Fernandes: Os crimes virtuais praticados na Covid-19

Considerando que a internet é uma ciência nova, se comparada com os demais ramos de estudo e pesquisas, como Engenharia, Medicina e áreas pontuais do Direito. Assustadoramente, a internet vem crescendo rapidamente, dominando o sistema, demitindo funcionários pela sua eficiência e facilidade em organização, armazenamento, manutenção e acúmulo de dados. De acordo com a *Fortinet Threat Intelligence Insider Latin America*, o Brasil sofreu mais de três bilhões de tentativas de ataques na

Nesse passo, existe um grande perigo e um afastamento da lei com a potência de atualização da internet e aplicativos, e, como sempre brinco nas palestras e aulas: a legislação sobe de escada enquanto a sociedade sobe de elevador, a cada degrau uma dificuldade para alcançar, a sociedade postando fotos, falando em *lives*, fazendo negócios em todo o mundo, transferindo dinheiro e conhecimento na cobertura do prédio.

Sendo assim, é de fácil percepção que a necessidade do Direito de existir é de pacificar um conjunto de normas para o convívio em civilização, ou seja, entre tais normas, existem as do Código Penal, que preveem crimes, no entanto, nem todos realizados na modalidade virtual/eletrônica.

Como estamos falando de uma legislação que ainda se encontra no primeiro degrau (o Código Penal é de 7 de dezembro de 1940), ainda temos outras leis, projetos de leis e várias formas de aplicar o que é feito na modalidade virtual à vida real (cobertura do prédio).

Dessa maneira, é necessário explicar alguns crimes comuns, algumas formas de se precaver e, principalmente, de buscar seus direitos.

Passamos, então, a tratar a questão da responsabilidade, seja criminal ou cível, mas em matéria do que acontece sobre o prisma da era digital e com base na LGPD (Lei Geral de Proteção de Dados).

Anonimato
O direito à liberdade de expressão é garantido pela Constituição Federal brasileira e considerado como direito fundamental por estar garantida pelo Pacto Internacional de Direitos Civis e Políticos. A liberdade de expressão não é absoluta, então, ainda que se cometa sobre esse prisma excessos, caberá a punição, grande problema que temos, é que por de trás das telinhas, na grande rede, é possível assumir e construir uma identidade livre de condicionamentos (podem ser omitidos o nome e a condição econômica e social do indivíduo).

Toda tentativa de limitar a possibilidade do anonimato (como, por exemplo, obrigando o usuário a fornecer a própria identidade ao gestor da rede, que poderia revelá-la somente ao magistrado em caso de crime ou dano civil) violaria um dos pontos cardeais da internet e, hoje em dia, violaria também a Lei Geral de Proteção de Dados. Quando algum dano é causado por usuário anônimo, é possível identificar o computador que utilizou pelo seu *internet protocol* (IP), com a gravação de endereço do usuário, o que muitas vezes demora meses, perícia e profissionais preparados para alcançar.

Em que pese haja o entendimento do STJ de que a identificação do IP é importante e suficiente para identificação de usuário anônimo, é válido lembrar que o IP identifica uma máquina, e não uma pessoa, o que prejudica determinados casos, haja vista as opções de *lan houses*, cafeterias e bibliotecas, onde o somente o IP se mostra insuficiente para identificação de um usuário. Dito isso, vamos tratar então dos crimes que em que existe diretamente a identificação de autoria.

Cyberbullying
Cyberbullying, na verdade, nada mais é do que um tipo de violência eletrônica derivada do *bullying* , em que as agressões se dão através da própria internet ou de outras tecnologias relacionadas.

Praticar *cyberbullying* significa usar o espaço virtual para intimidar e hostilizar uma pessoa, difamando, insultando ou atacando covardemente, em geral essas práticas estão relacionadas a crimes já previstos no Código Penal, o que muda é a forma em que passam a ser praticados.

Além disso, a prática dessas ofensas desencadeia efeitos também na esfera cível, entre elas a obrigação de reparar os danos morais ou materiais proporcionados pelos autores das ofensas, conforme preceitua o artigo 159 do Código Civil brasileiro, onde aquele que por ação ou omissão voluntária, negligência, imperícia ou imprudência violar o direito ou causar prejuízo a outrem fica obrigado a reparar o dano.

