O ESTADO DA ARTE DA LEGISLAÇÃO BRASILEIRA SOBRE A CRIMINALIDADE CIBERNÉTICA

Muriel Mazzetto

Introdução

- Com a facilidade de acesso à tecnologia atual, se tornou cada vez mais fácil causar dano contra patrimônio moral e material dos indivíduos.

- Os fatos anteciparam-se à previsão legal. Qual o legislador que preveria, há trinta anos, os recursos para gerir nosso patrimônio, movimentar nossas contas bancárias à distância declarar impostos e fazer pagamentos sem ir a banco ou repartição fazendária, retirar ou depositar dinheiro em caixas eletrônicos, em autoatendimento, com a segurança dos cartões magnéticos, que utilizamos correntemente em substituição aos cheques e ao papel moeda em espécie?

- As facilidades e o conforto decorrentes da evolução tecnológica trouxeram consigo a fragilidade da insegurança que seu indevido uso acarreta.

    - Entende-se como uso indevido o uso do conhecimento sobre as tecnologias para fraudes, invasões de privacidade, atendados aos serviços públicos e privados, crime organizado, espionagem, entre outros.

Crime cibernético

O histórico dos crimes cibernéticos, por sua vez, remonta à década de 1970, quando, pela primeira vez, foi definido o termo "hacker", como sendo aquele indivíduo que, dotado de conhecimentos técnicos, promove a invasão de sistemas operacionais privados e a difusão de pragas virtuais. Contudo, a universalização do termo "hacker" acompanhou o crescimento e a popularização da internet, ocorridos na década de 1990, sendo hoje muito comum, havendo inclusive subdivisões, como "hacker" (aquele que invade sistemas e computadores, furtando senhas, propagando vírus e cavalos de tróia) e "cracker" (aquele que sabota e pirateia programas de computador, fornecendo senhas e chaves de acesso obtidas de forma ilegal), "lammer" (aquele que possui conhecimentos limitados de informática e não possui grande potencial ofensivo), "spammer" [aquele que invade a privacidade de outrem por meio da difusão de mensagens eletrônicas (e-mails) indesejadas], dentre outros termos, cujo detalhamento é desnecessário para os objetivos do presente artigo.

Crime cibernético

Anteriormente ao ano de 2012, a falta de legislação específica tornava muito difícil a apuração dos crimes virtuais, uma vez que a legislação até então vigente havia sido direcionada aos crimes de forma geral, independentemente do meio utilizado para a sua prática. Nesse sentido, podemos citar, dentre outros, o Código Penal (CP), o Estatuto da Criança e do Adolescente (Lei n. 8.069/90) e Lei dos crimes de software (ou lei antipirataria, Lei n. 9.609/98) e a Lei de Segurança Nacional (Lei nº 7.170/83).

Crime cibernético

- As expressões crime cibernético, crime digital, crime de informática, ou simplesmente cibercrime, são usadas para se referir a um conjunto de condutas delituosas que, de certa forma, estão relacionadas à tecnologia da informação.

- Segundo a *International Telecommunication Union*, as ofensas podem ser classificadas da seguinte forma:

  - Relacionadas a direitos autorais;
  - Relacionadas a conteúdos;
  - Contra confidencialidade, integridade e disponibilidade de sistemas computacionais;
  - Relacionadas a computadores.

Direitos autorais

- Surgiu com a proteção da propriedade intelectual sobre programas de computador.
- Em dezembro de 1987, o Congresso nacional aprovou a Lei n 7.646, criminalizando as condutas de violação de direitos do autor (art. 35) e a importação, exposição, manutenção em depósito, para fins comerciais, de programas de computador, de origem externa, não cadastrados (art. 36).
- Essa lei foi revogada pela de nº 9.609, em 1998, que manteve o primeiro tipo penal (agora no art.12) com a mesma pena, e aboliu o segundo.
  - Detenção de seis meses a dois anos, ou multa.

