

## O combate à criminalidade cibernética no Brasil Parâmetros Objetivos de Tipicidade

**Juiz Robson Barbosa de Azevedo**

Ementa: 1- Breve intróito; 2- Conceito de crime cibernético; 3- A pedofilia; 4- A ameaça; 5- O furto (desvio de dinheiro); 6- A honra (calúnia); 7- A discriminação religiosa, de raça e de etnia; 8- Estelionato; 9- A fraude contra os cartões de crédito e a captura de senhas por monitoramento e interceptação; 10- Pirataria e propriedade industrial; 11- Conclusão; 12- Fontes.

### **1 – Breve intróito:**

A modernidade e as facilidades de comunicação permitiram uma grande difusão de idéias entre a população mundial e, por óbvio, ao povo brasileiro.

Atualmente, temos na internet uma enorme utilização para a obtenção de serviços, conhecimentos e produtos, facilitando a relação de consumo e multiplicando as operações bancárias, ou seja, a circulação livre de dinheiro e a informação por um mecanismo virtual e rápido o suficiente para a prática de lesões capazes de subsunção nos crimes já estabelecidos no Código Penal e Leis Especiais.

É com esse viés que se busca em tão breve artigo acadêmico prestar uma colaboração para o combate aos crimes cometidos pela internet nos moldes das leis já existentes no Brasil.

A questão impõe, quando diante de um caso concreto de crime cibernético, que a autoridade investigadora, mediante mandado judicial, e uma vez excluídas as hipóteses de endereço IP falso ou trocado por hackers e crackers, além de spam, que proceda a identificação do endereço IP corretamente e absolutamente verdadeira, tudo para que passe a ser a sua fonte formal de respectiva localização, de forma que obtenha a necessária materialidade e autoria, fazendo cessar imediatamente a lesão imposta pelo criminoso à vítima.

O agente ativo de crime cibernético pode ser pessoal física e ou jurídica, caso em que a primeira pode ser presa e condenada a desfazer o mal perpetrado, sem prejuízo dos danos de ordem moral e à imagem, o mesmo acontece com a pessoa jurídica que por ser imaterial não será presa, mas seus responsáveis e prepostos são co-autores dos delitos cibernéticos.

### **2 – Conceito de crime cibernético:**

Com o aumento já esperado de uso contínuo e proveitoso da internet, nos deparamos com condutas virtuais nocivas e com uma capacidade de atingir o cidadão brasileiro de forma muito gravosa e também a sociedade brasileira em geral.

Uma repugnante conduta típica se fez presente e acessível pelo simples uso do computador, como no caso da pedofilia, expondo fotos de crianças nuas e mediante exploração econômica.

Por certo, que a conduta de pedofilia somou-se a impunidade e a outros crimes já tipificados em nossa legislação, caso em que o povo brasileiro amargou pelo ambiente

virtual da internet a captura de senha bancária e desvio de dinheiro, bem como a feitura de negócios desastrosos, nos quais, mesmo pagando, nunca recebeu o produto prometido.

Foram e são tantas as fraudes que a criminalidade cibernética não mais poderia viver sob o manto da virtualidade como esconderijo para não ser criminalmente punida.

O conceito de crime cibernético no Brasil é exatamente o fato consistente na prática de crime contra uma pessoa ou sociedade, mediante o uso da internet, passível de enquadramento nas leis penais brasileiras, para fins de punição efetiva, ou seja, aquele que sai do virtual e entra na realidade de todos.

### **3- A pedofilia:**

O crime de pedofilia encontra punição expressa no art. 241 do Estatuto da Criança e do Adolescente *in verbis*: “*Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.*”

Assim sendo, quando se encontra na internet fotos de crianças nuas e tais fotos são remetidas pela rede de computadores, além de permutadas entre pessoas, os remetentes e o divulgador da foto já pode receber uma reprimenda e ser preso, podendo ser condenado em até 8 anos de prisão.

