Dodsworth : O crime quase perfeito: delitos nos ambientes digitais

Em março de 2020, os brasileiros se viram obrigados a se adaptar ao "novo normal": empresas instituíram o *home office*, as compras passaram a ser *online* e os encontros, virtuais. Todos tiveram de se crime.

O desenvolvimento da tecnologia e o crescimento de usuários, principalmente em meio à pandemia, possibilitou um aumento do número de crimes virtuais, o que tem preocupado bastante, principalmente as empresas. Recentemente, vimos uma das maiores lojas de comércio varejista do Brasil, as Lojas Renner, sofrer um ataque *hacker* que derrubou o site e os sistemas de pagamento, causando enorme prejuízo. Também não ficaram de fora os sites das cortes mais altas do país, que, em situações distintas, precisaram ter suas atividades paralisadas em razão de ataques aos seus sistemas no último ano. De acordo com estudo realizado pela McAfee, as perdas relacionadas aos crimes cibernéticos chegam a quase 1% do produto interno bruto (PIB) mundial.

Os cibercrimes, como também são chamados, são as infrações penais que acontecem no ambiente digital. Podem ser aqueles velhos conhecidos do Código Penal, como os delitos de estelionato, extorsão, furto, injúria, calúnia, difamação e outros, quando ocorrem por meio da rede mundial de computadores, ou crimes criados especificamente diante desse contexto digital, como, por exemplo, a invasão de dispositivo informático.

A elaboração de novos tipos penais é remanescente, considerando que quase toda conduta fraudulenta praticada em meio virtual se encaixa em um crime já existente. A atuação legislativa, portanto, tem sido no sentido de endurecimento de penas, criando causas de aumento da penalidade e formas qualificadas de crimes, quando praticados em ambiente cibernético.

Ainda assim, vemos muito poucas ações penais por esses delitos chegando ao fim. Há um problema muito anterior ao momento da sentença, que diz respeito à dificuldade de identificação dos autores de crimes dessa natureza. Primeiro, porque em não raros os casos se está diante de pessoas que possuem um amplo domínio da tecnologia, que criam diversos mecanismos para ocultar e dissimular sua identidade, fazendo com que seja extremamente difícil para os investigadores detectar quem são.

2023 - www.conjur.com.br - Todos os direitos reservados.

Nem todos os crimes virtuais, contudo, são praticados por *hackers* e *experts* da tecnologia. Têm crescido exponencialmente os golpes de WhatsApp e aplicativos de entrega, por exemplo, que costumam ter como principais vítimas pessoas comuns, com pouco conhecimento das redes. Os autores, nesses casos, usualmente são pessoas privadas de liberdade com fácil acesso a telefones, mesmo dentro das unidades prisionais.

Até mesmo nos casos em que os autores não são *hackers*, os procedimentos e ferramentas que dispõem as autoridades públicas são extremamente burocráticos e lentos. Somente agora o trâmite nessa fase preliminar tem se tornado eletrônico, e mesmo assim não acompanha a velocidade da prática do crime. Na verdade, a polícia está sempre alguns passos atrás.

A atuação preventiva passa a ser o melhor recurso; é preciso estudar como tornar os eletrônicos um terreno infértil para a prática desses crimes. Isso porque o aumento de penas, além de não surtir quase que nenhum efeito prático no combate à criminalidade, ignora o fato de que muitos desses criminosos praticam a conduta de dentro do ambiente prisional.

A solução passa, em um primeiro momento, pela conscientização dos usuários e das empresas, que precisam se informar sobre as melhores formas de proteger seus dados. No caso das pessoas físicas, o uso de senhas fortes e ferramentas como a autenticação de dois fatores apresentam-se como o primeiro passo para essa proteção. Mesmo seguindo essas medidas, contudo, ainda estarão sujeitos a fraudes, caso não saibam reconhecer sites não confiáveis, links suspeitos e não estejam cientes dos "golpes do momento".

Do ponto de vista coorporativo, torna-se urgente a implementação de sistemas e tecnologias de segurança da informação. Tal sugestão corresponde, inclusive, a uma obrigação imposta pela Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em agosto. O descumprimento das disposições legais pode resultar até mesmo em multa de 2% do faturamento anual da empresa, ou seja, interfere diretamente no financeiro. É importante que as empresas também atuem de acordo com a orientação de advogados sobre as melhores formas de conduta.

Os funcionários, por sua vez, devem receber treinamentos específicos sobre como utilizar os meios digitais, evitando que empregados que não dominam a tecnologia sejam alvos fáceis de entrada de *hackers* nos sistemas empresariais.

No mesmo sentido, as autoridades públicas devem unir esforços para aprimorar suas formas de investigação e combate a essas práticas. Devem ser pensados sistemas mais eficientes, que impeçam, por exemplo, estelionatários de criar contas vinculadas a CPFs de pessoas já mortas. Também precisam ser estudados trâmites mais céleres para auxiliar na identificação e localização dos autores, viabilizando que a polícia consiga rastrear a fonte da prática criminosa sem que se livrem das evidências antes.

Os ambientes digitais evoluíram em uma velocidade muito maior do que fomos capazes de garantir a segurança e privacidade dos usuários. A atuação para a prevenção desses delitos, portanto, se mostra a ferramenta mais eficiente para lidar com eles até o momento.

Date Created
15/09/2021

2023 - www.conjur.com.br - Todos os direitos reservados.