Como não é difícil de entender, como se tratam de crimes cibernéticos, é óbvio que toda ação deixa rastro probatório, e é por meio desses rastros que a pessoa que sofreu o aludido crime consegue fazer valer seus direitos. As vítimas podem ajudar e muito na descoberta agressor, tomando medidas simples como imprimir imediatamente as páginas onde constam as agressões, identificar as comunidades que são criadas com o intuito de manchar a imagem da vítima, enfim, produzir provas da agressão virtual vem a ser o primeiro passo, deixando a identificação dos autores, em alguns casos, para a delegacia competente.

Lembrando ainda que a modalidade que mais cresce nos aplicativos de mensagens é o envio de *nudes* , e, se for menor de idade, o artigo 241 do Estatuto da Criança e do Adolescente (ECA) qualifica como crime grave a divulgação de fotos, gravações ou imagens de crianças ou adolescentes em situação de sexo explícito ou pornográfica.

Apenas de passagem, abaixo elencamos os crimes mais comuns:

Calúnia: afirmar que a vítima praticou algum fato criminoso. Um exemplo comum seriam as mensagens deixadas no perfil de determinado usuário de uma rede social ou site de relacionamento imputando a ele a prática de determinado crime. Exemplo: dizer que certa pessoa praticou o crime de furto ou estupro.

Difamação: é imputar um fato a alguém que ofenda sua reputação, pouco importando se o fato é verdadeiro ou não, o que importa é que atinja a sua honra objetiva. Exemplo: fulana de tal é devedora, ou nos casos de fotos vazadas que viralizam na internet.

Injúria: é ofender a dignidade ou o decoro de outras pessoas, atingindo a sua honra subjetiva. Geralmente se relaciona a xingamentos que são postados no Facebook da vítima. Uma pessoa que filma a vítima sendo agredida ou humilhada e divulga no YouTube também pratica o delito. Tal fato pode ser ainda mais gravoso se decorre de elementos como raça, cor, etnia, religião ou com pessoas em condições diferenciadas (criança, idosos, portadores de necessidades especiais).

Ameaça: ameaçar a vítima de mal injusto e grave. O mais comum seria a vítima informar a autoridade policial que está recebendo ameaças de morte via *short message service* (SMS), mensagens *inbox* , telefonemas entre outras.

Constrangimento ilegal: em relação ao *cyberbullying*, esse crime se consuma no momento em que a vítima faz algo que não deseja fazer e que a lei não determine. Por exemplo, se um garoto envia uma mensagem instantânea para a vítima dizendo que vai agredir um familiar da mesma caso não aceite ligar a câmera do seu computador (*webcam*), nesse caso a pena é de detenção de três meses a um ano ou multa.

Falsa identidade: ação de atribuir-se ou atribuir a outra pessoa falsa identidade para obter vantagem em proveito próprio ou de outro indivíduo ou para proporcionar algum dano. Por exemplo, a utilização de perfis falsos em sites de relacionamento, no caso uma mulher casada que se passa por solteira para conhecer outros homens e vice-versa, ou até mesmo utilizar a foto de um desafeto para criar um perfil falso e proferir ofensas contra diversas pessoas, visando a colocar a vítima em situação embaraçosa e constrangedora. Caso também se aplica aos famosos que possuem perfis feitos com suas fotos e nomes mas que não administram e nem possuem conhecimento do que é feito ali.

Vem se tornando cada vez mais frequente o ingresso de ações judiciais envolvendo crimes praticados em redes sociais, especialmente Facebook e Instagram, e aplicativos como Whatsapp, entre outros. Na maioria dos casos, ações judiciais envolvendo crimes contra a honra, ou seja, crimes de calúnia, difamação e injúria, já citados acima.

A proteção está prevista no artigo 5º, X da Constituição Federal: *"São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou decorrente de sua violação"*.

O estelionato, que, como a lei determina, é fraude que induz alguém a uma falsa concepção de algo com o intuito de obter vantagem ilícita para si ou para outros. Nessa modalidade, acaba que conseguimos enquadrar a maioria dos golpes usados no espaço virtual.

O golpe do WhatsApp clonado
Esse é o recordista em tempos pandêmicos, e acredite, vem dividindo os tribunais sobre a responsabilidade. As ações contra as companhias telefônicas por motivo de WhatsApp clonado já são uma realidade em todos os tribunais do Brasil, e o cliente pode receber indenização pelo transtorno, pelos prejuízos financeiros e pelo próprio risco sofrido. Um golpe que está ganhando força é o do WhatsApp clonado. Existe uma modalidade desse golpe que o criminoso apenas invade o aplicativo e tenta extorquir os contatos do dono do celular. Mas há uma modalidade do golpe que traz consequências mais danosas ao consumidor: a clonagem do chip do celular, seja por meio de WhatsApp Web e até mesmo por descuido da operadora na hora de vender um novo chip ou não fornecer proteção quando houver fornecimento de dados pelo telefone. O dono da linha tem seu telefone invadido e pode perder o número.

