade de informação que possa ser considerada como tal, a base de dados armazenada em dispositivo de comunicação e o sistema informatizado, a senha ou qualquer meio que proporcione acesso aos mesmos e desta forma o Código Penal passa a ter na sua abrangência estes elementos virtuais, ou seja, qualquer outro crime não específico como furto de senha, fraude de informações etc passam a ser abrangidos pelo Código Penal.

A fim de que se tenha sucesso contra os que acessam indevida ou criminalmente uma rede de computadores fez-se consenso sobre a necessidade de identificar-se e cadastrar-se o usuário naquele que torne disponível este acesso sob sua responsabilidade. Assim somente será admitido como usuário, pessoa natural, dispositivo de comunicação ou sistema informatizado que for autenticado por meio hábil e legal à verificação positiva da identificação de usuário, ficando facultado o uso de tecnologia que garanta a autenticidade e integridade dos dados e informações digitais ou o uso de outras entidades de dados de identificação de usuário já existentes e que tenham sido constituídas de maneira presencial.

A identificação do usuário de rede de computadores poderá ser definida nos termos de regulamento, sendo obrigatórios para a pessoa natural os dados de identificador de acesso, senha ou similar, nome completo, data de nascimento e endereço completo e sendo obrigatória para os dispositivos de comunicação e sistemas informatizados a indicação de uma pessoa natural responsável.

O objetivo da identificação e autenticação é prover a autenticidade das conexões, a integridade dos dados e informações e a segurança das comunicações e transações na rede de computadores, dispositivos de comunicação e sistemas informatizados.

Foi definida uma fase de transição de cento e vinte dias após a entrada em vigor da Lei para que os atuais usuários tenham como providenciarem ou revisarem sua identificação e cadastro junto a quem, de sua preferência, torne disponível o acesso aqui definido.

E mais, o PLS prevê que o cadastro de identificação, a critério daquele que torna disponível o acesso, possa ser obtido mediante o uso de cadastros que já tenham sido constituídos de maneira presencial, que é o caso das empresas, bancos, órgãos públicos e provedores de acesso profissionais.

Assim a enorme maioria dos usuários de rede de computadores já se encontra cadastrada, porque o fazem a partir de computadores do seu local de trabalho, onde passam de dez a doze horas por dia.

Inclui-se um artigo que trata das obrigações dos provedores de acesso como:

I – manter em ambiente controlado e de alta segurança os dados de conexões realizadas por seus equipamentos, aptos à identificação do usuário, endereços eletrônicos de origem das conexões, data, horário de início e término e referência GMT, da conexão, pelo prazo de três anos, para prover os elementos essenciais para fazer prova da autenticidade da autoria das conexões na rede de computadores ou internet;

II – tornar disponíveis à autoridade competente os dados e informações elencados no inciso I no curso de auditoria técnica a que forem submetidos;

III – fornecer, quando solicitado pela autoridade competente no curso de investigação criminal, os dados e informações de conexões realizadas e os dados e informações de identificação do usuário;

IV – informar, de maneira sigilosa, à autoridade criminal competente à qual está jurisdicionado, fato do qual tenha tomado conhecimento e que contenha indícios de conduta delituosa na rede de computadores ou internet sob sua responsabilidade;

V – informar ao usuário, quando da requisição da sua identificação e autenticação, que aquela conexão obedece às leis brasileiras e que toda comunicação ali realizada será de exclusiva responsabilidade do usuário, perante as leis brasileiras, para prover os elementos essenciais para fazer prova da autenticidade da autoria das conexões na rede de computadores ou internet;

VI – alertar aos seus usuários, em campanhas periódicas, quanto ao uso criminoso de rede de computadores ou internet, dispositivos de comunicação e sistemas informatizados;

VII – divulgar aos seus usuários, em local destacado, as boas práticas de segurança no uso de rede de computadores ou internet, dispositivos de comunicação e sistemas informatizados.

O parágrafo único do artigo determina que os dados de conexões realizadas em rede de computadores ou internet, as condições de alta segurança de sua guarda, a auditoria à qual serão submetidas, a autoridade competente responsável pela auditoria e o texto a ser informado aos usuários de rede de computadores ou internet, serão definidos nos termos de regulamento em prazo não superior a noventa dias a partir da data de publicação desta lei, sendo obrigatórios aqueles dados de conexão definidos neste artigo.

Inclui um artigo para definir a exclusão da ilicitude por "Exercício regular de direito", ou seja, de que não pratica o crime de difusão injustificada o usuário, o agente técnico ou o profissional habilitado que, a título de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação manipula código malicioso detectado, em proveito próprio ou de seu preponente e sem risco para terceiros.

Inclui um artigo que determina à autoridade competente, nos termos de regulamento, a estruturar órgãos, setores e equipes de agentes especializados no combate à ação delituosa em rede de computadores ou internet, dispositivo de comunicação ou sistema informatizado.

Inclui um artigo que altera o art. 1º da Lei nº 10.446, de 8 de maio de 2002, a Lei da Repressão Uniforme contra os crimes interestaduais e internacionais que passa a abranger os delitos praticados contra ou mediante rede de computadores ou internet, dispositivo de comunicação ou sistema informatizado.

Finalmente inclui um artigo que acrescenta à Lei 8.078 de 11 de setembro de 1990, o Código do Consumidor, ao seu art. 9º, o parágrafo único que diz que a obrigação de informar sobre a nocividade do produto à saúde ou segurança do consumidor, também se aplica à sua segurança digital ou seja, da necessidade do uso de senhas ou similar para a proteção do uso, ou dos dados trafegados naquele dispositivo de comunicação, sistema informatizado ou rede de computadores ou internet.