

CRIMES ELETRÔNICOS: A INTERNET É UMA TERRA SEM LEIS?

Diferenças entre o Projeto de Lei sobre crimes eletrônicos de relatoria do Senador Azeredo, a proposta legislativa atual e a Convenção Internacional de Combate ao Cybercrime.

Dra. Gisele Truzzi¹

¹Advogada especialista em Direito Digital e Direito Criminal. www.truzzi.com.br / gisele@truzzi.com.br.

A internet, como qualquer tecnologia, trouxe-nos inúmeros benefícios. Porém, trouxe também desvantagens: ela é um celeiro para a proliferação de variados crimes.

Mas o fato de delitos serem praticados em um novo ambiente gera um questionamento. Estariam eles alheios à nossa legislação? A resposta é não! Nosso Código Penal abrange 95% dos ilícitos cometidos através dos meios eletrônicos (furto, estelionato, crimes contra a honra etc.). Para os 5% restantes, ainda não há legislação específica, e, por conta dessa lacuna legal, a prática de determinados delitos próprios do mundo informático resulta na impunidade.

A fim de sanar essa brecha, tramita há mais de 10 anos no Congresso Nacional o Projeto de Lei nº 84/99¹, que visa à criação de novas condutas penais na legislação. Ao longo desse período, o PL 84/99 englobou outras proposições que foram surgindo: PLS 76/2000, PLS 137/2000 e PLC 89/2003. Ao passar pelo Senado e pelo Congresso, o PL nº 84/99 sofreu modificações, conquistou inimigos, recebeu o apelido de “AI-5 Digital” e arrebanhou devotos, tornando-se objeto de discussão na sociedade. Atualmente, teve seu texto reduzido e recebeu nova numeração: PL nº 587/2011.

E se você se pergunta o que tem a ver com isso, saiba que tudo! Cada usuário da internet deve atentar a esse tema, para evitar ser vítima de um crime eletrônico ou, na pior das hipóteses, ser o próprio criminoso, se não tiver conhecimento da legislação.

Convenção de Budapeste

A necessidade de uma legislação específica para os crimes eletrônicos justifica-se também pela Convenção de Budapeste (ou Convenção Internacional contra o Cybercrime)². Tal tratado é um pacto internacional, criado em 2001 na Hungria pelo Conselho da Europa³, e suas principais finalidades são uniformizar a legislação sobre o tema, combater o crime eletrônico e criar uma rede de cooperação internacional, facilitando a disponibilização das provas eletrônicas e as investigações.

Atualmente, 47 países são signatários da Convenção, mas o Brasil não faz parte dessa lista⁴ – um dos motivos da ausência de legislação específica sobre delitos informáticos.

Projeto de Lei sobre Crimes Eletrônicos

Inicialmente, o PL de Crimes Eletrônicos previa a criação de 13 tipos penais. Por conta de tantas críticas, o texto foi alterado, a maioria dos delitos, excluída e tentou-se amenizar a polêmica mantendo somente três novos crimes.

¹ Acompanhamento legislativo: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>

² Texto integral disponível em <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

³ <http://www.coe.int/lportal/web/coe-portal/what-we-do/rule-of-law/cybercrime?dynLink=true&layoutId=36&dlgroupId=10226&fromArticleId=>

⁴ http://www.coe.int/lportal/c/document_library/get_file?uuid=6f607719-3f7a-40fa-8d82-eea54c5aa80f&groupId=10227

Algumas das alterações pelas quais o PL passou foram imprescindíveis, como a eliminação do conceito “defesa digital”, que permitiria a determinado usuário responder a um ataque sofrido. Uma das polêmicas, também findada, girava em torno da criação da figura do chamado “provedor dedo-duro”: provedores de internet deveriam repassar às autoridades ocorrências e indícios de crimes, mesmo sem possuir alçada para tanto. Outra situação muito debatida e ainda não resolvida diz respeito à obrigatoriedade de armazenamento dos “logs de conexão” pelos provedores, que teve prazo de guarda reduzido.

A questão do dano eletrônico foi acertadamente mantida. Porém, o texto atual nada diz sobre aumento de pena para os crimes contra a honra (calúnia⁵, difamação⁶ e injúria⁷) praticados pela internet, tendo em vista que o dano à imagem costuma ter proporções maiores se provocado via *web*.

