IDENTIFICAÇÃO DA AUTORIA NOS CIBERCRIMES

Autor: **Carolina de A. V. Chaves** Fonte: **Alfa-Redi**

A questão da identificação da autoria das condutas efetuadas no meio eletrônico, especialmente quanto aos crimes, é motivo de grande preocupação para os especialistas em novas tecnologias.

Diante do crescimento do número de litígios, especialmente relacionados à propriedade intelectual, à honra e ao patrimônio, juízes, advogados, sites, provedores e usuários estão cada vez mais envolvidos na busca de uma solução rápida, eficaz e economicamente viável para a determinação da autoria.

Não se tem aqui a pretensão de esgotar o tema ou mesmo apontar uma solução para a controvérsia mas alertar a comunidade sobre as situações que cada vez mais estarão presentes no cotidiano dos operadores do direito, assim como mostrar o material utilizado pelos especialistas, sem se ater a condutas específicas, buscando uma visão geral do problema.

O anonimato

Inicialmente, é importante demonstrar que o início das condutas socialmente reprováveis vem da sensação de anonimato e de impunidade da grande massa de usuários da Internet.

Apesar da Internet ser um local em que transitam milhares de pessoas espalhadas nos diversos locais do planeta, que circulam e interagem fazendo desta um ambiente a-nacional ou transnacional, existe uma nítida contradição na sua estrutura. Trata-se da pontualidade das relações, o “one to one”, que enseja a sensação de anonimato ao usuário comum e que, muitas vezes, geram atitudes que as pessoas não tomariam diante de olhos alheios. É a sensação de estar escondido atrás da tela do computador.

Entretanto, pressupor que a Internet é um local onde vigora o anonimato é um grande erro. A rastreabilidade das condutas efetuadas no meio eletrônico é absolutamente possível.

Foi o que ocorreu em janeiro deste ano com Pete Townshend, líder da banda The Who, que foi preso pela polícia londrina por ter acessado sites de pedofilia. Não há dúvidas de que o músico foi motivado pelo sentimento de anonimato e pela curiosidade, passando a visitar sites de conteúdo ilícito e socialmente reprovável na expectativa de que ninguém saberia ou descobriria.

Neste sentido, o “sentir-se protegido" invoca um sentimento de impunidade, por não se acreditar que qualquer conduta lesiva praticada pelo computador, poderá ensejar responsabilidades. E, não há como negar que, havendo possibilidade de rastrear os movimentos dos usuários, conforme demonstraremos a seguir, existe responsabilidade na Internet, civil e criminal, e que ela poderá ser requerida desde que se comprove o dano, a conduta do autor e seu nexo de causalidade.

Deve-se, portanto, alertar o usuário comum, leigo ou com poucos conhecimentos de informática, sobre suas responsabilidades, contribuindo para uma política preventiva que se destine a evitar determinadas condutas socialmente lesivas.

A maior dificuldade no combate às condutas no meio eletrônico é quando estas são praticadas por grandes profissionais. Estes costumam não deixar vestígios, utilizando-se de artimanhas a fim de enganar a polícia e dificultar a atuação dos peritos na sua identificação. Um especialista, por exemplo, jamais mandaria e-mail de conteúdo calunioso ou acessaria um site com conteúdo lesivo de seu próprio computador. Logo, políticas de combate aos especialistas são extremamente complexas e difíceis de serem implementadas.

O problema da identificação

O problema da identificação da autoria, para fins de responsabilização, civil ou criminal, se pauta em alguns aspectos fundamentais:

a) As informações utilizadas para identificação da autoria

b) Interpretação e a coleta das informações

c) Obstáculos no acesso às informações

d) Detentores das informações

Os criminosos na Internet, os chamados crackers estão cada vez mais atualizados em novas tecnologias, o que dificulta a prevenção das empresas nas políticas de segurança da informação e dos sistemas computacionais. E não restam dúvidas, de que nos próximos anos os atos criminosos, em sua maioria, serão praticados pelo computador.

a) As informações utilizadas para identificação da autoria - Os dados identificadores

A Identificação é possível e já é muito praticada. Utiliza-se de elementos peculiares ao meio eletrônico que possibilitam a individualização do usuário ou da máquina. São utilizados o número IP (Internet Protocol), o registro de logs de acesso, a conta do e-mail e seus dados cadastrais e senhas ou cadastros nos provedores e sites. Assim, com este material é possível identificar a máquina, o usuário, o tempo de acesso, os locais visitados e o perfil da visita.

Entretanto, esta identificação traz um grande problema: encontrar a máquina, o responsável pela conta de e-mail ou o responsável por um determinado site não significa que se identificou o autor do fato ou da conduta que ensejou uma investigação para eventual responsabilização.

As senhas podem ser violadas, o computador pode ter sido utilizado por pessoa não pertencente ao sistema, remotamente ou não, e outras situações. O único método que garante a autenticidade, ou seja, que proporciona a certeza da autoria é a assinatura digital, em que há o não-repúdio nos casos das assinaturas emitidas por autoridades homologadas pela ICP-Brasil, e poderá tranqüilamente ser utilizado como prova da autoria, num processo que tramita no judiciário brasileiro.

b) Interpretação e a coleta das informações

A análise dos dados identificadores depende de trabalho especializado para a coleta e interpretação das informações. Ocorre que, além de especialistas em tecnologia da informação e peritos em telemática, há necessidade de profissionais que compreendam os termos técnicos e saibam utilizá-los na defesa ou na acusação.

