



Identificar autores de crimes eletrônicos é cada vez mais possível

Embora ainda se discuta uma nova legislação para regulamentar os crimes na internet, hoje já se sabe que as regras atuais valem tanto para o mundo real como para o virtual. Sabe-se, também, que um dos principais desafios dos crimes eletrônicos é identificar o autor. Especialistas em Direito de Informática explicam que a maior dificuldade é a falta de obrigação dos servidores de gravar os dados de seus usuários.

“Não há uma lei que determine uma ‘identidade digital obrigatória’, apesar de a Constituição Federal Brasileira proibir o anonimato”, explica **Patricia Peck**, especialista em Direito Digital. Há casos no escritório de Patrícia em que provedores e *lan houses* estão sendo responsabilizados judicialmente por “risco de atividade” ou “omissão”, de acordo com as regras do Código Civil. “A Justiça também tem responsabilizado provedores quando o mesmo recebe uma solicitação de retirada de conteúdo do ar pelo canal de denúncia ou através de notificação extrajudicial ou judicial e não o faz, ou seja, apesar de ciente, tem conduta negligente.”

Para **André Zonaro Giachetta**, sócio da área de propriedade intelectual do escritório Pinheiro Neto, as decisões na Justiça já mostram que os servidores são obrigados a fornecer informações. “Grande parte das decisões hoje entende que o provedor não é responsável antes de saber do ato ilícito cometido pelo seu usuário.” Para o advogado, os servidores de acesso devem ter essa obrigação (de identificação do usuário) pois guardam a informação mais importante — o endereço IP.

Pegadas tecnológicas

Para o advogado Giachetta, que tem servidores entre a maioria de seus clientes, é muito mais fácil identificar crimes pela internet, que deixam pegadas, do que muitos crimes no mundo físico. “O meio digital possibilita muito mais a identificação e provas do que antes e, mais do que se imagina, é possível chegar ao verdadeiro autor do ato.” Ele cita como exemplo o caso de uma grande rede varejista que entrou com ação contra um servidor, que tem como usuário um blogueiro que denegria a imagem da empresa. O advogado convenceu seu cliente de que era possível correr atrás do verdadeiro autor do ato ilícito. Com ajuda do provedor de conteúdo, conseguiu localizar o blogueiro e tirar do ar as informações que prejudicavam o grupo varejista.

No escritório de Patricia Peck, a cada dois casos, em um é possível identificar o autor do crime. “Os acessos à rede mundial de computadores são feitos com um número de protocolo (IP) único. No entanto, é comum, também, já que um IP não ser uma pessoa, mas sim um acesso, não se conseguir identificar o usuário que estava na máquina naquele momento.” Isso acontece nos crimes cometidos por meio de computadores públicos, como *lan houses* e *cyber cafés*.

Para evitar o desgaste na busca pelo verdadeiro criminoso, alguns estados e municípios já estão fixando leis que obrigam *lan houses* a manter o cadastro de seus clientes. “Em São Paulo, temos a Lei 12.228/06, que disciplina a obrigatoriedade da guarda dos registros dos dados cadastrais dos usuários de conexão à rede mundial de computadores em *lan houses* e *cybercafés* por 60 meses”, conta Giachetta. Está também em tramitação na Câmara dos Deputados o Projeto de Lei 84/09, já votado no Senado, que deve

regulamentar a identificação de usuários em todo o país. A proposta é vista como censura e corre o risco de morrer antes de ser votada pelos deputados (clique [aqui](#) para saber mais).

André Giachetta acredita que identificar usuários em espaços públicos é um dos menores problemas do crime virtual. “Há graus de dificuldade para indicar o culpado, mas não é impossível.” Para ele, o número do IP hoje é muito mais relevante do que qualquer outro dado do internauta. “Em um crime de internet, ter o RG do suspeito é menos importante do que o endereço de IP, que prova o momento e local em que o ato foi cometido.”

Mundo sem fronteiras

Outro desafio para proteger a privacidade no mundo virtual é que a internet é global e a lei, brasileira. De acordo com Patricia Peck, se um site internacional, que não possui representação ou servidor no Brasil, ofender um internauta de alguma maneira e se recusar a tirar a informação do ar, o juiz pode emitir uma carta rogatória — que possibilita ações entre os Judiciários de diferentes países. “Mas isso gera um ônus de tempo que nem sempre a vítima está disposta a pagar e acaba não fazendo nada.” Para Patricia, as ações internacionais são complicadas, mas são possíveis. “Os sites ditos ‘internacionais’ devem saber que a exposição mundial gera um custo que é a possibilidade de responsabilização perante diversos ordenamentos jurídicos.”

Por conta destas dificuldades, a ordem é prestar atenção nos contratos firmados e estar ciente do que pode ocorrer com os dados, fotos e informações que o internauta disponibilizar. “A pessoa concorda e usa ou não concorda e não usa. O poder de escolha é do usuário, já que o concorrente está a um ‘click’ de distância.” A advogada **Alice Andrade**, especialista em Direito Digital e sócia do Patricia Peck Pinheiro Advogados, conta o caso de um cliente, presidente de uma grande empresa e professor de universidade, que teve um perfil falso criado no *Twitter* por seus alunos. Bastou entrar em contato com o site para retirar o perfil do ar.

Segundo ela, é claro que é possível denunciar abusos em contratos, como é previsto em lei, mas há uma certa dificuldade processual de fazer este direito valer. Por isso, os internautas optam pela pressão coletiva. A rede social *Facebook*, por exemplo, firmava em seu termo que todas os dados disponibilizados passavam a ser de propriedade do site, mas a empresa resolveu voltar atrás diante da reação desfavorável dos usuários.

Omar Kaminski, especialista em Direito de Informática, explica que os termos de uso dos sites são como contratos firmados. “Os termos de uso e de privacidade são como qualquer contrato de adesão. Tratando-se de relação de consumo, prevalece a hipossuficiência do consumidor e a aplicação da Lei 8.078/90”, explica.

Um exemplo de crime na internet foi noticiado pela rede de notícias BBC. Segundo a agência, *hackers* invadiram o sistema da página de microblog *Twitter*, acessando documentos importantes da empresa. Um dos sites de notícia que recebeu os documentos hackeados publicou as notícias que acreditavam ser de interesse público, como o fato da empresa estar prestes a criar uma produtora de TV. O fato se deu sob a legislação norteamericana mas, segundo especialistas, se fosse no Brasil, tanto quem distribuiu o material como quem o divulgou corre riscos de enfrentar uma ação judicial, pois trata-se da divulgação



de conteúdo estratégico da empresa, frente à concorrência.

Alice Andrade explica que a venda e divulgação de dados cadastrais de pessoas físicas na internet deve ser analisada caso a caso. “É possível entrar com uma ação judicial quando a divulgação deste dado cause algum dano”, explica. Antes que isso ocorra, segundo a especialista, é preciso analisar o nível de privacidade destes dados. Se o dado divulgado é o número de um telefone ou o de um CPF, por exemplo, também é aplicável o Código de Defesa do Consumidor (artigos 43 e 44). “Se a informação foi passada com uma ressalva de confidencial, ou seja, numa relação de confiança entre as partes, aquele que a divulga a terceiros sem prévia autorização pratica ato ilícito.”