### **4- A ameaça:**

O Código Penal Brasileiro estabelece em seu art. 147 o seguinte: “*Ameaça Art. 147 – Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave: Pena – detenção, de um a seis meses, ou multa. Parágrafo único – Somente se procede mediante representação.*”

Diante desse fato criminoso, por vezes encontrado na internet, a vítima deve representar, levando a impressão da ameaça como foi posta na tela do computador, indicando o autor do comunicado virtual ou fornecendo ao investigador o que dispõe para a identificação do criminoso.

De fato, no Brasil, a internet não se presta às ameaças criminosas contra cidadãos, mesmo porque a esfera penal estabelece punição de detenção, podendo ser lavrado um termo circunstanciado, caso não haja reincidência, para aplicação de transação penal e ou pena alternativa.

### **5- Furto qualificado (desvio de dinheiro):**

O furto é uma conduta típica muito conhecida pelo povo brasileiro, pois atualmente o número de vítimas de furto no Brasil é considerável. O furto está devidamente tipificado

no Código Penal Brasileiro, senão vejamos: **“Furto Art. 155 – Subtrair, para si ou para outrem, coisa alheia móvel: Pena – reclusão, de um a quatro anos, e multa. § 1º – A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno. § 2º – Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa. § 3º – Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico. Furto qualificado § 4º – A pena é de reclusão de dois a oito anos, e multa, se o crime é cometido: I – com destruição ou rompimento de obstáculo à subtração da coisa; II – com abuso de confiança, ou mediante fraude, escalada ou destreza; III – com emprego de chave falsa; IV – mediante concurso de duas ou mais pessoas. § 5º – A pena é de reclusão de 3 (três) a 8 (oito) anos, se a subtração for de veículo automotor que venha a ser transportado para outro Estado ou para o exterior.”**

No caso de furto de senhas e desvio de dinheiro decorrentes do furto a pena pode chegar aos 8 anos de reclusão e multa, pois trata-se de furto qualificado pela fraude ou abuso de confiança.

O cidadão encontra repressão penal em conduta típica expressa e previamente estabelecida na lei penal em vigor, pois a burla ocorre exatamente por força de fraude que retira do cidadão mediano a capacidade de manter a guarda necessária e contínua sobre o acesso à rede de computadores e sem o seu consentimento.

## **6- A honra (Calúnia):**

A mácula à honra da pessoa é um mal que pode gerar até sequelas psicológicas num território livre como a internet.

O território é mesmo livre, mas as pessoas que focam seus meios de vida e mesmo suas vinditas irresponsavelmente contra suas vítimas, não estão livres do cometimento dos crimes contra a honra e suas respectivas punições.

A calúnia faz uma imputação falsa sobre ofendido ao afirmar que ele cometeu um crime. A difamação busca macular a reputação da vítima, manchando-a de forma ofensiva e a injúria retira da vítima, mediante ofensa, sempre injusta, a dignidade ou o decoro. São crimes que se percebem facilmente quando um instrumento de comunicação pública ultrapassa a mera função informativa e passa a destacar o juízo de valor sobre uma pessoa e dando ênfase aos aspectos contrários aos fatos com potencialização da dor sofrida pela vítima, sem estabelecer contraditório e sem buscar a verdade, mantendo-se apenas no fato em si, mesmo que o fato seja uma unilateralidade institucional, pessoal e venal, ou seja, visa sempre lucro com a venda e propaganda posta no periódico, tudo em cima da honra da vítima como atrativo ao ato de aquisição da informação, perpetuando a desgraça alheia.

Não só a pessoa natural que de forma engenhosa busca redigir o texto ofensivo para macular a honra da vítima, mas também a pessoa jurídica responsável pela divulgação, recaindo sobre os seus editores, prepostos e proprietários que são também agentes passivos da conduta típica que estabelece o crime contra a honra.

