TUTELA CONCRETA DAS INFORMAÇÕES VIRTUAIS

Ivan Luís Marques

O substitutivo do relator **Regis de Oliveira**, da Comissão de Constituição, Justiça e Cidadania (CCJC) da Câmara, apresentado em 05.10.2010, alterou o PL 84/99 e agora aguarda aprovação parlamentar final, sanção e publicação para integrar nosso ordenamento jurídico.

Anseio de muitos, desde especialistas da área até vítimas de violação de dados armazenados em meios eletrônicos ou sistemas de informação, a segurança das informações presentes nos meios digitais carece de tutela específica.

A questão relevante oriunda desse cenário relaciona-se a qual tipo de tutela será necessária para, efetivamente, conseguirmos minimizar os riscos pessoais e patrimoniais presentes no plano cibernético.

Nossa contribuição ficará restrita aos critérios deônticos de *seleção* de condutas que atingem nossos bens da vida mais preciosos, à *eficácia* da tutela e, por fim, à *necessidade* da utilização do Direito Penal para buscar resultados concretos. A análise ficará restrita ao plano geral e às primeiras impressões, respeitando os limites sumaríssimos do presente trabalho.

1. Seleção de condutas típicas

Para selecionar condutas consideradas delituosas, importante buscar o máximo de informações concretas no âmbito social. Estatísticas policiais, procedimentos administrativos, problemas pessoais, estudos acadêmicos, informações da imprensa, audiências públicas, trabalhos publicados etc. formam a gama de informações que precisam ser consideradas no momento da elaboração do anteprojeto de lei penal. Dessa pesquisa, elabora-se um esboço normativo a respeito dos pontos mais importantes relacionados ao tema.

O ponto fulcral é identificar *o que* precisa ser tutelado pela lei, ou seja, o bem jurídico-penal. No caso dos delitos informáticos, identificamos como bem jurídico a segurança das informações pessoais e corporativas presentes em sistema informatizado ou rede de computadores.[1]

Tendo como objetivo proteger nossos dados pessoais (senhas, números de cartão de crédito, endereços, dados relacionados à identificação pessoal etc.), optou-se por criminalizar as seguintes condutas:

a) Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado;

b) Obtenção, transferência ou fornecimento não autorizado de dado ou informação;

c) Divulgação ou utilização indevida de informações e dados pessoais;

d) Inserção ou difusão de código malicioso;[2]

e) Além de outras adaptações em delitos presentes no Código Penal, como o dano, o estelionato e a falsificação de documentos, públicos e particulares, no âmbito digital.

2. Eficácia da tutela dos dados informáticos

No plano da eficácia – que entendemos ser a obtenção de resultados preventivos satisfatórios na tutela penal –, precisamos partir de uma análise do plano abstrato para chegarmos robustecidos normativamente ao plano concreto.

A questão relevante oriunda desse cenário relaciona-se a qual tipo de tutela será necessária para, efetivamente, conseguirmos minimizar os riscos pessoais e patrimoniais presentes no plano cibernético.

Abstratamente, a lei deve ser material e formalmente constitucional. Se carregar em seu texto vícios de inconstitucionalidade, está fadada ao desaparecimento. Todo o trabalho envolvendo sua elaboração e aprovação é desperdiçado. Um desrespeito não apenas ao nosso texto maior, mas também aos cofres públicos, pois o custo relacionado à aprovação de um projeto de lei que tramita há mais de dez anos no Parlamento, não pode ser desprezado por ignorância, teimosia, corporativismo, *lobby* etc.

Além da compatibilidade vertical, a análise horizontal não é menos importante. As novas regras devem estar atentas à vigência e validade do material legislativo já positivado, para evitar antinomias, revogações tácitas e discussões exegéticas judiciais, criando instabilidade nas relações cotidianas e insegurança jurídica para os destinatários da lei.

Saindo do confronto com outras regras jurídicas, volta-se a análise para o próprio projeto de lei. Como estamos lidando com algo novo, nem mesmo previsto na Constituição Federal de 1988, urge sejam apresentados conceitos. Felizmente, o projeto traz alguns conceitos no art. 16 do PL 84/99.[3] Busca-se, com essas normas penais explicativas, respeitar o princípio da legalidade, em especial, a taxatividade.

Mesmo preenchidos todos os requisitos constitucionais e legais, resta o principal problema do tratamento penal dos delitos cibernéticos: a sua aplicabilidade prática.

