jusbrasil.com.br
23 de Fevereiro de 2024

Crimes cibernéticos: O Papel indispensável do Advogado no combate aos crimes pela internet.

Publicado por Nicholas Merlone há 3 anos

Edson Schrot, Me. Advogado | Professor | Autor de diversos artigos. Email: edson.schrot@adv.oabsp.org.br

Nicholas Merlone, Me. Advogado | Professor | Autor de vários artigos & Escritor. E-mail: nicholas.merlone@gmail.com

Considerações Iniciais

Desde 2014, o avanço dos crimes cibernéticos está sendo monitorado pela Central Nacional de Denúncias de Crimes Cibernéticos, que se formou de uma parceria entre a ONG Safernet Brasil e o Ministério Público Federal (MPF). Em 2020, tirando proveito da crise do Covid-19, criminosos que agem através da internet, fortificaram seus delitos, registrando-se mais de 156 mil denúncias em 2020, cujo total é praticamente o dobro dos casos de 2019 (75.428 casos). No que se refere a estelionatos digitais, o aumento foi de 209%. Como veremos, a divulgação de informações para a sociedade, alinhada com ações estratégicas preventivas e repressivas e regulação são necessários para reduzir tais ocorrências. A prevenção é o remédio para não sermos vítimas, restando, após a ocorrência, procurar por direitos, tanto na esfera penal como na esfera cível.

Internet - Direito fundamental e riscos:

A economia mundial se encontra cada vez mais conectada, com expansão do capitalismo, sendo a internet um dos instrumentos essenciais para a integração completa de nossa sociedade. Trata-se de um direito fundamental o uso da internet, com fulcro em entendimento jurisprudencial da Constituição Federal e no artigo 19 da Declaração Universal dos Direitos Humanos da ONU.

Todavia, como se sabe, o ciberespaço e as suas relações sociais não são imunes à riscos, surgindo a necessidade de evolução da legislação penal, dos meios de investigação, dos instrumentos de cooperação, das ações preventivas e da forma de como atuar perante o Poder Judiciário para abarcar os crimes cibernéticos, que transpassam fronteiras e estão em expansão acelerada.

O uso contínuo e "inocente" da "web" por usuários, Pessoa Físicas e Jurídicas, geram oportunidades para criminosos praticarem crimes cibernéticos dos mais variados como criação de lojas virtuais falsificadas, extorsões via internet, fraude por e-mail e pela internet, fraude de identidades, com desvio e uso indevido de informações pessoais, desvio e venda de dados corporativos, extorsão cibernética, ataques de *ransomware*, *cryptojacking*, espionagem cibernética, crimes contra a honra e aplicativos maliciosos, *phishing*, *social killer*, *bullying* cibernético, *deep fake*, estelionato emocional, *stalking*, vingança pornô, dentre outros. Nessa esfera, os crimes cibernéticos afetam a economia global e patrimonial dos indivíduos, causando danos às atividades econômicas e financeiras de pessoas, empresas e governos.

Legislação sobre Crimes Cibernéticos e contínuo aprimoramento dos diplomas legais:

O Direito deve acompanhar as evoluções da sociedade, embora nem sempre seja tão fácil. Os computadores não distinguem "culpa" de "dolo". Uma pessoa ou várias pessoas, algumas vezes, transmitem mensagens eletrônicas com vírus sem saber. Ou ainda, o próprio computador pode ter sido utilizado maliciosamente como um artifício por criminosos virtuais que não são os proprietários em si do computador, causandor danos a terceiros.

No que tange a legislação penal, objeto deste artigo, observa-se três tipos de cibercrimes: a) crimes próprios, como de invasão de computadores, b) crimes impróprios que são os velhos crimes (de estelionato e outros) potencializados e facilitados por computadores e c) crimes de conteúdo indevido. A previsão legal no âmbito do direito penal iniciou-se em 2012, pela lei 12.737, com os crimes de acesso indevido (Art. 157-A: crimes de hacking), de interrupção de serviços telégrafos (se houver ainda), radiotelegráfico ou telefônico (art. 266), bem como de clonagem de cartão (Art. 298, CP). Em 2018, houve a previsão do revenge porn (pornografia de vigança) e em 2021, tornou-se penal o crime de stalking. As penas são muito dispares entre estes crimes, com críticas ao legislador por aplicação de punição branda a estes delitos, com exceção do *revenge porn* que nos parece adequado. A conduta de invasão de computadores por hackers é um exemplo, com pena apenas de 3 meses a 1 ano de detenção, nos termos do artigo 154-A do Código Penal, que pode ser conduzido nos Juizados Especiais Criminais, com todas as benesses da lei. Ao que tudo indica o legislador ainda não entendeu a potencialidade lesiva destes crimes, prevendo novamente pena branda, apesar de reclusão, em 2021 para o crime de stalking, no artigo 147-A do CP, com 6 meses a 2 anos, e multa.