De modo geral, nota-se que o novo texto do PL destaca-se do original, muito distante do que definiu a Convenção de Budapeste – devido ao volume de novos tipos penais propostos e ao subjetivismo de alguns trechos. O novo PL, com tipificações penais mínimas, conceitos definidos e texto enxuto, soma duas características: aproxima-se da Convenção, e tem aplicação prática mais adequada à realidade brasileira.

Aprovar o Projeto de Lei ou não?

A aprovação do Projeto de Lei sobre Crimes Eletrônicos é necessária para que o Brasil possa combater de modo eficaz os delitos informáticos, alinhar-se aos demais países em termos de legislação e possibilitar a cooperação internacional entre as autoridades.

Para evoluir, precisamos mudar, e o Direito não pode andar em passo dissonante com a tecnologia.

⁵ Art. 138, Código Penal - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
Pena - detenção, de seis (seis) meses a 2 (dois) anos, e multa.

⁶ Art. 139, Código Penal - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

⁷ Art. 140, Código Penal - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
Pena - detenção, de 1 (um) a 6 (seis) meses, ou multa.

PL 84/1999

Resumo das principais alterações

Proposições	Críticas	Mantida?
Dano eletrônico	Criação do delito de “dano eletrônico”, que contempla elaboração, disseminação ou venda de códigos maliciosos e combate tais práticas.	Sim
“Provedor dedo-duro”	Modifica as responsabilidades do provedor de acesso à rede, impondo-lhe a obrigação de levar ao conhecimento da autoridade policial ou judicial, de modo sigiloso e por <u>iniciativa própria</u> , todos os casos dos quais tenha indícios ou suspeitas da prática criminosa. (Ao fornecedor de acesso não cabe julgar ou ter poder de polícia sobre esse tipo de evento.)	Não
“Defesa digital”	Visava proteger profissionais que trabalhavam com segurança ou investigações e que necessitariam interceptar dados informáticos ou realizar contra-ataque para identificar o agressor.	Não
Registros de conexão	Obrigava os provedores a armazenar os dados de conexão (IP, data, horário e referência GMT) por três anos.	Prazo de armazenamento alterado para 18 meses.
Criação de 11 tipos penais	O volume de tipificações penais novas, com trechos subjetivos, criava situações difíceis de serem resolvidas adequadamente na esfera penal.	As tipificações penais foram reduzidas para três somente.
	Não prevê aumento de pena para os crimes contra a honra praticados através dos meios eletrônicos.	Sim
	Não prevê via de contato extrajudicial entre as partes, para solicitação de informações não sigilosas, que poderiam ser obtidas diretamente com o fornecedor de acesso.	Sim

Tabela: Dra. Gisele Truzzi

PL 587/2011

Resumo das principais novidades ou manutenções

Proposições	Críticas	Mantida?
Dano eletrônico	Criação do delito de “dano eletrônico”, que contempla elaboração, disseminação ou venda de códigos maliciosos e combate tais práticas. Criminaliza também a conduta daquele que dissemina ou insere códigos maliciosos com a finalidade específica de causar dano.	Sim
Acesso indevido	Inserção do art. 285-A no Código Penal, que define como crime a atitude de invadir rede de computadores ou sistema informatizado sem autorização do seu titular, com o fim de obter vantagem ilícita.	Sim. A redação poderia ser alterada, suprimindo “com o fim de obter vantagem ilícita”, para englobar a prática de invadir redes ou sistemas somente para espionar.
Definição de “log de acesso”	Especificação do termo “log de acesso” para definir “informações referentes à hora, data, início, término, duração, endereço de Protocolo Internet (IP) utilizado e terminal de origem da conexão.”	Sim
Diferenciação entre “logs de acesso” e “dados cadastrais”	A diferenciação dos termos permitiu que os “dados cadastrais” fossem definidos como sigilosos – devendo ser armazenados separadamente – e vinculou os “dados cadastrais” a uma pessoa e a um documento de identificação.	Sim
Redução dos 13 tipos penais para apenas três	A redução dos tipos penais é eficaz para garantir punição para os principais crimes praticados nos meios eletrônicos, e também visa a uniformizar as polêmicas surgidas anteriormente. Além disso, o texto foi melhorado com a exclusão de pontos subjetivos ou definições abstratas.	Sim
	Não prevê aumento de pena para os crimes contra a honra praticados através dos meios eletrônicos.	Sim
	Não prevê via de contato extrajudicial entre as partes, para solicitação de informações não sigilosas, que poderiam ser obtidas diretamente com o fornecedor de acesso.	Sim