Ofensas relacionadas a conteúdo

1. Pornografia infantil:

    - Disciplinado pelo Estatuto da Criança e do Adolescente;
    - Alteração em 2003 e em 2008, para se enquadrar nos modelos de disseminação tecnológica.
    - Punição por manter registros de menores de 18 anos em cenas de sexo e pornografia. Também o comportamento daqueles que trocam, transmitem, disponibilizam publicam ou divulgam, por qualquer meio, qualquer registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.
    - Visou ainda punir montagens e edições de filmes, em geral, contendo imagens sexuais de jovens. Quem simula sexo explícito ou pornografia envolvendo crianças e adolescentes, por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual também estará sujeito aos rigores da lei.
    - Punição por aliciação em salas de bate-papo, redes sociais e outros sistemas de interações.
    - Detenção de dois a seis anos, e multa.

Ofensas relacionadas a conteúdo

2. Atuação de grupos racistas e outras organizações criminosas:

   - Foram sofridas alterações na lei n 7.716, de 1989 com a adição de leis em 1990, 1994, 1997, 2003 e 2012, resultando em um montante que atua sobre os seguintes quesitos:

   - Manifestação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional cometidas por meio da Internet, nas diferentes formas de veiculação das informações.

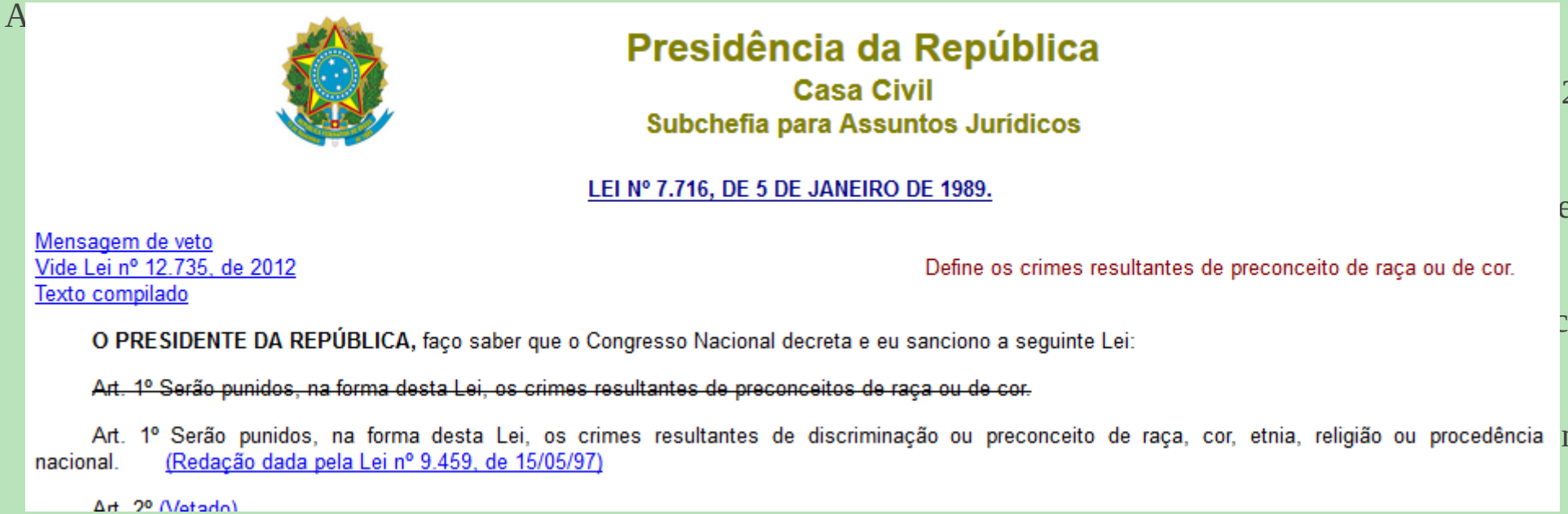
   - Tendem a repercutir de forma mais intensa pela Internet que em discussões verbais, devido a abrangência da rede.

