Entrevista Daniel Burg, especialista em crimes virtuais

Spacc

Em 2016, mais de 42 milhões de brasileiros foram vítimas de crimes virtuais. Um aumento de 10% se comparado com o ano anterior, de acordo com dados da Norton, empresa de soluções de segurança cibernética. Segundo esse levantamento, o prejuízo total da prática para o país foi de US$ 10,3 bilhões.

Com a internet, o crime se renovou. Foram criadas novas maneiras de se cometer velhos crimes, explica o advogado **Daniel Allan Burg**, sócio do escritório de Direito Criminal Burg Advogados Associados. No mundo virtual os alvos são variados e a cada dia são criados novos golpes. Um caso contado por Burg para exemplificar é de um taxista que simula corridas como se estivesse atendendo a pedidos de aplicativos de celular. Assim, embolsa o dinheiro sem levar nenhum passageiro e deixa o prejuízo com a empresa responsável pelo aplicativo.

E os problemas dos chamados cibercrimes vão além da pluralidade e da velocidade com que eles se multiplicam. Na visão de Daniel Burg, a internet facilita a impunidade, uma vez que a investigação é mais complicada e, muitas vezes, quando é identificado o autor, já ocorreu a prescrição. Isso sem contar na questão da fronteira: o crime pode ser cometido por alguém que está em outro país, com leis completamente diferentes.

"A fronteira acaba motivando também, de certa forma, a impunidade. E aqui, infelizmente, não tem muito o que fazer. Porque não tem como criar uma lei obrigando o cidadão da Estônia a vir para o Brasil no prazo", comenta.

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

Apesar das dificuldades, o advogado acredita que o trabalho de investigação e a condenação desses criminosos podem ser facilitados se houver investimento, tanto em pessoal e treinamento, quando em leis que hoje são, segundo avalia, mal redigidas e não levam em consideração o modo como acontecem os crimes na internet.

Leia a entrevista:

ConJur — Como o escritório se especializou nesta área de crimes virtuais?
Daniel Burg — Isso começou por conta de um dos primeiros clientes do escritório, uma empresa de pagamento on-line, e todos os casos em que eles figuram como investigados ocorre por uma incompreensão das autoridades policiais acerca das atividades da empresa. Então, naturalmente, a gente teve que se especializar e os resultados positivos fizeram com que o escritório atraísse mais casos desta área.

ConJur — O crime virtual é uma questão recente e em constante evolução. Como o advogado se prepara para atuar nesta área?
Daniel Burg — Além do estudo do Direito Penal, é preciso sempre se aprofundar no estudo das atividades específicas de cada empresa. E é interessante notar que muitas não são reguladas por leis, ou pelo menos há pouco tempo atrás não eram. Então é preciso analisar a própria empresa e até mesmo leis antigas que podem ser adequadas ao caso concreto. Temos um caso que deu visibilidade ao escritório que serve de exemplo em que precisamos explicar que as empresas de intermediação de pagamento não se confundem com instituição financeira, que são reguladas por uma lei antiquíssima e totalmente abrangente. A investigação da Polícia Civil concluiu que a empresa atuava como instituição financeira sem autorização do Banco Central. E coube a nós estudar exatamente no que constitui a atividade da empresa para demonstrar que a conclusão estava errada, pois não se tratava de uma instituição financeira.

Conjur — O que diferencia o crime cibernético de um crime comum cometido pela internet? Um e-mail com ameaça de morte é um crime cibernético ou uma ameaça como outra qualquer?
Daniel Burg — Neste caso, será enquadrado como crime de ameaça como outro qualquer, conforme o artigo 147 do Código Penal. A diferença do crime comum para o cometido pela internet, como no caso exemplificado, está na dificuldade de se identificar o autor, mesmo existindo delegacias especializadas em crimes cibernéticos. E isso é mais um motivador para o cometimento desses crimes.