Assim, existe a dificuldade de se saber quais dados coletados são importantes ou dispensáveis para comprovação do fato e de sua autoria e que possa ensejar ingresso de ação na esfera criminal e cível.

c) Obstáculos no acesso às informações – o sigilo e a privacidade das informações

O acesso e a utilização de dados, especialmente na fase de investigação, apresenta uma questão fundamental: estes são sigilosos? Podem ser fornecidos mediante notificação? Somente uma legislação poderá resolver esta questão, especialmente no relacionamento com os provedores e sites.

A busca por maior segurança no meio eletrônico, as políticas preventivas das empresas pontocom e a necessidade de identificação para fins de responsabilização por condutas reprováveis são temas importantes para a atual realidade da Internet.

Estes temas, entretanto, chocam com questão da privacidade e do sigilo das informações pessoais. Não temos dúvidas que a palavra privacidade, nos últimos tempos, está cada vez mais sendo utilizada e suas proporções são muito maiores do que há alguns anos.

Privacidade e sigilo são direitos garantidos por nossa Constituição e em importantes tratados internacionais, já ratificados pelo Brasil. Ambos se relacionam com informações estratégicas, identificadoras e individualizadoras das pessoas físicas e jurídicas. Como ponderar a necessidade de maior segurança com a questão da Privacidade e do sigilo, ainda é, e por um bom tempo será, uma dúvida latente.

E, em especial, existe a dúvida se os dados identificadores com IP, registro de logs, contas de e-mail são de fato passíveis de proteção baseada na privacidade e no sigilo assim, como assim ocorre no caso das correspondências e das comunicações telegráficas.

d) Detentores das informações – O papel dos provedores e dos sites

Rastrear o e-mail que enviou mensagem ilícita, de caráter desonroso ou ameaçador, detectar quem foi o responsável pela violação dos direitos autorais e outros exemplos corriqueiros dependem de um elemento essencial: o provedor de Internet. Os provedores são os que mais estão preocupados com tal tema, tendo em vista os gastos elevados para atuar de acordo com as disposições legais.

De fato, após a entrada em vigor do Novo Código Civil, e com a adoção completa da Teoria do Risco do artigo 927, parágrafo único, os provedores passaram a se preocupar com a questão da identificação e, principalmente, com a possibilidade de serem chamados em juízo ou notificados para prestarem informações sobre eventos ocorridos dentro de seus sistemas.

Os provedores devem conter bancos de dados suficientes para armazenar os dados de todos aqueles que se conectam ao seu serviço. E diante do conselho de especialistas, os provedores deverão armazená-los por tempo mínimo de três anos.

E, neste sentido, não há como negar que, sem a atuação do provedor no fornecimento de dados, haveria sim, a impunidade na Internet, e muitos casos ficariam sem efeito.

A dificuldade na questão está pautada em 2 aspectos gerais que são utilizados como argumentos pelos provedores: o sigilo garantido pela Constituição de 1998 e a privacidade do fluxo da informação.

E como a privacidade é um dos temas que ganharam dimensões enormes na Internet é sob este argumento e baseados na legislação sobre interceptação de fluxo que as empresas provedoras evitam a disponibilização das informações requeridas.

Entretanto, a opinião de que tais dados infrinjam tal legislação não parece acertada, principalmente quando pautados na necessidade da prestação jurisdicional. Isto não significa que os provedores atuam condizentes com a criminalidade crescente na Internet, mas que se utilizam tais argumentos para salvaguardar as informações de seus usuários.

Desta forma, havendo necessidade, e após tal demonstração, os provedores deverão sim, disponibilizar dados que comprovem a autoria, ou seja, quem estava utilizando o computador e praticou a conduta, sob pena de se aplicar às sanções determinadas pela responsabilidade objetiva, tendo em vista a atividade que exercem.

Neste paradigma, atualmente, para haver a devida prestação jurisdicional, o autor deverá ingressar com ação própria contra os provedores para obter primeiramente os dados, caso mediante outros meios estes não sejam fornecidos.

A responsabilidade objetiva dos provedores se dá a partir da notificação. Sabendo da consulta e da necessidade de disponibilizarão, este se vincularia ao autor numa relação de responsabilidade civil, de caráter indenizatório, pelos danos decorrentes da falta da informação necessária para propositura de demanda contra o autor da conduta lesiva.

Uma legislação neste sentido facilitaria o trabalho e diminuiria os custos para as partes. Esta deveria ser pautada na fundamentada necessidade de disponibilização da informação. Assim, comprovando o dano, estas poderiam ser fornecidas.

Da mesma forma ocorre com os sites que devem guardar os dados de seus usuários para eventuais litígios. Não há duvidas de que este posicionamento ensejará, num futuro próximo, a exigência dos sites de que seus usuários, antes de ter acesso ao seu conteúdo, se loguem. O principio da responsabilidade objetiva aplica-se também e da mesma forma, aos sites.

Estas questões supracitadas cada vez mais serão discutidas e em breve deverá ser elaborado projeto de lei a respeito. E a exemplo de outros países, precisamos garantir segurança jurídica na Internet com uma junção de normas jurídicas e técnicas para o controle daqueles que utilizam mal a tecnologia visando vantagens indevidas.

E a Internet será mais confiável quando as pessoas souberem utilizá-la com bom senso e quando se prevalecerem da sensação de estarem anônimas para aumentarem seus relacionamentos de forma positiva e que haja, sim, responsabilização dos eventos provenientes do meio eletrônicos.

E que principalmente, os usuários tenham a consciência que privacidade na Internet estará cada vez mais restrita e que seus dados, seu perfil, sua conduta em algum lugar ficará registrada e por alguém, que poderá utilizá-la no caso de litígio.

Utilizar o computador com bom senso, consciência e boa-fé são requisitos para um convívio seguro com as novas tecnologias.