A Lei Geral de Proteção de Dados, a LGPD – Lei Federal n. 13.709/2018, reforçou a questão da proteção dos dados pessoais, com fulcro no artigo 52 da lei, que prevê multas e outras

consequências para vazamento, furto ou extravio de dados. Além disso, temos o Marco Civil da Internet (Lei Federal n. 12.965/2014), a lei de software, Lei 9.609/98

A Lei Federal 12.735/2012 determinou aos órgãos da polícia judiciária ordem para se estruturarem, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Outrossim, há previsão no ECA, na Lei 9.504/97 (crimes eleitorais), Lei

7.716/89 (de racismo) e Lei 13.260/16 (lei antiterrorismo). A Polícia Federal tem atribuição para tratar de infrações que difundam conteúdo misógino, incluída pela Lei 13.642/2018.

Como vetores para a legislação nacional, destaca-se a Convenção de Budapeste (2001), relativa a crimes cibernéticos, que finalmente o Brasil aderiu em 2020. Isso mesmo, no ano passado – 19 anos depois!. O protocolo de Estrasburgo, de 2003, com intenção de regulamentar o *cloud computer*. Há também a Convenção de Palermo, contra crimes transnacionais, inclusive, como reflexos os crimes virtuais. Prima-se pela cooperação internacional na resolução de crimes eletrônicos, cometidos em escala global, cruzando fronteiras pelo mundo.

Notas sobre o Crime Cibernético, Anonimato nas Redes e Prevenção do crime:

O crime digital, em muitos casos, é meio para crimes gravíssimos como de estelionato, extorsão, falsidade ideológica, fraude, entre outros.

O meio de concretização é virtual, embora o crime nem sempre seja. A maior parte dos crimes na internet também ocorre no mundo real. A rede mundial somente facilita o delito, através do

anonimato, o que, ressalte-se, na verdade, nem sempre prevalece. Há de fato fiscalização de segurança no ambiente virtual, uma vez que, por exemplo, se tem o número IP do usuário (identificação virtual), o que torna o anonimato relativo na internet. Não se pode confundir liberdade de expressão na rede com anonimato, pois, já que ofensas cometidas podem ser identificadas e punidas.

Em outros países, há uma cultura de programas de recompensa para que profissionais de TI descubram falhas em sistemas eletrônicos. Uma área ofensiva para explorar vulnerabilidades nas plataformas digitais. Sem dúvidas, isso deveria ser mais incentivado em nosso país. Outros países têm uma preocupação maior com isso. O Brasil e as empresas brasileiras deveriam adotar tais práticas preventivas.

Ao tratarmos de segurança, devemos considerar não só fatores externos, mas também internos. Isto para que os fatores externos não violem a segurança. Sem segurança da informação, pode-se ter prejuízos milionários e irreversíveis.

Para assegurar a segurança, é preciso conhecer todas as nuances de um sistema de informação. Ou seja, não só o software, mas todos os aspectos na organização dos dados, que produzem um banco de dados. Assim, os sistemas de informação podem ser vistos como armas a serem usadas a favor e contra a organização que os dispõe, já que o histórico e as informações da organização se encontram neles.

Para buscar a segurança na internet, devem-se usar senhas seguras, recorrer ao uso de criptografia, fazer *backup*, usar *firewall*, bem como atentar para o sigilo de documentos, de modo que procure se preservar a integridade, a restrição, o registro, a confidencialidade e a disponibilidade.

É preciso, portanto, controle, monitoramento e

atualização. Os dados podem ser muito valiosos, daí a relevância da segurança, diante dos infratores, que busquem alguma vantagem. Deve-se atentar para as vulnerabilidades do sistema, pois sistemas seguros afastam a incidência dos criminosos. Não é possível um sistema totalmente seguro. Porém, deve-se buscar perseguir esse horizonte.

Finalmente, para preservar a segurança nesses sistemas, é preciso investir em ferramentas, análise e controle de segurança, além do investimento em pessoas, que usarão o sistema. É preciso, pois, uma equipe de defesa bem treinada. Por fim, com as ameaças que se descortinam, a segurança da informação se torna uma necessidade diária das organizações, que deve ser levada muito a sério.

Provas Virtuais

É preciso atentar quanto à territorialidade e à investigação das provas. As provas digitais são fundamentais para o bom andamento do processo. E-mails, postagens em redes sociais, blogs e sites são apenas alguns itens que podem ser utilizados como prova pelo advogado que atua na área.