ConJur — Em que consiste essa dificuldade?
Daniel Burg — A legislação brasileira não está adequada e, muitas vezes, o crime prescreve sem que haja um avanço significativo nas investigações. Nos crimes contra a honra, por exemplo, há uma enorme dificuldade para se identificar o autor de ofensas realizadas na internet, e sem a identificação sequer é possível oferecer queixa-crime.

ConJur — E como é o procedimento para identificar o autor?
Daniel Burg — Vamos supor que o Google seja o responsável por manter os dados cadastrais do autor da ofensa. Nós temos que enviar um ofício à empresa solicitando os dados. O Google apresenta os dados cadastrais mas, com base no Marco Civil da Internet, se recusa a fornecer o IP (*internet protocol*) e outros dados que necessitam de autorização judicial para se obter. Em regra, até o Google responder

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

isso, a autoridade policial remeter o inquérito para o fórum e ter a representação judicial, um considerável tempo já se passou. É preciso ser bastante claro com o cliente que procura um advogado com esse tipo de caso de que é possível que o resultado almejado pode não ser alcançado por causa desses entraves. Além disso, nós que atuamos nessa área precisamos ficar atentos e cobrar celeridade nesse processo. De certa forma a internet criou a impunidade para a prática de alguns crimes.

ConJur — Podemos concluir então que a internet facilitou a prática desses crimes?
Daniel Burg — Facilitou é uma boa definição. Os crimes continuam os mesmos, mas se aumenta a gama da forma como eles podem ser praticados. Antigamente o sujeito que queria obter R$ 200 mil ia pegar uma arma e assaltar um banco. Hoje, se ele tem um conhecimento virtual um pouco mais avançado, consegue por detrás do computador, sabendo da dificuldade que as autoridades têm de identificar autoria, entrar numa conta e surrupiar esses valores. Então, facilita a prática de um crime e até cria uma nova tendência, sobretudo dos crimes patrimoniais. Não só dos crimes contra a honra, mas também de crimes patrimoniais.

ConJur — Quais são os crimes mais comuns com os quais o senhor tem se deparado?
Daniel Burg — As empresas têm sido constantemente vítimas justamente do crime de estelionato. Contas acessadas indevidamente para subtração de valores, mesmo em casos de aplicativos. Hoje, em não raras oportunidades, os taxistas criaram mecanismos, através desses aplicativos de deslocamento, para simular a existência de corridas que na verdade eles não fazem e, mesmo assim, obter os valores relacionados em detrimento de algumas dessas *startups*.

ConJur — Eles atuam em conjunto com um fraudador que consegue roubar os dados de cartão de crédito?
Daniel Burg — Exatamente — e não necessariamente envolve crime pela internet. Alguém frauda um cartão de crédito, não necessariamente pela internet. O sujeito pega um cartão de crédito clonado e, por coincidência ou não, tem um amigo taxista. Chama esse taxista através do aplicativo, por exemplo, combina, fala “Olha, eu vou chamar um táxi no endereço X. Esteja perto desse endereço, fique atento a esse chamado e o receba”. Aí o taxista recebe o chamado, só que o fraudador, aquele que possui o cartão de crédito fraudado, não entra no carro.

ConJur — Ele simula a corrida.
Daniel Burg — O taxista fica rodando por quantas horas quiser, em alguns casos até mesmo fica parado, ao final da suposta corrida efetua a cobrança. Pronto. O aplicativo paga em menos de 24 horas o valor da corrida para esse taxista e na enorme maioria das vezes muito antes até do próprio titular do cartão perceber que foi vítima. A operadora ressarce e suporta o prejuízo. Infelizmente, isso tem sido uma prática bastante comum.

