Os Crimes Cibernéticos

Aula 1 – Governança da Internet e Crimes Cibernéticos

– Introdução

Crimes cibernéticos são aqueles praticados pela rede mundial de computadores ou por qualquer sistema informático.
Existem os crimes cibernéticos próprios, que são aqueles cujo tipo penal descreve a prática delituosa que somente ocorre se praticada pelo meio virtual ou informático.
Já os crimes cibernéticos impróprios são aqueles praticados pelo meio virtual ou eletrônico, embora esse meio não esteja descrito no tipo penal.
Exemplos de crimes cibernéticos próprios são os arts. 313-A (inserção de dados falsos em sistema de informações) e 313-B (modificação ou alteração não autorizada de sistema de informações) do Código Penal , o artigo 154-A (invasão de dispositivo informático) do Código Penal e o artigo 241-A (oferecer, trocar, disponibilizar, transmitir, distribuir, publicar, ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente) do Estatuto da Criança e do Adolescente – ECA.

Exemplos de crimes cibernéticos impróprios são a fraude bancária através do *internet banking* ou o estelionato praticado através de um sítio fraudulento na *internet.*

A principal característica de um delito praticado em meio virtual é que ele deixa rastro. Isto porque para que um sistema informático ou para que a *internet* funcionem, existe uma lógica matemática que permite a difusão das informações e a entrega de dados exatamente ao destino pretendido.

Isso faz com que toda a movimentação nesse meio fique registrada, permitindo ao investigador seguir a pista e identificar os autores da movimentação.

No entanto, como esse funcionamento implica na geração de uma quantidade gigantesca de *bits* e *bytes*, a vida útil dessas informações não é garantida, restando preservados somente os dados relevantes ao próprio sistema, a menos que haja ordem específica para tanto. Aqui está a segunda característica desses delitos: as provas digitais que podem levar ao criminoso são voláteis, sendo imprescindível a existência de agilidade na sua coleta.

A investigação de crimes cibernéticos implica no conhecimento acerca da lógica do sistema informático e da *internet* que se sofistica conforme diferentes aplicações de *internet* ou sistemas passam a ficar disponíveis para utilização.

Para o funcionamento da rede mundial de computadores, a *internet*, é necessária uma conexão à rede, que se realiza através de um provedor de conexão. Esta conexão pode ser paga ou gratuita, mas implica em receber um número IP, isto é, um protocolo de *internet* (*internet protocol*) para acessar a infraestrutura de rede mantida pelas empresas de telecomunicações.

Uma vez de posse do número IP, o indivíduo pode navegar pelos diversos aplicativos disponibilizados pelos provedores de aplicação ou conteúdo.

A governança da Internet
É preciso fazer um pequeno parêntese para explicar como funciona a governança da *internet.*

A *internet* é regulada pela ICANN – *Internet Corporation for Assigned Names and Number*s http://archive.icann.org/tr/portuguese.html, uma entidade multissetorial, sem fins lucrativos, de âmbito internacional, onde se fazem representados governos, setor técnico e a sociedade civil, que determina os rumos da *internet.* No seu início, na década de 1960, era utilizada para fins militares e depois para fins acadêmicos, sendo controlada pelo Departamento de Comércio dos Estados Unidos. Recentemente, após o escândalo *Snowden*, de controle sobre os dados de usuários de *internet* pela Agência Americana de Segurança, NSA - *National Security Agency*, cresceu a pressão para que a ICANN passasse ao controle de uma entidade também multissetorial, como é a natureza da *internet*, sem estar vinculada a nenhum governo especialmente, estando-se atualmente em período de transição para esse modelo.

O que importa compreender é que a ICANN desempenha diferentes funções como o controle de nomes e domínios, funções de administração central da rede e, a função desempenhada pela IANA, que é a responsável pela alocação dos *Internet Protocols* no mundo.
Assim, cada região do globo recebeu um lote de IPs para gerir.

