DOS CRIMES VIRTUAIS - implicações legais, prevenção e medidas diante da sua ocorrência

A atuação de criminosos nos ambientes virtuais cresceu drasticamente após meados do ano de 1990, onde houve uma expansão da era digital no Brasil. Antes disso não havia nenhuma tipificação de delitos cibernéticos, pois não era comum e tampouco difundido o uso de meios digitais.

Ocorre que com o passar do tempo o uso de internet tem aumentado de maneira exponencial e por consequência os crimes neste ambiente também. A falsa sensação de anonimato acaba culminando na prática de tais atos ilícitos, visto que sabemos que uma das dificuldades na internet é a identificação do transgressor, mas isso não quer dizer que se propaga a impunidade.

A internet para alguns é tida como um território livre, sem lei e sem punição, todavia esse cenário é diferente, vez que o judiciário vem coibindo a sensação de impunidade dos delitos cometidos no meio virtual, bem como com o passar dos anos vem surgindo previsões legais tanto no que concerne a punição dos crimes cibernéticos, regulando a prática do comércio eletrônico, guarda e tratamento de dados pessoais e sigilosos, dentre outros assuntos atrelados ao meio digital.

Sobre o assunto a Lei n. 12.737 de 2012 - dos crimes cibernéticos - chamada Lei Carolina Dieckmann, foi precursora, ou seja, a primeira lei a contemplar duas tipificações penais, incluindo no Código Penal nos artigos 154 – A e B a previsão sobre o delito de invadir dispositivo informático alheio conectado ou não à rede de computadores, mediante violação indevida de mecanismos de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressão ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Portanto, nos deparamos com as possíveis condutas: invadir computadores, roubar senhas, violar dados de usuários e divulgar informações.

Essa lei ganhou essa denominação após a atriz Carolina Dieckmann ter sido vítima de furto das suas fotos de seu dispositivo móvel.

Podemos considerar então, o furto de identidade praticado no ambiente virtual como incluso na previsão acima (art. 154-A) e que consiste no golpe que envolve perda de informações pessoais, números de cartões, senhas, nomes de usuários e dados bancários, através da invasão de dispositivo móvel, onde o objetivo de quem comete este delito é praticar fraudes com os dados alheios para obtenção de vantagem indevida. Tal ato também pode igualmente configurar o crime de falsa identidade incluso no art. 307 do Código Penal.

O meio mais comum e utilizado pelos criminosos para esse delito é o *Pisching*, ou seja, o indivíduo envia mensagens falsas à vítima a fim de conseguir ter acesso à informações sigilosas.

Importante acrescentar que se, depois de obter conteúdo sem autorização o criminoso divulgar, vender ou transmitir os dados ou informações obtidas a qualquer pessoa, a pena aumentar-se-á de um a dois terços.

É notório o fato de que as redes sociais movimentam muito o uso da internet em todo mundo, seja com o objetivo de lazer ou profissional, e por causa disso se tornaram o alvo de roubos de informações, isso também em razão dos dados terem um valor para mercado, e igualmente as redes sociais proporcionarem um excelente ambiente para proliferação de vírus para posterior implementação de fraude.

E no caso de ser vítima do roubo de contas ou de identidade na internet, aconselha-se a proceder: a) agir rápido procurar um computador e bloquear a conta ou dispositivo móvel roubado ou furtado; b) comunicar a aplicação nas redes sociais, que a conta foi furtada; c) solicitar o bloqueio do chip antigo e adquirir um novo; d) modifique suas senhas; e) faça um boletim de ocorrência;

Cabe citar que são igualmente crimes: a) produzir, oferecer, distribuir ou difundir dispositivo ou programa de computador que sirva para cometer o crime previsto no art. 154-A do CP; falsificar cartão de crédito ou débito.

Em 2014, o Marco Civil da Internet ("MCI") cuidou de tutelar os direitos e deveres dos internautas, protegendo os dados pessoais e a privacidade dos usuários. De forma, que somente mediante ordem judicial pode haver quebra de dados e informações particulares existentes em sites ou redes sociais.