ConJur — O prejuízo sobre para a operadora do cartão?
Daniel Burg — Não. Na cadeia, quem acaba suportando o prejuízo nesse exemplo é a *startup*, a empresa que dispõe do aplicativo. Infelizmente, isso tem sido comum e, se não fosse a modernidade dificilmente seriam descobertos. Nesse caso o traçado da corrida no GPS permitiu à empresa identificar a inconsistência da rota. Ninguém acorda num belo dia pensando "vou passear de táxis pelas estradas, gastar R$ 700 e não parar em nenhum lugar". Agora eles já estão sendo investigados pela prática não só do estelionato, mas também no crime de associação criminosa do Artigo 288 do Código Penal, uma vez

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

que há três ou quatro pessoas participando do crime juntos. Esse é um exemplo que reforça o que eu disse. A internet não aumenta os tipos penais, mas ela aumenta a forma como esses crimes podem ser praticados.

ConJur — Como funciona a investigação desses crimes virtuais?
Daniel Burg — Se atentar contra bens jurídicos da União a competência é da Polícia Federal. Nos demais casos, compete à Polícia Civil que, felizmente, cada vez mais conseguem compreender a lógica desses delitos. Mas é preciso ir além. Os agentes que atuam nas delegacias especializadas precisam estar ainda melhor preparados e também é preciso aumentar o contingente, para que essas delegacias consigam acompanhar o crescimento da prática desses crimes.

ConJur — O senhor enxerga um investimento nesse sentido?
Daniel Burg — Se tem, é imperceptível. Ainda há policiais que preferem não entender no que consiste a atividade dessas empresa, as investigando injustamente. Mesmo quando essas empresas são vítimas, alguns policiais não têm o menor estímulo em entender o modus operandi utilizado pelos fraudadores e não cooperam para a celeridade das investigações.

ConJur — O Judiciário está preparado para lidar com esses crimes?
Daniel Burg — Como são práticas recentes, a maior parte desses crimes ainda está em fase de investigação, tramitando entre polícia e Ministério Público. Mas tivemos uma experiência recente positiva com o Tribunal de Justiça de São Paulo, quando a corte determinou a suspensão de uma fiscalização da Receita Federal porque decorria de uma incompreensão das atividades da empresa investigada. No outro caso, coube ao Judiciário esclarecer aos investigadores a diferença entre instituição financeira e empresa intermediação de pagamento online. Com essa distinção ficou claro que não havia a prática do crime investigado. Então, a gente percebe que o Judiciário, pelo menos nas nossas recentes experiências, está de fato se atentando para essas questões e não estão propagando no tempo essas ilegalidades.

ConJur — E quanto à legislação?
Daniel Burg — Tenho severas críticas ao Legislativo, por exemplo no que diz respeito à forma ambígua ou que dá margem às mais variadas interpretações com que são criadas as leis. Além disso temos o caso recente da CPI dos Crimes Cibernéticos que, salvo algumas raríssimas exceções, foi mais uma oportunidade que o Legislativo perdeu de criar um diploma legal que de fato auxiliasse aos operadores do Direito na elucidação da prática de alguns crimes, tanto quanto na compreensão no que consistem esses crimes.

Conjur — No que a CPI dos Crimes Cibernéticos poderia ter sido melhor?
Daniel Burg — Sabendo-se da dificuldade que se tem na identificação, poderia, por exemplo, aumentar a pena para tais delitos. O Código Penal tem um dispositivo que aumenta a pena nos casos de crime contra a honra quando praticado por meios que facilitam a propagação da divulgação, mas ainda continuam sendo baixa as penas. Se de fato aquele que ofende se vale de uma conta de e-mail que não a pessoal dele, usa dados cadastrais falsos para criar essa conta e muitas das vezes também faz tudo isso através de uma *lan house*, perde-se muito tempo na identificação da autoria desses crimes. A incidência de crimes virtuais contra a honra e inquéritos que acabam sendo arquivados e considerável.