A modalidade da injúria é a que mais se revela dentre os crimes contra a honra, pelo fato de retirar facilmente a dignidade do ser humano vitimado, atingindo seus filhos na

escola, sua esposa no trabalho, seus familiares em grande repercussão e irreversível dificuldade de convivência social, praticamente retirando a pessoa da *polis*.

O Código Penal Brasileiro estabelece retratação, mas o estrago costuma voar como penas de pássaros e com o vento por todo o planeta terra, sendo impossível recolher cada desdobramento da ofensa original.

Por esta razão, a lei penal prevê o crime e a punibilidade, sem prejuízo da indenização cabível. Só há de fato democracia, quando o cidadão comum tem elementos suficientes para opor-se individualmente ao poder econômico dominante nas grandes empresas e conglomerados. Os arts.138 a143 do Código Penal Brasileiro são eficazes para a obtenção de punibilidade e até possível retratação.

A internet no Brasil se tornou um campo fértil para ofensas morais postas irresponsavelmente por pessoas ou empresas que buscam praticar o crime, demonizando um cidadão e enaltecendo outro, de acordo com o interesse político vigente, sempre bem remunerada e com ouvintes para gargalhar em um espetáculo de horrores. Informar não é caluniar, difamar e ou injuriar. E a sombra da internet não se presta à impunidade penal e nem prejudica a obtenção de indenização.

A censura não existe quando se respeita a lei e se afasta do cometimento de crimes. No Brasil pode-se falar tudo desde que assumam-se a responsabilidade pelo que se falou. Não há que se falar em irresponsabilidade nas manifestações públicas e ou particulares em ambiente público.

## **7- A discriminação religiosa, de raça e de etnia:**

Os crimes eletrônicos ou digitais se desenvolveram ainda mais, ou seja, não pararam na pedofilia, na ameaça, no furto (desvio de dinheiro) e na honra (calúnia). A utilização da internet foi mais além e nem mesmo poupou os antigos conflitos religiosos, as fomentações de ódios quanto à raça e etnia.

A lei 7716/89 é a que define os crimes resultantes de preconceito de raça ou de cor e afirma o seguinte: “Art. 20. *Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. (Redação dada pela Lei nº 9.459, de 15/05/97) Pena: reclusão de um a três anos e multa. § 1º Fabricar, comercializar, distribuir ou veicular símbolos, emblemas, ornamentos, distintivos ou propaganda que utilizem a cruz suástica ou gamada, para fins de divulgação do nazismo. (Redação dada pela Lei nº 9.459, de 15/05/97) Pena: reclusão de dois a cinco anos e multa”*, restando claro que a discriminação pode ocorrer em quaisquer ambiente, não escapando o ambiente virtual da internet.

A norma jurídica penal especial estabelece pena de até 5 anos de reclusão e multa para quem discriminar pela internet, quer seja em *emails* ou *chats*, quer seja com a divulgação de matérias discriminatórias ou mesmo em comentários desairosos os ranços pejorativos de cor, raça, religião e etnia para atingir o cidadão brasileiro.

As legislações específicas somam-se ao Código Penal Brasileiro, formando o arcabouço válido e aplicável nos crimes cibernéticos, reprimindo os atos criminosos e retirando do

convívio social os que insistirem na prática de crimes pela internet.

## 8- O estelionato:

A internet no Brasil tem sido campo fértil para a prática de estelionato contra o cidadão de boa-fé que acredita na segurança dos mecanismos de consumo ofertados pela internet.