Outro ponto é sobre a retirada de dados e conteúdo da internet, o que antes do advento do MCI não havia regra clara sobre o assunto. E atualmente só é possível igualmente por ordem judicial com exceção de casos que versam sobre pornografia infantil ou pornografia de vingança – ou seja, nesta situação as pessoas vítimas de violação de intimidade podem solicitar a retirada do conteúdo, de forma direta aos sites ou serviços que hospedem esse conteúdo.

São cautelas para evitar o furto de identidade na internet:

- **a)** Seja crítico, desconfie de tudo;
- **b)** Não divulgue informações pessoais – notadamente data de nascimento; endereço etc;
- **c)** Não abra e-mails considerados *spam;*
- **d)** Não responda sms que contenha *link*;
- **e)** Instale um bom antivírus; firewall e malware e os mantenha atualizados, e frequentemente realize uma varredura;
- **f)** Troque suas senhas regularmente, ou diante de um *login* desconhecido;
- **g)** Implemente a autenticação em dois fatores;
- **h)** É aconselhável ter senhas longas, com números, letra em maiúsculo e símbolo;
- **i)** Controle sua conta bancária;
- **j)** Proteja sua rede sem fio;
- **k)** Evite conectar-se a internet pública ou rede compartilhada;

Porém há outros delitos igualmente cometidos no âmbito virtual: insultar a honra de alguém (art. 138 – calúnia); espalhar boatos eletrônicos sobre determinada pessoa (art. 139 –

difamação); insultar pessoas considerando suas características ou utilizar apelidos grosseiros (art. 140 – injúria); ameaçar alguém (art. 147 – ameaça); utilizar dados da conta bancária de outrem para desvio ou saque de dinheiro (art. 155 – furto); comentar, em chats, e-mails e outros, de forma negativa, sobre raças, religiões e opção sexual etc. (art. 20 da Lei n. 7.716/89 preconceito e discriminação); enviar ou compartilhar fotos de crianças nuas (art. 247 do ECA – pedofilia).

Como se denota, mesmo diante de inexistência de previsão legal especifica sobre os delitos cometidos no ambiente digital, o Superior Tribunal de Justiça atuando como uniformizador da legislação infraconstitucional firmou o entendimento da aplicação da legislação existente. Como por exemplo, nos casos de furto e estelionato virtual que compreendem a apropriação de valores em conta corrente mediante transferência fraudulenta via internet sem o consentimento do correntista configura furto qualificado pela fraude, vez que este última é utilizada para burlar o sistema de proteção e vigilância do banco sobre os valores mantidos sob sua guarda. Também decidiu que competência para julgar esse tipo de crime é o do juízo do local da consumação do delito de furto, que se dá no local onde o bem é subtraído da vítima.

Também configura crime a criação de sites na internet para vender mercadorias com a intenção de nunca as entregar, o que caracteriza o crime contra a economia popular – previsto no artigo 2º, inciso IX da Lei n. 1.521/51.

Outro delito muito comum é a propagação de ofensas via internet, o que culmina nos delitos contra a honra, tais atos não se confundem com a liberdade de expressão abarcada pelo MCI, e estão sujeitos a punição tanto no âmbito penal como civil, com a competente reparação de danos.

Isto se dá em razão da propagação de informações falsas, vexatórias, compartilhamento de imagem ou vídeo pornográfico, ou disseminação de ofensas e contra a honra de um indivíduo acarretarem grandes prejuízos de ordem moral, econômica e psicológica à vítima, como repúdio de amigos (as) e familiares, afastamento social, perda de emprego etc. Até mesmo porque uma vez propagado um conteúdo na rede não mais possível o controle sobre sua visualização e compartilhamento, sendo que em alguns casos há até a viralização.

O Direito a preservação da intimidade e privacidade são, como dito acima, tutelados pelo MCI mas também nossa constituição no art. 5º, inciso X: "*São invioláveis e intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação".*

É importante mencionar que o Marco Civil da Internet fixou a competência dos Juizados Especiais para decidir sobre a ilegalidade ou não dos conteúdos. Isso se aplica aos casos de ofensa a honra ou injúria – que serão tratados da mesma forma como os que acontecem fora da internet. Não importa, assim, o lugar do provedor de acesso e será sempre considerado o lugar da consumação do delito – como prescreve o art. 70 do CP.