ConJur — E essas leis que foram recentemente criadas para essa área, como a lei Carolina Dieckmann, o Marco Civil da Internet, são eficazes para o que se propõem?
Daniel Burg —

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

A Lei Carolina Dieckmann não é. Apenas trouxe um novo dispositivo, inclusive redigido de forma bastante confusa, também com prazo prescricional de pena bastante baixa. Eu não ouvi falar de nenhuma denúncia recebida envolvendo esse tipo de crime. E o Marco Civil da Internet, por enquanto, para manter no exemplo que eu dei ao falar que o IP e outros dados que somente podem ser fornecidos com representação judicial, prejudica o ofendido. Como iniciativa, pelo menos dá para ver, existe alguma intenção do Legislativo em trazer ao mundo das leis alguns dispositivos para tratar do tema, mas como conteúdo ainda é muito pouco. Se o legislador pegasse uma coletânea de situações, decisões e artigos jurídicos do que vem acontecendo no dia a dia dos crimes virtuais com certeza veria que tem muita coisa para melhorar.

ConJur — Uma das dificuldades do crime virtual é a questão das fronteiras. Se uma pessoa na Estônia, por exemplo, rouba a senha de banco de um brasileiro. Como fica a investigação?
Daniel Burg — Depende do que ele vai fazer com a senha. O crime de estelionato, por exemplo, se consumaria quando o criminoso subtrai valores da conta aqui no Brasil. Como o crime se consumou no momento da subtração, a investigação seria de responsabilidade do Brasil.

ConJur — Só o fato dele roubar os dados já não é crime?
Daniel Burg — Vai depender das provas do caso, mas em regra não chega ser um crime se não gerar um efetivo prejuízo, seja patrimonial ou seja de conteúdo moral. Então o simples fato de pegar a senha por si só não configuraria o delito. Além disso, mantendo o exemplo citado, existe a dificuldade de o cidadão estar na Estônia. Você identificou quem fez o crime, mas como se dará a investigação? Vai expedir uma carta rogatória para lá, para o sujeito ser ouvido num inquérito policial? Também não é possível que se crie uma lei no Brasil obrigando o cidadão da Estônia a vir para cá. Esse é um caso clássico que, provavelmente, o crime investigado esbarraria na prescrição. A fronteira acaba motivando também, de certa forma, a impunidade.

ConJur — E quanto à investigação envolvendo empresas que não são sediadas no Brasil. Há a questão de empresas que dizem não cumprir determinadas ordens por não estarem sediadas no país.
Daniel Burg — Antes de mais nada, deixo claro que, para mim, são arbitrárias as decisões que suspendem o uso de determinado aplicativo porque não houve cooperação da empresa responsável. O que precisa ser feito é responsabilizar essas empresas e insistir no fornecimento. Caso ele continue a negar as informações solicitadas, instaura-se um inquérito policial por desobediência.

ConJur — Mesmo em casos de organização criminosa, como alguns juízes tem justificado, o boqueio desses aplicativos seria um exagero?
Daniel Burg — Sim, pois está ferindo toda a coletividade sendo que, em muitos casos, nem vai chegar no autor do crime através da informação que está sendo solicitada. É preciso sopesar os bens jurídicos que estão sendo tutelados. Às vezes o sujeito precisa do WhatsApp, por exemplo, para o trabalho e um juiz suspende o funcionamento do aplicativo. A decisão lesa o país inteiro para auxiliar na investigação de um crime. Esse é mais um exemplo de uma das milhares de arbitrariedades do Judiciário, que infelizmente vêm se tornando cotidianas.

ConJur — A publicação de notícias falsas na internet é crime? Quem responde por isso?
Daniel Burg — Em regra, é um crime contra a honra e responde por isso quem publica. Quem

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

compartilha essas notícias, mas não tem vínculo com a publicação, pode também ser condenado. Mas para isso é necessário que haja a comprovação de dolo de atingir a honra, objetiva ou subjetiva, daquele que está sendo vitimado. Mas é muito difícil comprovar esse dolo de quem apenas compartilha a falsa notícia.

Date Created
05/02/2017

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