O estelionato encontra conduta típica, prévia e expressa no art. 171 do Código Penal, senão vejamos: **“Estelionato Art. 171 – Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de um a cinco anos, e multa. § 1º – Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2º. § 2º – Nas mesmas penas incorre quem: Disposição de coisa alheia como própria I – vende, permuta, dá em pagamento, em locação ou em garantia coisa alheia como própria; Alienação ou oneração fraudulenta de coisa própria II – vende, permuta, dá em pagamento ou em garantia coisa própria inalienável, gravada de ônus ou litigiosa, ou imóvel que prometeu vender a terceiro, mediante pagamento em prestações, silenciando sobre qualquer dessas circunstâncias; Defraudação de penhor III – defrauda, mediante alienação não consentida pelo credor ou por outro modo, a garantia pignoratícia, quando tem a posse do objeto empenhado; Fraude na entrega de coisa IV – defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém; Fraude para recebimento de indenização ou valor de seguro V – destrói, total ou parcialmente, ou oculta coisa própria, ou lesa o próprio corpo ou a saúde, ou agrava as conseqüências da lesão ou doença, com o intuito de haver indenização ou valor de seguro; Fraude no pagamento por meio de cheque VI – emite cheque, sem suficiente provisão de fundos em poder do sacado, ou lhe frustra o pagamento. § 3º – A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.”** O básico do estelionato é o ardil utilizado pelo criminoso para enganar o cidadão que é vitimado em seu consentimento e entrega voluntariamente a informação ou meio adequado à prática da fraude contra sua própria pessoa, se não fosse o artifício ardiloso posto na internet o cidadão vítima não cairia na fraude.

O Código Penal Brasileiro é o diploma legal que estabelece pena de até 05 anos e multa para o criminoso cibernético que passou a praticar estelionato no chamado “território virtual”.

Como poder-se-ia dizer que faltam normas, se até aqui estamos preste a punir mais de 90% (noventa por cento) dos crimes cibernéticos cometidos no Brasil ou com resultados no Brasil.

## 9- A fraude contra os cartões de crédito e a captura de senhas por monitoramento e interceptação:

Se não bastasse, o estelionato pela internet, temos uma conduta típica muito comum no ambiente virtual que alcança o cartão de crédito do cidadão brasileiro em sua boa-fé e descuido, mesmo que leve, no uso dentro do ambiente cibernético.

Os criminosos são regra geral, muito conhecedores das brechas do mundo virtual e das montagens fantasiosas que podem fazer. Não raro, divulgam suas armadilhas em sítios de busca na internet com forte credibilidade nacional e internacional, dando uma aparência de legalidade e segurança, que nunca existiram.

Em 1996, foi posta em vigor a lei que regulamentou o art. 5º ,XII , da nossa Constituição Federal que afirma o seguinte: *“é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;”* A Lei nº 9296/96 proporcionou um grande passo para garantir a cidadania brasileira o sigilo de suas comunicações e criou pena de até 4 anos de reclusão e multa, como podemos observar de seu próprio texto: *“Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa.”*

Senão bastasse, o aparato constitucional para livrar o cidadão brasileiro de atos criminosos contra a sua privacidade, conseguiu-se com a lei a consagração constitucional de proteção inequívoca contra os males das interceptações de informática e de telemática que tanto propiciam a fraude em cartões de créditos pela internet.

Como já mencionei no item 1 do presente artigo acadêmico, tudo deve ser apurado pelo investigador, *‘mediante mandado judicial, e uma vez excluídas as hipóteses de endereço IP falso ou trocado por hackers e crackers, além de spam, que proceda a identificação do endereço IP correta e absolutamente verdadeira, tudo para que passe a ser a sua fonte formal de respectiva localização, de forma que obtenha a necessária materialidade e autoria, fazendo cessar imediatamente a lesão imposta pelo criminoso à vítima.’* É claro que sem a Constituição Federal, Código Penal Brasileiro e Leis Especiais nada poderia ser feito civilizadamente e com punição efetiva estatal.

Aqui se entra no território mais escuro da atividade virtual na internet, pois para fraudar o cartão de crédito, o criminoso busca na interceptação de informática ou de telemática a captura de senha. O monitoramento ilegal limita-se ao que não foi avisado ao usuário e ao que não foi autorizado pelo usuário, sempre de forma expressa e inequívoca.