   - Páginas e demais mídias de comunicação que comumente disseminam tais formas de discriminação podem ser interditadas mediante pedido do Ministério Público.

   - Detenção de dois a cinco anos, e multa.

Ofensas relacionadas a conteúdo

2. A



Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos

LEI Nº 7.716, DE 5 DE JANEIRO DE 1989.

Mensagem de veto
Vide Lei nº 12.735, de 2012
Texto compilado

Define os crimes resultantes de preconceito de raça ou de cor.

O PRESIDENTE DA REPÚBLICA, faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

~~Art. 1º Serão punidos, na forma desta Lei, os crimes resultantes de preconceitos de raça ou de cor.~~

Art. 1º Serão punidos, na forma desta Lei, os crimes resultantes de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. (Redação dada pela Lei nº 9.459, de 15/05/97)

Art. 2º (Vetado)

2012,

etidas

cia da

m ser

- Detenção de dois a cinco anos, e multa.

Ofensas relacionadas a conteúdo

3. Cyberbullying:

   - Define as atitudes agressivas, intencionais e repetidas, que ocorrem sem motivação evidente, adotada por um ou mais indivíduos contra outro por meio da Internet. Causam dor e angústia, executadas dentro de uma relação desigual de poder.

   - Não é tipificado como crime no Brasil, porém está coberto pelas normas do Estatuto da Criança e do Adolescente.

   - Destacam-se as formas de calúnia, difamação, injúria, ameaça, constrangimento ilegal, falsa identidade, molestar ou perturbar a tranquilidade.

   - As penas são de acordo com o crime e as leis que o cercam, variando de acompanhamento psicológico e trabalho comunitário até prisão.

Ofensas contra confidencialidade, integridade e disponibilidade de sistemas computacionais

- Engloba as ações de espionagem, invasão, interceptação, ataques e interferência em sistemas computacionais ou eletrônicos.

1. Interceptação telemática ilegal:
   - Constitui crime a interceptação de comunicação telefônica, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
   - Ataques MITM são exemplos de interceptação de comunicação, porém a lei n 9.296, que rege tal crime, é de 1996 e não inclui tipificação para interceptação em redes.
   - Pena de reclusão de dois a quatro anos, e multa.
   - Em processos são comumente descartadas e inadmissíveis provas, ainda que favoráveis, obtidas por meios ilícitos.
   - Ministérios Públicos, a Polícia Judiciária (a Federal e as Civis dos Estados) e a Polícia Militar (quando da realização de Inquéritos Policiais Militares) poderão, com base no art. 17-B da Lei nº 9.613, de 1998, expedir requisições diretamente às pessoas jurídicas detentoras dos dados cadastrais, ordens estas que deverão ser cumpridas sob pena de desobediência (art. 330 do Código Penal).

Ofensas contra confidencialidade, integridade e disponibilidade de sistemas computacionais

2. Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública:
   - Considerado crime quando impossibilita-se o uso dos meios de comunicação de tais serviços, instaurado em 2012 pela lei 12.737.
   - Tende a proteger a normalidade dos serviços de telecomunicação.
   - Ataque DDOS, quando impossibilita o funcionamento de algum serviço de comunicação, é tipificado como crime segundo tal lei.
   - Danos em cabeamentos e equipamentos.
   - Pena de um a três anos de detenção, e multa.
   - Pena dobrada quando atentado é cometido por ocasião de calamidade pública. Utilizado em punição caso se identifique os indivíduos que causam tais ataques em situações de desastre, onde meios de comunicação são essenciais.

Ofensas contra confidencialidade, integridade e disponibilidade de sistemas computacionais

3. Invasão de dispositivo informático:

   - Invasão de dispositivo alheio, mediante violação indevida de mecanismos de segurança e com fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.
   - Tratado pela lei n 12.737, de 2012. Considerada um marco na revolução da legislação brasileira.
   - Conhecida pelo apelido de “Lei Carolina Dieckmann”.
   - Detenção de três meses a um ano, e multa.