No Brasil, o NIC.br é o braço executivo do Comitê Gestor da *Internet* é o responsável por alocar os números IP para as operadoras de telefonia que, por sua vez, disponibilizam um único número IP para cada conexão de *internet*, sendo, portanto, possível identificar o endereço a partir de onde foi feita aquela conexão. Assim, uma simples consulta no http://registro.br, Tecnologia, Ferramentas, *whois*, é possível saber quem é o responsável por determinado domínio e que poderá indicar o IP, data e hora utilizados na conexão à *internet.* De posse dessas informações, outra consulta no mesmo sítio indica qual empresa de telefonia é a responsável por alocar o IP pesquisado, à qual se deve dirigir o pedido de informação relativo à informação cadastral desse usuário, o que leva ao endereço físico onde se deu a conexão de *internet* para a difusão do conteúdo pesquisado.

O esgotamento do IPv4

A princípio, o *Internet Protocol* era composto por quatro grupos de números, o chamado IPv4. Porém, devido à utilização crescente da *Internet*, com cada vez mais conexões sendo utilizadas por cada pessoa, já que uma pessoa não representa mais somente uma conexão, mas várias, pois podem estar logados ao mesmo tempo o aparelho celular, o *tablet*, o *notebook*, o aparelho de TV e uma infinidade de outros aparelhos que apontam para o desenvolvimento da *Internet* das Coisas -IoT – *Internet of Things*, ocorreu o esgotamento do modelo IPv4.
Atualmente, muitos países já migraram para o IPv6: número de *Internet Protocol* com seis conjuntos de três números o que aumentou consideravelmente as possibilidades de conexões à rede.

O que temos atualmente no Brasil é a seguinte situação: os provedores de aplicações de *internet* já migraram para o IPv6, mas os provedores de conexão, aqueles que dão o acesso à internet, estão em fase de implantação do IPv6. Essa disparidade acabou gerando um problema para as investigações dos delitos cibernéticos.

A falta de IPs disponíveis para conexões à *internet* e a necessidade de investimento para a implementação do IPv6 fez com que as operadoras de telefonia passassem a utilizar o NAT-44: um sistema no qual um mesmo IP passa a ser compartilhado por muitos usuários ao mesmo tempo. Seria mais ou menos como utilizar um filtro de linha, com diferentes usuários se plugando nas tomadas/entradas de um mesmo IP. Para identificar o usuário seria necessário que cada "tomada" fosse identificada, isto é, cada porta lógica precisaria ser guardada tanto pelos provedores de conexão à *internet*, quanto pelos provedores de aplicações, além do número de IP, data e hora, o que demanda mais investimento. A consequência disso é que, embora os provedores de conexão de *internet* estejam avançando na implementação do IPv6, muitas investigações que dependiam somente da informação referente àquelas conexões efetuadas através do NAT 44 acabaram ficando sem solução.

A seguir temos os *links* de vídeos explicativos produzidos pelo nic.br, braço executivo do CGI, que dão uma explicação didática sobre o funcionamento da *Internet.* Os vídeos mais importantes são o primeiro, sobre o Protocolo IP e o quarto sobre Governança da *Internet.*

1.Como funciona a internet ? Parte 1: O Protocolo IP
https://www.youtube.com/watch?v=HNQD0qJ0TC4

2.Como funciona a internet ? Parte 2: Sistemas Autônomos
https://www.youtube.com/watch?v=C5qNAT_j63M&t=41s

3. Como funciona a internet ? Parte 3: DNS
https://www.youtube.com/watch?v=ACGuo26MswI

4. Como funciona a internet ? Parte 4: Governança da Internet
https://www.youtube.com/watch?v=ZYsjMEISR6E

Investigação em crimes cibernéticos

A forma mais tradicional de investigação de delitos cometidos por meio da *internet* ou de sistemas de computação é a identificação do IP, data e hora da conexão à *internet* ou ao sistema informático. Porém, dependendo do meio empregado para cometimento do crime ou do tipo de prova digital que se precisa obter para a elucidação de um delito, a forma de investigação será diferente.

