SEARA JURÍDICA — ISSN 1984-9311 — V.1 | N. 11 | JAN - JUN 2014

Crimes cibernéticos: algo de novo no Direito Penal?

Misael Neto Bispo da França[1*]

Partindo-se de uma abordagem constitucional, tem-se que o Direito Penal serve para tutelar os bens jurídicos essenciais, em face de lesões ou ameaças de lesões sérias provocadas por terceiros. Trata-se do que se entende por intervenção mínima daquele que deveria ser tratado pelo Estado como a *ultima ratio* de controle social. Em linhas outras, fala-se aí no binômio fragmentariedade-subsidiariedade do sistema punitivo, que convergem para a noção de proporcionalidade-necessidade.

Sob esta óptica, é de se reconhecer que o Direito Penal precisa evoluir junto com a sociedade, sob pena de, atrasado, não corresponder mais aos anseios da sociedade, na medida em que fecha os olhos para novos bens jurídicos e novas formas delitivas.

Eis, então, que se fala em crimes cibernéticos, rótulo sob o qual se estudam condutas lesivas ao próprio meio cibernético e outras que se valem deste meio para atingir bens jurídicos já tutelados pelo Direito Penal de outrora.

No primeiro caso, tem-se os crimes cibernéticos próprios; no segundo, os impróprios.

Ora, se o Direito Penal, ramo do ordenamento jurídico que é, deve aliar-se às transformações sociais, força é convir que as condutas citadas não podem passar ao largo da tutela punitiva.

O fenômeno corresponde ao que se denominou de expansão do Direito Penal, um movimento cujas origens situam-se no final do séc. XIX, com o processo de globalização, que implicou o incremento de riscos preexistentes e o surgimento de outros nunca dantes vivenciados. Dir-se-ia que este processo desembocou em uma sociedade do risco, que, por seu turno, passou a exigir do Estado o recrudescimento da sua resposta penal, a identifica-la como a *prima ratio* do controle estatal.

1 *Mestre em Direito. Professor de Direito Penal do Centro Universitário Jorge Amado.

Em que pese o tratamento deste setor – criminalidade cibernética – como algo novo, ideia que se alimenta do argumento de que não há legislação pátria específica para o tema, constata-se que o assunto não se reveste de qualquer novidade; ao menos se considerado como novo aquilo que não transcende uma década, apenas para fixar o referencial para o curso do presente trabalho.

Ora bem. Os crimes que se convencionou denominar de cibernéticos, com grande frequência, estão relacionados a ofensas contra a honra de alguém. Neste nexo, são cometidas calúnias, difamações e injúrias, através, por exemplo, das redes sociais. São condutas que, conforme o próprio nome indica, já estão tipificadas no Código Penal brasileiro, a partir do seu artigo 138.

Cumpre aduzir que tais condutas, com o passar do tempo, vêm perdendo sua dignidade penal. É que, em suas formas simples, submetem-se ao rito das infrações penais de menor potencial ofensivo, que traz uma multiplicidade de medidas despenalizadoras, descambando para o tratamento de cunho civil.

Aliás, a resposta civil a condutas desta natureza parece mais célere e eficiente, se comparada à morosidade do processo penal. Sob outro pálio, corrobora-se a ideia de perda de dignidade penal o anseio de muitos com a concretização da justiça restaurativa, por conduto das técnicas de mediação, que encontrariam solo fértil no âmbito as infrações de menor potencial ofensivo.

Em suma, o crime contra a honra que acontece pela internet pode muito bem submeter-se aos institutos da legislação penal existente – Códigos Penal e de Processo Penal, Lei no. 9.099-95, etc. – já que as categorias dogmáticas são as mesmas, alterando-se, talvez, a forma de cometimento.

Não se pode exigir do legislador o dom da vidência e da profecia. Ele opera para o futuro, a fim de que o produto de sua ação – a lei – gere efeitos para o porvir, o que não significa, em absoluto, ofensa à legalidade-taxatividade.