Para responsabilizarmos uma pessoa pela prática de um delito clássico, importante identificar o *autor* da conduta, o *local* dos fatos, o momento da *consumação* do delito e a *materialidade*.

Desloque essas questões para o plano virtual e inúmeros questionamentos surgem. O local de cometimento dos delitos é um *Internet Protocol* – IP, um sistema, um hardware, um software, enfim, endereços diferentes do que a estrutura clássica investigativa do Estado conhece; quanto à autoria e à materialidade, a distância e o anonimato de quem está por trás do microcomputador, locais públicos de acesso à internet, programas que confundem o rastreamento de informações mostram-se como obstáculos aparentemente intransponíveis; entre outros pontos que precisam ser verificados.

Estaria o Direito Penal, engessado por sua gama de direitos e garantias, apto a resolver essas questões?

3. Direito penal como *ultima ratio*

Dano eletrônico, estelionato eletrônico, falsificação de dado informático público ou particular são condutas que acompanham delitos clássicos por todos conhecidos. A tutela penal, nesses casos, parece-nos necessária.

Mas os problemas estruturais de identificação de autoria e materialidade passam, necessariamente, por perícias especializadas e aparato investigativo técnico.

Pensando nessas questões e em suas soluções, o PL 84/99 traz duas regras importantes: *a)* desloca a solução para a estrutura que precisará ser desenvolvida, em seu art. 17: "*Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado*"; *b)* transfere para o responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público, uma série de deveres, obrigando o provedor, agente público ou particular, a fiscalizar o conteúdo que hospeda.[4] Não iremos ingressar, por ora, na discussão sobre a inconstitucionalidade do art. 20 do PL 84/99.

4. Considerações conclusivas

- Entendemos que a tutela penal específica das informações virtuais é necessária;
- O bem jurídico-penal tutelado é a segurança das informações pessoais e corporativas presentes em sistema informatizado ou rede de computadores;
- Os grandes responsáveis pela eficácia da nova lei serão os departamentos especializados de investigação e perícia policiais e a cooperação forçada dos provedores de internet para identificar conteúdo criminoso nos meios virtuais e denunciá-lo

às autoridades com o fim de auxiliar na responsabilização dos agentes ativos dos novos delitos.

Há muitas outras questões relevantes relacionadas ao tema, como a pena a ser aplicada, a interceptação de dados para investigar os delitos informáticos, a ação controlada na investigação, a cooperação particular de *hackers*, a regulamentação prévia de utilização de *lan houses* para fins de investigação, o tratamento internacional do tema, com a necessária cooperação entre os Estados etc.

A busca pela paz no ambiente virtual é positiva. Só não pode se deixar seduzir pelo simbolismo negativo e pelo discurso vazio e pouco efetivo da chamada *lei e ordem*. Se a responsabilidade criminal no âmbito virtual é complexa, mais inteligente será se utilizarmos mecanismos preventivos, no âmbito administrativo, com fiscalização séria e resultados concretos.

NOTAS

(1) Há ampla discussão doutrinária a respeito do bem jurídico dos delitos informáticos. Sobre a identificação de qual bem é tutelado nos delitos envolvendo dados informáticos, cf. **LOPES DA SILVA, Rita de Cássia**. *A informação como bem jurídico-penal e o sistema informático*. *Revista Ciências Penais* n. 7, p. 242; **VIANNA, Túlio Lima**. *Do delito de dano e de sua aplicação ao direito penal informático*. *Revista dos Tribunais* n. 807, p. 486.

(2) Sobre os tais códigos maliciosos (vírus), antivírus e a legítima defesa, cf. importante trabalho do Prof. **Spencer Toth Sydow**, *A pertinência do instituto da legítima defesa frente ao recurso informático do antivírus*, *Revista dos Tribunais* n. 896, p. 463.