Impende mencionar que os provedores de conteúdo que não acatarem em 48 (quarente e oito) horas uma ordem judicial para remoção de determinado conteúdo ou solicitação do usuário em caso de pornografia infantil ou vingança pornográfica poderá ser

responsabilizado – eis um debate e proposta de mudança legislativa de forma a contemplar especificamente esta hipótese.

Porém, diante da hipótese de ser vítima um crime contra honra na internet, o que devemos fazer?

a) É aconselhável reunir provas do crime (print/captura da publicação, da imagem, anotar o endereço eletrônico onde o crime foi cometido; etc), é importante salvar estas informações, vez que os criminosos tendem apagar rapidamente a publicação. Não se deve realizar modificações nas imagens e comentários, o conteúdo deve ser apresentado na sua forma original. Se puder, se dirija à um tabelionato de notas e registre tais provas e conteúdo numa ata notarial – a qual terá fé pública;
b) É valido reunir testemunhas que estejam dispostas a relatar o ocorrido ao juiz;
c) Registre um Boletim de Ocorrência numa delegacia especializada em crimes eletrônicos, ou numa Delegacia comum caso não exista uma especializada na sua região;
d) É indicado ingressar com uma representação criminal e também com uma ação civil para reparação de danos morais e materiais, bem como para remoção do conteúdo das redes sociais;
e) As redes sociais geralmente permitem à vítima que denunciem o crime, ou seja, a publicação, ofensa, imagem não autorizada, etc;
f) Procure um (a) advogado (a) para lhe auxiliar.

Como sabido, são inúmeras as utilidades e facilidades da internet, e por outro lado os delitos cometidos em tal meio são também diversos, e vão desde crimes que ofendem a honra da pessoa (calunia, difamação, injurias raciais, bullying) como os que invadem a privacidade do usuário, seu patrimônio (através de fraudes financeiras), e usurpação de dados particulares, pessoais sigilosos. Com o desenvolvimento e necessidade da sociedade surgem normas, utiliza-se muitas vezes da analogia e dos princípios do direito para resolução dos casos, e assim trabalham os tribunais com o intuito de sanar as lacunas legislativas e criar precedentes hábeis a tutelar dos direitos e gerar sanções para os transgressores da lei, notadamente no que concerne ao Direito Digital do qual não há um código ou regulação especifica.

Assim, mesmo diante da ausência de previsão especifica, os crimes e atos perpetrados no meio digital não ficarão sem punição e aplicação da lei competente, sendo possível a todas as pessoas atingidas recorrerem à justiça para garantir o seu direito e também em alguns casos a justa reparação.

- **AUTORA.:**

DAIILLE COSTA TOIGO.

Doutoranda em Direito Comercial pela Pontifícia Universidade Católica de São Paulo/SP (PUCSP).

Mestre em Direito Comercial pela Pontifícia Universidade Católica de São Paulo/SP (PUCSP).

Pós-Graduada e especialista em Direito Comercial pela Pontifícia Universidade Católica de São Paulo/SP (COGEAE/PUCSP) em 2011;

Graduada em Direito pela Fundação Armando Álvares Penteado – FAAP, 2007

Autora dos livros:

"*Planejamento Sucessório Empresarial*: proteção patrimonial nacional e internacional" pela Editora AGWM. São Paulo. 2016

"*Internet Banking*: a responsabilidade civil das instituições financeiras", Editora AGWM. São Paulo. 2016

Palestrante. Advogada e consultora empresarial.

ATUAÇÃO PROFISSIONAL

No Direito Empresarial e Digital.

Ministra treinamento e palestra para empresas, operadores do Direito, e instituições bancárias sobre o tema Planejamento Sucessório e em São Paulo e demais Estados, bem como Lei Geral de Proteção de Dados.

Sócia proprietária do Escritório de Advocacia Costa Toigo.

COSTA TOIGO ADVOCACIA

daiille@costatoigoadv.com.br

www.costatoigoadv.com.br