Um advogado experiente em crimes cibernéticos levantará evidências do crime, catalogando-as e confeccionando relatórios que suportarão ações judiciais no futuro. Na maioria dos casos é necessário efetuar ata notarial para resguardar direitos e também fazer denúncias de crimes em canais apropriados.

Com diligência, o advogado buscará atuar em diversas esferas para reduzir prejuízos do cliente, inclusive avaliando possíveis falhas em face da LGPD – Lei Geral de Proteção de Dados, que-

rendo identificar possíveis responsáveis pelo vazamento de dados.

O que fazer se for vítima de crime eletrônico e o Papel do Advogado no combate aos crimes eletrônicos

Assim,

caso seja vítima de crimes cibernéticos, o primeiro passo é procurar um advogado especialista. O advogado especialista em crimes cibernéticos, com compreensão de técnicas digitais e como ocorrem os ataques virtuais estará preparado para fornecer diagnósticos, elaborar estratégias e planos de ação deste fenômeno criminal, sempre atualizado em conformidade com os precedentes dos Tribunais, definindo quais medidas judiciais adequadas deverão ser propostas, como ingressar com ações de reparação de danos morais, ações judiciais para remover conteúdos indevidos da internet, contra empresas e responsáveis que desrespeitam normas de segurança, a Lei Geral de Proteção de Dados e contra eventuais sistemas de segurança que falharam. O advogado deve orientar seu cliente, atuar em parceria com as autoridades que investigam cibercrimes, participando ativamente de diligências, com o fim de recolher todas as provas necessárias e utilizá-las adequadamente.

Não há dúvidas, o advogado assume papel central no enfrentamento de crimes eletrônicos. O advogado, assim, deve orientar adequadamente seu cliente no que se refere aos procedimentos e à proteção de seus direitos, inclusive, com caráter preventivo para que não caia em armadilhas. Nesse sentido, é preciso auto preservar-se e, para isso, é preciso informação e conhecimento. E, por fim, e não menos relevante, é importantíssimo a sensibilidade do advogado, de se colocar no lugar do cliente, e sigilosamente, apoiar a vítima abalada pelas ações de criminosos que, em muitos casos, detém diversas informações privadas do cli-

ente e comprometedoras, capazes de causar sérios danos à imagem, família e a seus ativos financeiros, atuando racionalmente em seu benefício, buscando a melhor solução, para seu problema.

Referências

LOBO, Edson J. R. **Segurança da Informação: Ameaças e Controles**. Rio de Janeiro: Editora Ciência Moderna Ltda., 2019.

PINHEIRO, Patrícia Peck. **Direito Digital**. 6ª. edição. São Paulo: Saraiva, 2016.

PLANTULLO, Vicente Lentini. **Estelionato Eletrônico: Segurança na Internet**. Curitiba: Juruá, 2003.

Notícias CNJ. Crimes digitais: o que são, como denunciar e quais leis tipificam como crime? 22 jun / 2018. Disponível em: <https://www.cnj.jus.br/crimes-digitaisoque-são-como-denunciare-quais-leis-tipificam-como-crime/>. Acesso em: 12 maio / 2021.

Disponível em: https://www.jusbrasil.com.br/artigos/crimes-ciberneticos-o-papel-indispensavel-do-advogado-no-combate-aos-crimes-pela-internet/1222913995

Informações relacionadas

José Milagre
Artigos • há 4 anos

Como é a atuação do advogado especialista em crimes cibernéticos?

O exercício da Advocacia especializada em crimes virtuais vem chamando a atenção de inúmeros profissionais e alguns fatores são considerados chave,

como o crescimento das fraudes, golpes e ofensas...

Paulo Roberto Moreira
Artigos • há 2 anos

O que são Crimes Cibernéticos?

Os crimes cibernéticos no Brasil cresceram em tempos de pandemia. Em 2020, o registro de denúncias anônimas contabilizou 156.692 casos, segundo os dados da Central Nacional de Denúncias de Crimes...

Rebeka Assis
Artigos • há 4 anos

Crimes Virtuais: descubra quais são os 7 mais cometidos!

Com o ano de 2020 batendo à porta, muitas pessoas ainda acreditam que a internet é “terra de ninguém” e que a sua opinião ou conduta pessoal prevalece quando comparada aos direitos coletivos. A...

Para profissionais

Jurisprudência

Doutrina

Diários Oficiais

Peças Processuais

Modelos

Legislação

Seja assinante

API Jusbrasil

Transparência

Termos de Uso

Política de Privacidade

Proteção de Dados