Ofensas contra confidencialidade, integridade e disponibilidade de sistemas computacionais

3. Invasão de dispositivo informático:

   - Invasão de dispositivo alheio, mediante violação indevida de mecanismos de segurança e com fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.
   - Tratado pela lei n 12.737, de 2012. Considerada um marco na revolução da legislação brasileira.
   - Conhecida pelo apelido de “Lei Carolina Dieckmann”.

> Entretanto, no mês de maio de 2012, foi notícia na mídia a divulgação de imagens da intimidade da atriz Carolina Dieckmann em diversos sítios eletrônicos da rede mundial de computadores, o que causou uma grande comoção social, o que abriu campo para a edição da Lei n. 12.737, de 30/11/2012, publicada no DOU de 03/12/2012, com *vacatio legis* de 120 (cento e vinte) dias, apelidada de “Lei Carolina Dieckmann”, que, dentre outras providências, dispôs sobre a tipificação criminal dos delitos informáticos, introduzindo osarts. 154-A, 154-B, e alterando os arts. 266 e 298, todos do Código Penal.

Ofensas contra confidencialidade, integridade e disponibilidade de sistemas computacionais

4. Alteração de sistemas de informação:
   - Modificação do Código Penal pela lei n 9.983 de 2000, para coibir fraudes na previdência social.
   - Tipificação penal da inserção de dados falsos ou alteração e exclusão indevida de dados dos sistemas de administração pública.
   - Criminalização da alteração de softwares de administração pública.
   - Roubo e divulgação de informações de administração pública.
   - Reclusão de dois a doze anos, e multa.

Ofensas contra confidencialidade, integridade e disponibilidade de sistemas computacionais

5. Espionagem:
   - Descritos pelo Código Penal Militar e pela Lei de Segurança Nacional.
   - Várias dessas condutas de espionagem são facilitadas pelo uso da Internet.
   - *Spyware*.
   - Desde facilitação de acesso aos dados sigilosos até obtenção, alteração e divulgação de informações.
   - Penas segundo Lei n 7.170, de 1983, variam de um a quinze anos de prisão, e multa.

Ofensas relacionadas a computadores

- Estelionato e fraudes eletrônicas em sistemas bancários:
  - Tipificado pelo art. 171 do Código Penal, de 1940, consiste em obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.
  - O projeto de lei nº 5.485, de 2013, que tramita no Congresso Nacional, propõe a tipificação criminal do estelionato eletrônico, configurado pelo envio mensagens digitais de qualquer espécie, fazendo-se passar por empresas, instituições ou pessoas a fim de induzir outrem a revelar informações pessoais, de identidade, ou senhas de acesso.
  - Criminalização do *phishing*.
  - Como meio legislativo atual, a Lei n 12.737, de 2012, é utilizada para equiparar cartão de crédito ou débito como documento particular, incluso na penalização descrita pela invasão e aquisição ilegal de informação pessoal.
  - Serviços de armazenamento que hospedam tais tipos de páginas, ao identifica-las, devem retirá-las imediatamente de circulação, caso contrário serão notificados e penalizados como indivíduos criminosos.

Responsabilidade penal dos provedores de Internet

- Atualmente, não existe lei específica quanto a responsabilidade criminal dos provedores de acesso e dos provedores de conteúdo e de armazenamento.
- Tais provedores são notificados e penalizados de acordo com o conteúdo que se encontra disponibilizado.
- São puníveis quando, após notificado, não desabilita o acesso ao conteúdo ilícito.
- Casos comuns de violação de direitos autorais em vídeos, que devem ser removidos ao pedido de gravadoras.
- A obrigatoriedade da guarda de *logs* de acesso à Internet não é procedimento regulamentado por leis, cabendo aos meios estaduais e municipais, dentro de investigações.
- Paraná, Santa Catarina e São Paulo são alguns dos estados com leis próprias que definem o armazenamento de *logs* para provedores que disponibilizam acesso oneroso ou gratuito à Internet.