A maioria das pessoas só repara que são vítimas de clonagem de WhatsApp quando seus conhecidos recebem mensagens estranhas em que se solicitam depósitos em dinheiro com urgência. Essa é talvez a prática mais comum nesse tipo de crime.

Ainda muito usado é o golpe do envelope na boca do caixa: a pessoa utiliza a máquina de depósito bancário para depositar um envelope vazio e com ele, "comprovar" pagamento. Na verdade, para o banco o dinheiro só entra na conta quando passar pela conferência de valores, mas infelizmente, várias pessoas já foram lesadas com essa modalidade de golpe, elas pegam no banco o comprovante de depósito do envelope e o apresentam ao possuidor do bem, que o entrega de boa-fé e cai no golpe, também conhecido como "golpe do envelope vazio", e só funciona por uma brecha no sistema de depósito por envelope em caixa. Esse equívoco é sobre o valor depositado estar bloqueado. Com isso, o criminoso mostra o comprovante, o que induz a pensar que o dinheiro foi depositado, quando não foi. Portanto, o golpe do envelope vazio é uma prática criminal realizada por um estelionatário em que o envelope depositado não tem conteúdo. Esse crime é um aproveitamento da inocência do vendedor ou beneficiado que esquece de checar junto ao banco se o valor foi depositado.

Veja bem, o crime de estelionato exige quatro requisitos intrínsecos e obrigatórios para sua caracterização: 1) obtenção de vantagem ilícita;
2) causar prejuízo a outra pessoa; 3) uso de meio de ardil, ou artimanha; 4) enganar alguém ou a leva-lo a erro.

Entendendo que muitas vezes os quatro requisitos são supridos e realizados facilmente na modalidade virtual, inclusive com um aumento significativo de quase 70% dos crimes na pandemia, sejam eles:

Phishing
Que nada mais que é o crime de enganar as pessoas para que compartilhem informações confidenciais como senhas e número de cartões de crédito. Como em uma verdadeira pescaria, há mais de uma maneira fisgar uma vítima, mas uma tática de *phishing* é a mais comum.

Golpe do cartão de crédito ou boleto bancário
O que acontece é que muitas vezes o usuário, sem perceber, é infectado com um *software* malicioso, que contamina as máquinas com o objetivo de roubar senhas bancárias ou do cartão. Automaticamente, possuindo a senha, faz compras e acaba com a estabilidade emocional da vítima. No caso de um boleto bancário, criminosos geram um documento forjando e simulando a compra de um *e-commerce*, ou até mesmo de um boleto de pagamento mesmo, e encaminha para quitação.

Nesse momento, o código de barras é trocado e o dinheiro pago vai para outra agência e conta. O usuário de boa-fé só descobre que caiu no golpe quando a empresa cobra o pagamento do produto novamente ou da conta novamente. Esse golpe demora algumas vezes, meses para ser descoberto, o que normalmente dificulta a empresa a identificar a fraude e a polícia a chegar aos criminosos.

Mobile malware
Considerado um golpe mais sofisticado, trata-se de vírus desenvolvido por *hackers* que se instala nos computadores ou celulares com a função de roubar todas as informações pessoais do usuário, bem como suas senhas e dados bancários.

Recomendação final
Reúna documentos e provas contra a pessoa criminosa (endereço, nome completo, capturas de tela, e-mails, descrição física e afins); contate um advogado para abrir um processo em desfavor de quem gerou o prejuízo, ou sob quem tinha a responsabilidade de evitá-lo; utilize as provas reunidas previamente e possíveis testemunhas; tente descobrir o IP ou o número utilizado pelos criminosos, se for o caso, dê *print* de tudo; em determinadas ações pode ser necessário fazer uma ata notarial de modo a preservar a prova (um ato notarial por meio do qual o tabelião — a pedido de parte prejudicada — lavra um instrumento público formalizado pela narrativa fiel de tudo aquilo que verificou por seus próprios olhos, sem juízo de valores), procure sempre que necessário a delegacia especializada.

Date Created
24/05/2021