

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 2000 que está apensado ao PLC 89 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 Constituição 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 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 SUBSTITUTIVO 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, identificação de usuário, autenticação de usuário, provedor de acesso e de serviço e dados de conexões realizadas.

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.

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, dispositivo de comunicação ou sistema informatizado, ou se tiverem sido praticados mediante uso de rede de computadores, 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 calúnia, 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
- 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
- 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

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 no provedor de acesso. 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 ao seu provedor de acesso.

E mais, o PLS prevê que o cadastro de identificação 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;

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, 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 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;

VI – alertar aos seus usuários, em campanhas periódicas, quanto ao uso criminoso de rede de computadores, dispositivo de comunicação e sistema informatizado;

VII – divulgar aos seus usuários, em local destacado, as boas práticas de segurança no uso de rede de computadores, dispositivo de comunicação e sistema informatizado.

O parágrafo único do artigo determina que os dados de conexões realizadas em rede de computadores, 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, 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, ou seja, de que é isento de pena 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, sem devio de finalidade e com documentação apropriada.

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, 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, 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.

Em outubro, o parecer incorporou entendimento recente do STJ, reforçando a tese de que não importa onde (em que país) é gerada a página da internet, mas sim onde os efeitos do crime são sentidos. A competência para julgar o caso é da Justiça estadual, mesmo que o crime seja cometido pela internet em site hospedado no exterior.

Ainda com relação às decisões do STJ, em 18/09, o tribunal, em atendimento a pedido vindo da Comarca de Düsseldorf, na Alemanha, decidiu que um provedor nacional de acesso à internet (UOL) informe os dados de pessoa que bloqueou acesso aos sites atendidos pela empresa Online-forum. Segue trecho do parecer do STJ que aborda essa decisão, com destaque também para parecer do ministro Sepúlveda Pertence, do STF, de que esses dados não têm proteção constitucional.

A propósito da repressão internacional, entendimento recente, de 16 de outubro de 2006, da 3ª Seção do Superior Tribunal de Justiça, reforça a tese de que não importa onde é gerada a página da internet, mas sim onde os efeitos do crime são sentidos. Se não há lesão direta a bens, serviços ou interesses da União, a competência para julgar o caso é da Justiça Estadual, mesmo que o crime tenha sido cometido pela internet, por meio de site hospedado no exterior.

E Em decisão recente, de 18 de setembro de 2006, o Ministro Barros Monteiro, do Supremo Tribunal de Justiça, por solicitação do Tribunal da Comarca de Düsseldorf, República Federal da Alemanha, decidiu que um provedor nacional de acesso à internet "*informe os dados da pessoa que, em 25 de fevereiro de 2004, às 3:20 hs (hora da Europa Central), a partir do IP n. 200.98.154.187, bloqueou o acesso aos sites atendidos pela empresa Online-forum*".

No curso do processo o provedor apresentou impugnação invocando o princípio constitucional da inviolabilidade de dados, previsto no art. 5º, XII, da Constituição Federal, que, segundo alega, impede a quebra do sigilo de dados cadastrais, não se opondo a fornecer as informações solicitadas, desde que mediante expressa autorização judicial.

Considerando não haver caráter construtivo no pedido do Tribunal alemão, vez que visa somente obter os dados do usuário conectado ao IP n. 200.98.154.187, no dia e hora mencionados, a fim de instruir investigação instaurada perante a Justiça estrangeira, o Excelentíssimo Ministro mencionou o estudo de Tércio Sampaio Ferraz Júnior em seu trabalho "Sigilo de Dados: O Direito à Privacidade e os Limites à Função Fiscalizadora do Estado" (Revista da Faculdade de Direito USP, vol. 88, 1993, p. 449), ao explanar sobre o alcance da proteção à vida privada:

"Pelo sentido inexoravelmente comunicacional da convivência, a vida privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos — como o nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial etc, condicionam o próprio intercâmbio humano em sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura.

Por isso, a proteção desses dados em si, pelo sigilo, não faz sentido. Assim, a inviolabilidade de dados referentes à vida privada só tem pertinência para aqueles associados aos elementos identificadores usados nas relações de convivência, as quais só dizem respeito aos que convivem.

Dito de outro modo, os elementos de identificação só são protegidos quando compõem relações de convivência privativas: a proteção é para elas, não para eles.

Em consequência, simples cadastros de elementos identificadores (nome, endereço, R.G., filiação, etc.) não são protegidos. Mas cadastros que envolvam relações de convivência privada (por exemplo, nas relações de clientela, desde quando é cliente, se a relação foi interrompida, as razões pelas quais isto ocorreu, quais os interesses peculiares do cliente, sua capacidade de satisfazer aqueles interesses, etc) estão sob proteção.

Afinal, o risco à integridade moral do sujeito, objeto do direito à privacidade, não está no nome, mas na exploração do nome, não está nos elementos de identificação que condicionam as relações privadas, mas na apropriação dessas relações por terceiros a quem elas não dizem respeito".

Ao preparar-se para decidir pelo encaminhamento dos autos à Justiça Federal do Estado de São Paulo, para as providências cabíveis, o Ministro evocou a jurisprudência emanada do Supremo Tribunal Federal, em especial o trecho do voto proferido pelo Ministro Sepúlveda Pertence, que também dá amparo ao acolhimento da ordem pleiteada pelo Tribunal estrangeiro:

"Não entendo que se cuide de garantia com status constitucional. Não se trata da 'intimidade' protegida no inciso X do art. 5º da Constituição Federal. Da minha leitura, no inciso XII da Lei Fundamental, o que se protege, e de modo absoluto, até em relação ao Poder Judiciário, é a comunicação 'de dados' e não os 'dados', o que tornaria impossível qualquer investigação administrativa, fosse qual fosse." (voto proferido no MS n. 21.729-4/DF, DJ 19.10.2001).