CRIMES PELA INTERNET, NOVOS DESAFIOS PARA A JURISPRUDÊNCIA

Publicada em 17/06/2018 | **Link para a matéria**

Foto: iStock (https://www.istockphoto.com/br)

Os crimes cibernéticos no Brasil afetam anualmente cerca de 62 milhões de pessoas e causam prejuízo de US$ 22 bilhões, de acordo com estudo divulgado no início de 2018 pela empresa de segurança virtual Symantec.

Segundo o especialista em segurança da informação do Superior Tribunal de Justiça (STJ) Antonio Horácio Boa Sorte, os riscos estão relacionados principalmente à forma como o usuário faz uso da tecnologia. “Obter conhecimento a respeito do assunto ainda é a melhor forma de evitar ser vítima”, afirmou.

Para aumentar a segurança enquanto navega na internet, Antonio Horácio aconselha evitar redes *wifi* gratuitas (em restaurantes, por exemplo); utilizar, quando disponível, navegação anônima, por meio de *anonymizers* ou de outras opções disponibilizadas pelos navegadores; e ter cuidado no uso de cookies, pois eles podem servir para rastrear e manter as preferências de navegação do internauta.

Além de sempre manter o antivírus atualizado também nos dispositivos móveis, como o celular, é fundamental, segundo o especialista, que o usuário seja cuidadoso ao acessar sites de comércio eletrônico, sempre verificando se a página utiliza conexão segura.

Outras importantes dicas são usar apenas programas originais e nas versões mais recentes, e ser cauteloso ao acessar a internet em locais públicos.

O uso cada vez mais intenso e diversificado da internet vem abrindo caminhos para a prática de novas fraudes, ou para novas formas de cometimento de velhos crimes, em casos nem sempre fáceis de enquadrar no ordenamento jurídico. O Superior Tribunal de Justiça (STJ) tem sido acionado para apresentar a correta interpretação das normas infraconstitucionais em relação aos ilícitos praticados pela rede.

EXTORSÃO

Recentemente, o tribunal decidiu manter preso preventivamente um homem que usou a internet para obter fotos e vídeos com conteúdo erótico e depois extorquiu mulheres para não divulgar as imagens.

Por meio das mídias sociais, um rapaz de 19 anos compelia jovens (algumas menores de idade) a enviar fotos e vídeos íntimos, e depois exigia que elas lhe entregassem dinheiro e outros bens para não divulgar o material na internet. Ele também estendia as ameaças às famílias das vítimas.

Para o ministro que relatou o caso no STJ, Rogerio Schietti Cruz, ficou nítido que o acusado se aproveitou da vulnerabilidade das vítimas no ambiente virtual para exigir os valores, que eram cada vez mais altos a cada ato de extorsão.

Ao negar o habeas corpus, Schietti destacou que os crimes sexuais virtuais são impulsionados pela oportunidade do anonimato e, independentemente dos aspectos que permeiam a vida pessoal e socioeconômica do criminoso, estariam "diretamente relacionados ao comportamento sexista, comumente do gênero masculino" (processo em segredo de Justiça).

MENSAGENS

O STJ tem adotado a tese de que é ilícita a prova obtida diretamente dos dados armazenados no celular do acusado. A jurisprudência do tribunal entende que são inválidas mensagens de texto, SMS e conversas por meio de aplicativos como o WhatsApp obtidas diretamente pela polícia no momento da prisão em flagrante, sem prévia autorização judicial.

No caso analisado (*AgRg no RHC 92.801*), policiais civis acessaram as mensagens que apareciam no WhatsApp do celular do acusado no momento da prisão em flagrante, sem autorização judicial. Para a Quinta Turma, a prova obtida tornou-se ilícita, e teve de ser retirada dos autos, bem como os outros elementos probatórios derivados diretamente dela.

Segundo o ministro que relatou o caso, Felix Fischer, os dados armazenados nos celulares decorrentes de envio ou recebimento de dados via mensagens SMS, programas ou aplicativos de troca de mensagens, ou mesmo por correio eletrônico, dizem respeito à intimidade e à vida privada do indivíduo, sendo, portanto, invioláveis, nos termos do artigo 5°, X, da Constituição Federal.

