



Leonardo Cecílio: Marco civil embasará futuras leis sobre cibercrimes

27/06/2014

Na última segunda-feira (24/6) entrou em vigor a Lei 12.965/14, instituindo o marco civil da Internet no Brasil. Trata-se de um ineditismo normativo de escala internacional ao positivizar princípios, direitos e garantias para o uso da web no País e traçar diretrizes para a atuação dos entes federativos.

Pioneira em abrir consulta à sociedade civil, através de uma plataforma online, em linhas gerais, a nova lei estabelece como fundamentos a finalidade social da rede, os direitos humanos, o exercício da cidadania e a livre concorrência, e, para isso, consagra a liberdade de expressão, a proteção da privacidade, a preservação da neutralidade, da liberdade negocial e da natureza participativa da internet. Insculpindo no ordenamento jurídico uma série de direitos de usuários e provedores de conexão, o diploma cataloga bens jurídicos ligados à tecnologia até então flutuantes na doutrina, moldando um novo parâmetro para futuras legislações sobre crimes na web.

Modernamente, costuma-se creditar à disciplina penal a eficácia no combate à criminalidade, recorrendo-se à incriminação reiterada de condutas e ao recrudesimento das penas em uma desajeitada tentativa de se aplacar a ânsia por segurança de uma coletividade que se autocompreende como vítima. A identidade de *ultima ratio* do Direito Penal vai, assim, sendo subvertida pela cultura da emergência, e conduzida à condenável prática de se legislar baseando-se em episódios determinados.

As atuais configurações ostentam a valoração de novos elementos (ou, ao menos, nova valoração de elementos já existentes) como indispensáveis para uma vida plena e autorrealizada no contexto social, o que os torna novos paradigmas da intervenção do Direito Penal. Mas, se a disciplina tem se expandido e se condicionado a partir da urgência, a política criminal no ambiente web não seria diferente.

Diretamente proporcional ao incremento das tecnologias da informação e comunicação (TICs) é o aumento das atividades mal intencionadas no campo informático. Sejam ações já previstas ou não na legislação penal, as *hostilidades informáticas* são hoje destaque crescente nos relatórios de segurança e na imprensa internacional, e sua complexa linguagem *sui generis* desafia produtor, operador e destinatário da norma. A maior dificuldade na definição de crimes no ambiente tecnológico é, seguramente, a identificação do que se pretende tutelar.

Há um embaraço conceitual que faz considerar como *crime informático* qualquer conduta hostil relacionada a computadores, chegando-se ao contrassenso de assim se classificar até mesmo ações que sequer são definidas como crime. De todo modo, a drasticidade do comparecimento do Estado no cotidiano social pela via incriminadora declara que a escolha do legislador pelo Direito Penal demanda parcimônia e precisão. Deve-se a isso o fato de a incriminação, para ser legítima, ter de partir da eleição do *bem jurídico*.

Afirmava José Frederico Marques que toda infração penal pressupõe a violação de uma proibição normativa de outro campo do Direito; a sanção punitiva complementa uma outra norma (não penal), exercendo uma função de reforço e mantendo sob sua égide o bem jurídico. Contudo, por força normativa do princípio da fragmentariedade da disciplina, somente os bens jurídicos *mais relevantes* são dignos da tutela penal, e para isso é necessário um juízo de importância social bastante para se justificar sua real necessidade.

A política criminal que toca o ambiente de alta tecnologia hoje confunde condutas direcionadas contra a informática com as que dela se valem como mero instrumento para atacar bens jurídicos já contemplados no direito positivado. A própria Convenção de Budapeste – que inaugurou no plano internacional o combate normativo ao chamado *cibercrime* – propôs definições de delitos específicos a partir da combinação de tipos já conhecidos com a circunstância peculiar de serem praticadas através de sistemas informatizados – como os crimes contra a honra e os crimes de ódio, que, como sabemos, já possuem seu bem jurídico bem definido e não representam, por si só, qualquer risco à segurança da informação. Uma difamação praticada em ambiente de trabalho ou em uma comunidade residencial, por exemplo, não se difere de uma cometida via internet. Da mesma forma, discursos racistas são discursos racistas – ocorram dentro ou fora da rede.

Em casos como esses, temos – quando muito – *crimes informatizados*, que nada mais são que meras versões digitais de delitos já tipificados e profundamente estudados pela doutrina penalista. Hipótese totalmente diversa é aquela em que uma conduta representa um ataque à segurança da informação ou das ferramentas (físicas ou lógicas) responsáveis pelo processamento, armazenamento e transferência de dados.

O marco civil da internet contempla a proteção da *estabilidade, segurança e a funcionalidade da rede* (art 3º, V), trazendo para o direito positivo o resguardo da *disponibilidade* da informação – garantia de que estará a serviço do usuário quando acessada, e que é ameaçada, por exemplo, nos *ataques de negação de serviço* (DDoS), que suspendem websites pela sobrecarga do servidor.

Outro exemplo é a *proteção dos dados pessoais* (art. 3º, III), que corresponde à *confidencialidade*, à *autenticidade* à *integridade* da informação – garantidoras de que ela será acessada somente por usuários autorizados e legítimos, e de que não serão corrompidas. São violadas, dentre variadas possibilidades, quando há o *acesso indevido* – seja remoto ou local – a um terminal.

É fundamental compreendermos a inviabilidade de se inserir na mesma categoria de crimes condutas que violem bens jurídicos diferentes simplesmente porque relacionadas à cibernética, porque, em geral, trata-se de uma questão de *modus operandi*. O meio especializado hoje fala na tendência da *Internet of Things* (IoT), a *internet das coisas* – que já está sendo construída.

Hoje, a internet já possui alcance interplanetário, conectando de satélites a eletrodomésticos, e estima-se que, em futuro não muito distante, haverá uma conexão *absoluta* em rede – incluindo seres vivos. Conceber como crime informático toda a gama de possíveis delitos pela circunstância de estarem vinculados às TICs será tão leviano quanto seria considerar como

crime econômico todo delito que guarde relação com dinheiro, como o furto de uma carteira contendo moeda em espécie.

Referências:

BECK, Ulrich. *O que é Globalização: equívocos do globalismo, respostas à globalização*. Trad. CARONE, André. São Paulo: Paz e Terra, 1999.

CECILIO, Leonardo Rezende; *et al.*. Complejidad Janus: La doble cara de la información. In: *FODERTICS 3.0*. Coord. Federico Bueno de Mata. Santiago de Compostela: Andavira, 2014 (no prelo).

MARQUES, Jose Frederico. *Tratado de Direito Penal*. Vol. 1. 2ª Ed. Propedêutica Penal e Norma Penal. São Paulo: Saraiva, 1964.

SILVA SÁNCHEZ, Jesús María. *La Expansión del Derecho Penal: Aspectos de política criminal en las sociedades postindustriales*. Tercera Edición. Madrid: EDISOFER S.L., 2011.

PRADO, Luiz Régis. *Bem jurídico penal e Constituição*. Revista dos Tribunais, 1997.

Fonte: <https://conjur.jumps.com.br/2014-jun-27/leonardo-cecilio-marco-civil-embasar-futuros-diplomas-ciber Crimes/>