Responsabilidade penal dos

LEI ESTADUAL Nº 16.241/2009-PR - 06/10/2009
(Publicado no Diário Oficial nº 8.077 de 15/10/2009)

Súmula: Estabelece a obrigatoriedade da adoção de sistema de monitoramento por câmeras e identificação de usuário em estabelecimento de acesso público a internet.

A Assembléia Legislativa do Estado do Paraná aprovou e eu promulgo, nos termos do § 7º do Artigo 71 da Constituição Estadual, os seguintes dispositivos do Projeto de Lei nº 053/09:

Art. 1º. Todos os estabelecimentos voltados à comercialização do acesso à internet, em funcionamento no Estado do Paraná, deverão adotar sistema de monitoramento por câmeras de vigilância, em especial nos acessos aos computadores.

Art. 2º. Os estabelecimentos de que trata esta lei deverão manter, pelo prazo de dois anos, cadastro de todos os usuários, contendo os seguintes dados:

I - o tipo e o número do documento de identidade apresentado;
II - o endereço e o telefone;
III - o equipamento usado, bem como os horários do início e do término de sua utilização;
IV - o Protocolo Internet - IP - do equipamento usado.

Parágrafo único. Os dados de que trata o caput deste artigo serão armazenados por meio eletrônico, ficando proibida sua divulgação, exceto mediante expressa autorização do cliente, pedido formal de seu representante legal ou ordem judicial.

Art. 3º. Esta lei entrará em vigor na data de sua publicação.

Palácio Dezenove de Dezembro, em 06 de outubro de 2009.

Nelson Justus
Presidente

gratuito à Internet.

Cooperação internacional

- Para o crime cibernético, registra-se a Convenção sobre o Cibercrime [Council of Europe 2001], assinada 23 de novembro de 2001, na cidade de Budapeste/Hungria, ainda não ratificada pelo Brasil.

- A regra geral é a territorialidade, podendo haver a persecução de crimes cometidos fora do território nacional em virtude da nacionalidade do autor (princípio da personalidade ativa), nacionalidade da vítima (princípio da personalidade passiva), bem jurídico afetado (princípio da defesa ou real), local onde foi praticado o ilícito (princípio da representação) e características do delito, hábil a afetar ou não valores da comunidade internacional (princípio da justiça universal). Havendo elementos de extraneidade (como fases do seu cometimento no exterior, vítima ou autor estrangeiros) a necessidade de cooperação internacional afigura-se em regra mais evidente.

- O Brasil possui acordos de cooperação com Estados Unidos, Japão, Reino Unido, Alemanha e China.

- Todos possuem acordos próprios, poucos seguem a regulamentação das Nações Unidas.

- A forma como se descreve a cooperação está ligada com os diferentes meios de punição entre os países, e as diferentes tipificações dos crimes.

Conclusão

- A criminalidade cibernética é relativamente nova, com graves danos e riscos.
- A compreensão e conduta é difícil de se estabelecer no país.
- Faz-se o uso de Leis já estabelecidas para cobrir demais delitos encontrados dentro da esfera tecnológica.
- A legislação brasileira é antiga e portanto falha perante os meios de ataques atuais.

REFERÊNCIAS

- http://www.conteudojuridico.com.br/artigo,os-crimes-ciberneticos-e-a-lei-no-127372012,52253.html
- http://www.planalto.gov.br/ccivil_03/leis/L9609.htm
- http://www.planalto.gov.br/ccivil_03/leis/2003/L10.764.htm
- http://www.planalto.gov.br/ccivil_03/leis/L7716.htm
- http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm
- http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm#art3
- http://www.planalto.gov.br/ccivil_03/LEIS/L9983.htm

REFERÊNCIAS

- http://www.planalto.gov.br/ccivil_03/leis/l7170.htm
- http://www.crianca.mppr.mp.br/modules/conteudo/conteudo.php?conteudo=1246