Em outro caso (*RHC 89.981*), o STJ também anulou provas obtidas por policiais que acessaram as mensagens no celular de um suspeito que indicavam o repasse de informações sobre imóveis onde uma quadrilha pretendia cometer furtos.

"A análise dos dados armazenados nas conversas de WhatsApp revela manifesta violação da garantia constitucional à intimidade e à vida privada, razão pela qual se revela imprescindível autorização judicial devidamente motivada, o que nem sequer foi requerido", concluiu o relator, ministro Reynaldo Soares da Fonseca, ao determinar o desentranhamento das provas.

FURTO ELETRÔNICO

A Terceira Seção do STJ firmou entendimento no sentido de que a subtração de valores de conta-corrente mediante transferência eletrônica fraudulenta configura crime de furto, previsto no *artigo 155*, parágrafo 4º, inciso II, do Código Penal.

Uma discussão frequente em processos que chegam à corte diz respeito ao juízo competente para analisar os casos em que o furto acontece via rede mundial de computadores. Nesses casos, para o STJ, a competência é definida pelo local onde o bem foi subtraído da vítima.

Ao apreciar conflito de competência (*CC 145.576*) em processo que envolveu furto mediante transferência eletrônica fraudulenta de contas-correntes situadas em agência bancária de Barueri (SP) – mesmo tendo os valores sido enviados para Imperatriz (MA) –, o colegiado entendeu que o juízo da cidade paulista tem a competência para julgar o caso, uma vez que os valores foram subtraídos das vítimas a partir dessa localidade.

COMÉRCIO *ON-LINE*

A praticidade é um dos fatores mais atraentes para os consumidores que utilizam serviços ou compram algum produto por meio da rede mundial de computadores. É preciso ficar atento, porém, a golpes praticados por sites que vendem produtos que nunca serão entregues.

De acordo com o STJ (*CC 133.534*), a criação de sites na internet para vender mercadorias com a intenção de nunca entregá-las é conduta que se amolda ao crime contra a economia popular, previsto no artigo 2º, inciso IX, da Lei 1.521/1951.

Segundo a corte, ao criar um site para vender produtos fictícios pela internet, os criminosos não têm por objetivo enganar vítimas determinadas, mas, sim, um número indeterminado de pessoas, vendendo para qualquer um que acesse o site.

Recentemente, um empresário denunciado por induzir a compra virtual de produtos que não eram entregues teve negado seu pedido para que fosse revogada a ordem de prisão.

Ao negar o recurso em habeas corpus (*RHC 65.056*), a Quinta Turma considerou não haver ilegalidade no decreto prisional, baseado, entre outros elementos, na garantia de ordem pública e no risco de reiteração delitiva.

Consta do processo que o denunciado registrava domínios de vários sites e oferecia produtos eletrônicos como *notebooks* e câmeras digitais por valores menores que os praticados no mercado.

AMEAÇA

Nas hipóteses de ameaças feitas por redes sociais como o Facebook e aplicativos como o WhatsApp, o STJ tem decidido que o juízo competente para julgamento de pedido de medidas protetivas será aquele de onde a vítima tomou conhecimento das intimidações, por ser este o local de consumação do crime previsto no *artigo 147* do Código Penal.

Com base nesse entendimento, a Terceira Seção fixou a competência da comarca de Naviraí (MS) para a análise de pedido de concessão de medidas protetivas em favor de mulher que teria recebido pelo WhatsApp e Facebook mensagens de texto com ameaças de pessoa residente em Curitiba (*CC 156.284*).

O relator, ministro Ribeiro Dantas, destacou que o *artigo 70* do Código de Processo Penal estabelece que a competência será, em regra, determinada pelo lugar em que se consumar a infração.

Esta notícia refere-se ao(s) processo(s):
RHC 92801
RHC 89981
CC 145576
CC 133534
RHC 65056
CC 156284