As empresas e órgãos que monitoram seus servidores para não incidirem na conduta típica comunicarão a todos os usuários o monitoramento, evitando-se assim que senhas e dados pessoais se espalhem indevidamente pela rede mundial de computadores.

As compras pela internet sem oferta de boleto ou que demandem pagamento no ato, mesmo que parcial, não devem merecer crédito para que seus dados do cartão de crédito sejam passados. Acautele-se.

Não obstante o aspecto da captura de senha por hackers e crackers, a prevenção e atenção do cidadão faz a diferença para evitar a captura e interceptação de seu computador por criminosos. E a proteção pelo antivírus serve como grades que guardam as janelas da casa.

## **10- Pirataria e propriedade industrial:**

Nesta fase do artigo proposto, podemos analisar a Lei nº 9609/98 que estabelece prisão para a pirataria praticada contra a propriedade intelectual do programa de computador e sua comercialização indevida. O alcance ora revelado pela lei é no sentido de evitar que a pirataria dos programas de computador, possam facilitar o monitoramento e a interceptação dos computadores, em face do fato que atinjam os usuários pela ineficácia plena dos programas que integram a máquina e sua formatação, bem como a sua vulnerabilidade aos mais diversos vírus que circulam na rede mundial de computadores.

No momento, o mais adequado é observar a legitimidade dos programas de computador para prevenir o fato e não amargar ser vítima de vírus que capturem sua máquina. Observe a lei: *Art. 12. Violar direitos de autor de programa de computador: Pena – Detenção de seis meses a dois anos ou multa. § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente: Pena – Reclusão de um a quatro anos e multa; § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.* A norma jurídica em vigor estabelece até 4 anos de reclusão e multa para os atos de pirataria e nos remete aos programas originais como seguros.

Tanto as pessoas jurídicas como as físicas devem buscar em seus programas a fidelidade capaz de garantir a originalidade, repudiando as brechas por onde vírus se instalam e só usarem seus equipamentos com segurança máxima na navegação junto à rede mundial de computadores.

Este aspecto que ora se busca alertar está nos poucos casos em que as leis atuais, pouco ou nada podem fazer criminalmente, em face dos vírus eletrônicos e suas diversas formas de contaminação não saírem do mundo virtual e partir de uma origem escusa e de quase nenhuma identificação, por vezes, internacional.

Faltam em nosso ordenamento uma defesa objetiva de *lege ferenda* que nos permita ir além da proteção criminal da marca e patente de uma empresa que por semelhança forjada na internet desvie o usuário para mais uma armadilha, caso em a legislação especial estabelece pena de detenção para os crimes contra a patente dos produtos.

## **11- Conclusão:**

O presente e breve trabalho não passou de uma mera colaboração voltada para a identificação e punição da prática de crimes cibernéticos e não esgota nem de perto a amplitude do tema que se enfrenta.

Ao menos, aponta que nem tudo que ocorre na internet é imune à aplicação das penas no Brasil e que seu efeito no Brasil deve e pode aqui ser punido.

A punição tem se efetivado em reclusão, detenção e ou multa, tudo sem prejuízo da busca indenizatória estabelecida legalmente na via cível.

O problema da criminalidade na internet não é só do Poder Público e das leis já existentes, mas também de toda sociedade brasileira, mesmo diante das penas criminais existentes nas normas em vigor, pois o cuidado e a observância de uso dos programas originais e a prevenção contra vírus cada vez mais presentes na internet, nos reúne em um grupo social do qual o Poder Público deve necessariamente apresentar os meios cabíveis de enfrentamento da questão.

12- Fontes do Trabalho:

Constituição Federativa do Brasil de 1988 e respectivas emendas.  
Código Penal Brasileiro de 1940 e respectivas emendas.  
Legislação Especial  
Estatuto da Criança e do Adolescente

Autor: Robson Barbosa de Azevedo é Juiz de Direito do TJDF, professor universitário e mestre em Direito Público pela Universidade Federal de Pernambuco (UFPE).