Assim, as redes sociais constituem mais um panorama para a prática de crimes que ocorriam em outros moldes.

Ao argumento de que os crimes propriamente cibernéticos, cujo bem jurídico sob tutela seria o próprio sistema virtual e seus dados, configuram ineditismo que clama por uma legislação específica, também são lançadas críticas.

Quando da publicação da lei no. 12.737-2012, entendeu-se que suas disposições inovaram o ordenamento jurídico pátrio, sobretudo diante do

acréscimo do artigo 154-A no Estatuto Repressivo. Este artigo pune, com três meses a um ano de detenção e multa, e a conduta de "Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismos de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita".

Ora, de novo, mesmo, só o efetivo acréscimo de mais um dispositivo ao Diploma em tela, posto que o *meio cibernético*, como bem jurídico-penal, já era tutelado em outros momentos do Direito.

Em 2000, a lei no. 9.983 acrescentou os artigos 313-A e 313-B ao Código Penal, como espécies de peculato. Em ambas as hipóteses, o bem material engloba o *sistema informatizado,* em clara demonstração de que o tema não é, nem de longe, novo.

Muito antes da sobredita alteração nos crimes contra a Administração Pública, a lei no. 9.296-1996, já dispunha sobre a interceptação de dados e comunicações telefônicas e *sistemas de informática e telemática,* para fins processuais penais.

Neste passo, cumpre abordar alguns problemas causados pelo legislador de 2012, no que tange à higidez de princípios de Direito Penal. Trata-se de equívocos que surgem no afã de se coibir as novas formas delitivas, com o estímulo de setores da imprensa.

Em primeiro lugar, o já citado artigo 154-A vai de encontro à ideia de lesividade, afinal, que lesão séria existe na conduta de invadir dispositivo informático alheio com o mero fim de obter informações?

Não nos parece que tal conduta ostente relevância para a seara da pena! Que outros ramos do Direito, mais adequados e mais céleres, sirvam de guarida ao ofendido em casos quejandos.

Por outro ângulo, o mesmo dispositivo contraria o princípio da adequação social. A ação de *haker's* vem sendo estimulada por grandes empresas que os contratam para que apontem as vulnerabilidades dos seus sistemas, com o propósito final de corrigir eventuais falhas.

A própria segurança jurídica resta abalada com a referida estratégia legislativa, com interferências no campo da proporcionalidade. É que o artigo 10, da lei no. 9.296-1996, já tipificava a mesma conduta, praticamente,

cominando, todavia, a pena de dois a quatro anos de reclusão, além da multa.

O silêncio do legislador de 2012 sobre a lei de 1996 enseja o seguinte raciocínio: houve revogação tácita do aludido artigo 10 e, consequentemente, advento de *lex mitior*, dada a reprimenda mais branda, que, portanto, deve retroagir para beneficiar quem respondia pela conduta tipificada na lei no. 9.296.

Vê-se, pois, que o tema "crimes cibernéticos" não é novo; para além disto, constata-se que a política criminal que tende a salvaguardar o ambiente virtual incorre em alguns equívocos, gerando a incerteza da própria necessidade de tutelá-lo através do Direito Penal.

O que desponta como certo, no entanto, é que a vítima das condutas referenciadas têm papel relevante na sua prevenção. Diga-se isto, mais especificamente, a respeito dos crimes contra a honra praticados por meio da internet, carro-chefe dos crimes virtuais. A banalização da vida privada, com a exposição frequente de imagens e com a divulgação detalhada de rotinas contribui, efetivamente, para a atuação criminosa sobre estes dados.

No ambiente cibernético, muito por força da impessoalidade que o caracteriza, não se sabe, ao certo, quem *curte alguém* ou quem *curte com alguém*.

SEARA JURÍDICA — ISSN 1984-9311 — V.1 | N. 11 | JAN - JUN 2014