(3) *"Art. 16. Para os efeitos penais considera-se, dentre outros: I – dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia; II – sistema informatizado: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente; III – rede de computadores: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial através dos quais é possível trocar dados e informações; IV – código malicioso: o conjunto de instruções e tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida; V – dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado; VI – dados de tráfego: todos os dados informáticos relacionados com sua comunicação efetuada por meio de uma rede de computadores, sistema informatizado ou dispositivo de comunicação, gerados por eles como elemento de uma cadeia de comunicação, indicando origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente."*

(4) *"Art. 20. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público é obrigado a: I – manter em ambiente controlado e de segurança, pelo prazo de três anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, destino, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade policial e ao Ministério Público, mediante requisição; II – preservar imediatamente, após requisição, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade; III – levar ao conhecimento, de maneira sigilosa, da autoridade policial ou judicial, informação em seu poder ou que tenha ciência e que contenha indícios da prática de crime sujeito a acionamento penal, cuja prática haja ocorrido no âmbito da rede de computadores sob sua responsabilidade, ressalvada a responsabilização administrativa, civil."*

Ivan Luís Marques
Mestre em Direito Penal pela USP.
Professor de Ciências Criminais e Direito Constitucional.
Advogado e parecerista.
Coordenador Editorial da Thomson Reuters.

ALGUMAS REFLEXÕES SOBRE OS CRIMES DE PERIGO CONCRETO

Fabio Roberto D'Avila e Stephan Doering Darcie

No direito penal brasileiro, os crimes de perigo concreto têm sido tradicionalmente definidos como uma categoria típica que se particulariza por exigir a comprovação de que o bem jurídico tutelado tenha estado efetivamente em perigo. Opõem-se, assim, aos denominados crimes de perigo abstrato, nos quais o perigo, na posição de mero elemento de motivação da lei, é presumido pelo legislador. Para essa compreensão, tais traços distintivos decorrem do fato de que, enquanto nos crimes de perigo concreto o perigo constitui elementar típica, nos crimes de perigo abstrato ele traduz apenas um atributo genérico da conduta, motivo pelo qual a sua efetiva verificação no caso concreto se afigura prescindível aos fins a que se presta a norma, manifestamente o de coibir a prática da própria conduta (normalmente perigosa).

Referida distinção, por óbvio, acaba por admitir um contexto jurídico no qual o princípio da ofensividade resulta mitigado em importância e aplicabilidade. Têm lugar, a partir disso, as já conhecidas decisões em que se reconhece a tipicidade de condutas como a de portar arma de fogo sem munição ao alcance ou a de mera desobediência a determinações administrativas em âmbito econômico e ambiental, nas quais não há, nem de perto e nem de longe, qualquer possibilidade de dano aos respectivos bens jurídicos tutelados.

Todavia, como já se sabe e como há muito se vem defendendo,(1) o erigir do princípio da ofensividade como barreira infranqueável à intervenção penal não permite tal leitura. Para se adequar à exigência de ofensividade, a compreensão dos crimes de perigo abstrato deve desvencilhar-se da noção de perigo presumido, estabelecendo o perigo como noção normativa condicionada à constatação de, ao menos, uma possibilidade não insignificante de dano a um bem jurídico-penal e, como tal, revestida de um autônomo desvalor de resultado. Apenas assim é que podemos falar em perigo e, pois, em ofensividade, uma vez que, como há muito observou **Binding**, presunção de perigo não é perigo e tampouco poderá ambicionar sê-lo.(2) Para tal incompatibilidade, contudo, a doutrina jurídico-penal parece já haver atentado, e, conquanto não se possa ainda falar em consenso quanto à sua resolução, fato é que ao menos o problema parece já percebido.

Nesse cenário, entretanto, um outro problema de igual importância passa desapercebido: a insuficiente conceituação dos crimes de perigo concreto.

> Torna-se necessário buscar no próprio conteúdo material dos crimes de perigo concreto o seu traço definidor. O que, por sua vez, nos reconduz diretamente à **Binding**, para quem o perigo é sempre um "*abalo da certeza de ser*"...

Como já observado, segundo a sua corriqueira definição, os crimes de perigo concreto particularizam-se por exigir a comprovação *in concreto* de que o bem jurídico tutelado tenha estado em perigo, o que decorre da específica menção ao termo "perigo" no *Tatbestand*. Sabe-se, no entanto, que a necessidade de verificação do perigo traduz uma exigência ínsita a todos os crimes de perigo, razão pela qual se faz presente também nos crimes de perigo abstrato. Daí a absoluta insuficiência de um critério meramente formal para a delimitação entre crimes de perigo concreto e crimes de perigo abstrato. Uma adequada leitura dos crimes de perigo concreto não deve, pois, limitar-se a constatar a referência típica ao perigo, mas sim atentar para o significado material da expressa referência ao perigo no âmbito da descrição típica.