Podemos elencar como formas mais comuns de criminalidade cibernética:

a) Fraudes bancárias (furto e estelionato eletrônicos)*:* arts. 155, §§ 3º e 4º, II, e 171 do Código Penal

b) Falsificação e supressão de dados: arts. 297, 298, 299, 313-A, 313-B do Código Penal

c) Invasão de dispositivo informático e furto de dados: art. 154-A do Código Penal (introduzido pela Lei "Carolina Dieckman)

d) Cyberbullying/Revenge Porn (criação e publicação de perfis falsos visando a veiculação de ofensas em blogs e comunidades virtuais inclusive com a publicação não autorizada de fotos da vítima nua ou em situações vexatórias) – arts. 138, 139, 140 do Código Penal

e) Ameaça: art. 147 do Código Penal

f) Incitação e apologia de crime - arts. 286 e 287 do Código Penal

g) Interrupção de serviço art. 266, § 1º do Código Penal

h) **Terrorismo cibernético** – Lei 13.260/2016: Prática de atos terroristas servindo-se de mecanismos cibernéticos art. 2º, IV – praticado por razões de xenofobia, discriminação ou preconceito de raça, cor etnia e religião – finalidade: provocar terror social ou generalizado

i) Publicação, troca, obtenção, posse de vídeos e imagens contendo pornografia infantil, simulação: art. 241-A, 241-B e 241-C do ECA – Estatuto da Criança e do Adolescente

j) Assédio e aliciamento de crianças: art. 241-D do ECA – Estatuto da Criança e do Adolescente

k) Discurso do ódio: discriminação e preconceito - art. 20, §2º da lei 7.716/89

l) Injúria racial – art. 140§3º do Código Penal

m) Crimes contra a propriedade intelectual e artística - art. 184 do Código Penal e lei 9.609/98

n) Venda ilegal de medicamentos– art. 273 do Código Penal

Neste estudo vamos principalmente analisar os delitos envolvendo discurso do ódio na *internet*, isto é, discriminação e racismo e pornografia infantil na *internet*, comentando os demais delitos.

Dos crimes

a. As fraudes bancárias ocorrem principalmente pela clonagem de cartões de débito e de crédito e pelo direcionamento de usuários para páginas falsas na *internet* onde o usuário é induzido a informar seus dados bancários e senhas, imaginando estar atualizando dados no App do banco onde mantém conta-corrente ou outras. Em geral, são quadrilhas com atuação por todo o país, dificultando as investigações, principalmente porque as fraudes envolvem pequenas quantias que não parecem um grande prejuízo, mas que quando somadas revelam o montante do desfalque que tais criminosos alcançam. Para investigar e combater essas fraudes, foi desenvolvida uma ferramenta apta a armazenar e cruzar os dados referentes a cada fraude de forma que seja possível mapear as quadrilhas, identificá-las e prender os criminosos que operam o sistema de fraudes. Essa foi a Operação Tentáculos.

b. A inserção de dados falsos em sistema de informações ou banco de dados da Administração Pública e a modificação ou alteração não autorizada em sistema de informações são crimes praticados por funcionário público contra a administração pública e que são crimes cibernéticos próprios porque o elemento sistema informático integra o tipo penal. Quando tais condutas são praticadas por qualquer pessoa em sistemas informáticos que não são da administração pública, elas poderão se amoldar ao tipo penal da falsidade ideológica – art. 298 CP – ou seja, utilizamos o tipo penal comum para encaixar a conduta praticada pelo meio informático, já que não há tipo penal específico.

c. A conduta de invadir dispositivo informático e furto de dados foi introduzida no Código Penal com a criação do tipo penal do artigo 154-A pela Lei 12.737, de 2012. A aprovação dessa lei foi impulsionada pelo furto de fotos da atriz Carolina Dieckman de seu *notebook* pessoal.

Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o 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:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

Esse tipo penal recebe críticas por exigir que o acesso indevido a um dispositivo informático, conectado à *web* ou não, se dê mediante a violação de um mecanismo de segurança, o que acaba isentando de pena outras formas de acesso indevido, além de exigir a finalidade específica de obter vantagem ilícita. Outra crítica que se faz a esse tipo penal é o fato de que no parágrafo 3º não há menção a fotografias privadas, como é o caso dos *nudes* que costumam ser utilizados para extorsão e/ou para desmoralizar a vítima com a sua ampla divulgação na *internet*, também conhecida como pornografia de vingança ou *revenge porn*.
Os artigos 154-A, mais seu §1º, mais o artigo 158 do Código Penal (extorsão) podem vir a caracterizar o *Ransomware*, sequestro de dados de um computador mediante a inserção de um *malware* e posterior extorsão- frequentemente em troca de *bitcoins* ou outra moeda virtual.

d. O chamado *revenge porn*, exposição de fotos íntimas da vítima, em geral com o motor da vingança e desejo de expor a vítima a situação vexatória, costuma ser associado aos delitos contra a honra, pois frequentemente vem acompanhado da injúria e difamação. No entanto, esses tipos penais não possuem agravamento pelo meio empregado, o que é de suma importância uma vez que a divulgação por meio da internet aumenta os danos à vítima. Também a simples exposição das fotos íntimas não se subsome por si só a nenhum delito, deixando sem a proteção do delito penal tais condutas. Existe hoje em tramitação na Câmara dos Deputados o Projeto de Lei 5.555/2013 que prevê a criminalização da simples exposição de fotos íntimas, bem como o agravamento da pena pela sua divulgação na internet.

Tal conduta, quando ocorre no ambiente escolar, ganha os contornos do *Cyberbullying*, que engloba a exposição de fotos íntimas de adolescentes – em geral ex-namorados – bem como humilhações entre estudantes. Essas condutas se subsomem à tipificação como divulgação de pornografia infantil e aos delitos contra a honra. Porém, quando praticados por adolescentes acabam por configurar ato infracional sujeitos ao juízo da infância e juventude onde devem merecer a devida repreensão face aos danos morais e físicos que têm como consequência na vida de adolescentes, muitos chegando a cometer o suicídio.

e. Vale destacar também o delito de interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública previsto no artigo 266 do Código Penal que se diferencia do terrorismo cibernético, introduzido pela Lei 13.260/2016, já que este segundo prevê a prática de atos terroristas servindo-se de mecanismos cibernéticos praticados por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião com a finalidade de provocar terror social ou generalizado.

Ressalte-se que a Lei 13.260/2016, promulgada no ano em que o Brasil sediou os Jogos Olímpicos, teve aplicação no mesmo ano com a Operação *Hashtag* a qual frustrou um atentado terrorista que estava sendo planejado para acontecer durante as Olimpíadas – lembrando que é a primeira lei que tipificou atos preparatórios como crime – porém, não se tratou de terrorismo cibernético, pois este, para estar tipificado, precisa utilizar-se dos meios cibernéticos para sabotar o funcionamento ou apoderar-se do controle total ou parcial, ainda que de modo temporário, de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento.

Conclusão

É importante que haja uma adaptação da nossa legislação com a previsão específica de determinados tipos penais que somente podem ocorrer através da internet ou de sistemas informatizados devido às suas peculiaridades.

Embora na maioria dos casos seja possível dizer que a conduta cometida se amolda ao tipo penal já existente e foi cometida pelos meios cibernéticos, muitas outras práticas criminosas somente são possíveis de ocorrer se praticadas pela *internet* ou por sistemas informatizados, o que pode vir a causar impunidade e dificuldade na sua prevenção e repressão.

Tendo em vista a natureza transfronteiriça da *internet*, revela-se a importância da cooperação jurídica internacional no combate a esses delitos, sendo por isso tão premente que haja uma uniformização nos tipos penais e nos meios de investigação, para que a cooperação possa ocorrer de forma mais fluida e rápida, posto que conhecido o arcabouço jurídico que embasará tais investigações também transfronteiriças.

É urgente a adesão do Brasil à Convenção de Budapeste, conhecida como Convenção do Cibercrime que desempenha tal papel descrito acima.