

ENTREVISTA - Tema: DIREITO DIGITAL

Concedida à Acadêmica de Direito Srta. Patrícia Queiroz Madeira

Universidade Presbiteriana Mackenzie

1) Como se pode avaliar o direito digital brasileiro atualmente em comparação com o direito estrangeiro?

GT: A legislação brasileira atual já é aplicável a diversas situações relacionadas ao Direito Digital, tais como contratos, crimes digitais, provas eletrônicas, demissão por justa causa por uso indevido de ferramentas tecnológicas, dentre outros.

No âmbito do Direito Penal, podemos dizer que cerca de 95% dos crimes praticados pelos meios eletrônicos são puníveis pelo nosso Código Penal. Estes são os chamados crimes informáticos impróprios: delitos já tipificados pela legislação penal, que podem ser praticados através de um ambiente informatizado ou da Internet. (Exemplo: furto, crimes contra a honra, pedofilia).

A porcentagem restante refere-se aos crimes informáticos próprios, que são condutas ilícitas praticadas contra um ambiente informatizado. (Exemplo: disseminação de vírus, ataques de negação de serviço – “DOS”, etc.). Estas condutas ainda não são tipificadas e por conta desta lacuna legal é que surgiu a necessidade de possuímos uma legislação específica. Já existe um projeto de lei sobre o assunto, de autoria do Senador Eduardo Azeredo, que foi aprovado no Senado Federal e recebido pela Câmara dos Deputados sob a denominação de PLC nº 89/2003.

Em relação às provas eletrônicas, nosso Código de Processo Civil já prevê em seu artigo 332 a utilização de quaisquer meios legais para se provar a verdade dos fatos, autorizando-se a utilização de provas eletrônicas, que podem ser: emails, logs, SMS, banco de dados, documento gerado eletronicamente, etc. No mesmo sentido, nosso Código de Processo Penal (art. 155) e a Constituição Federal (art. 5º, LVI) também já dão margem ao uso de provas eletrônicas na esfera judicial.

Um ponto importante que deve ser observado quanto à prova eletrônica é a preservação de sua integridade. Para demonstrar que um arquivo eletrônico não foi alterado, sendo possível a realização de perícia, é necessário que o arquivo original seja preservado corretamente. Exemplo: em uma questão que discute a identificação do remetente ou destinatário de um email, caso

exista necessidade de periciar esta mensagem eletrônica, deverá ser apresentado o email original, que é aquele armazenado na caixa postal ou nos servidores, e não um email impresso. Isto porque, o email impresso não permite a realização de perícia, tendo em vista que é somente uma cópia daquele arquivo gerado eletronicamente.

Comparando o Direito Digital pátrio em relação à outros países, uma diferença evidente é a falta de legislação sobre a privacidade em nosso ordenamento. Há menção em nossa Constituição Federal quanto à violação de privacidade, porém, não temos uma legislação civil que regule essa questão, principalmente no tocante à identificação digital. Por exemplo, a comunidade européia possui ordenamento jurídico específico relacionado à privacidade do cidadão.

2) Quais são os casos mais comuns?

GT: No âmbito penal, os crimes digitais mais comuns são:

- **Crimes contra a honra** (calúnia, injúria e difamação – arts. 138 a 140, CP);
- **Ameaça** (art. 147, CP);
- **Pedofilia** (art. 241, ECA – Lei nº 8069/90, alterada pela Lei nº 11829/08);
- **Furto** (art. 155, CP) ou **Estelionato** (art. 171, CP) = transferência indevida de valores entre contas bancárias;
- **Falsa identidade** (art. 307, CP) = uso indevido de senha;
- **Concorrência desleal** (art. 195, Lei nº 9279/96) = vazamento de informações;
- **Violação de Direitos Autorais** (art. 184, CP).
- **Violação do Segredo Profissional** (art. 154, CP) e **Violação do Sigilo Funcional** (art.325, CP) = vazamento de informações – “insider”

Na esfera trabalhista, é muito comum ocorrerem casos de demissão por justa causa por conta de:

- **Uso indevido de email e de outras ferramentas tecnológicas corporativas** (celulares, smartphones, notebooks, etc). Exemplos: colaborador utiliza email corporativo para tratar de assuntos pessoais ou para envio/recebimento de conteúdo alheio ao trabalho

(pornografia/pedofilia); uso de equipamento corporativo para armazenamento de conteúdo pessoal (ex: notebook da empresa contendo material de uso particular do colaborador).

- **Assédio moral ou sexual por email;**
- **Violação de segredo profissional.**

Na esfera cível, os casos mais comuns são:

- **Indenização por danos morais (e materiais), devido à prática de crimes contra a honra;**
- **Identificação de autoria** *(geralmente há incidentes em que é necessária a identificação da autoria do ilícito, para posteriormente demandarmos na esfera penal. Nesses casos, a maioria das vítimas (pessoa física ou jurídica) acaba preferindo mover uma ação de obrigação de fazer no âmbito cível, para identificar o autor do fato através de uma ordem judicial enviada ao provedor de acesso à Internet . Devido ao recebimento de um mandado judicial, os provedores acabam fornecendo os dados de identificação do usuário.*
- **Indenização por danos morais e materiais, por quebra contratual** *(caso muito comum em relação a contratos de TI e Telecom, em que a indisponibilidade do serviço acaba provocando sérios impactos a uma empresa, gerando prejuízos institucionais e financeiros).*

3) Quais são as maiores dificuldades do direito digital hoje no Brasil?

GT: Uma das maiores dificuldades que encontramos em nosso cotidiano é levar o entendimento das questões relacionadas ao Direito Digital ao Judiciário, pois muitas vezes, os operadores do Direito ainda não compreendem determinados aspectos da Tecnologia que se relaciona ao mundo jurídico.

4) Acredita que existe conflito entre a liberdade de expressão, a privacidade na internet e a fiscalização dos meios eletrônicos? É possível fiscalizar sem ferir essas garantias?

GT: É perfeitamente possível combater os crimes digitais sem ferir a privacidade. É exatamente esse um dos pontos principais do PLC 89/2003, que prevê em seu art. 22 o armazenamento dos dados cadastrais dos responsáveis pelas contas de acesso à Internet. Essa obrigatoriedade seria dos provedores de acesso à Internet, vez que já possuem tais dados: nome de usuário, IP, data e horário

da conexão, referência GMT. Essas informações são apenas os dados de conexão dos usuários, que não são sigilosos. Logo, não há qualquer lesão à privacidade se armazenados tais dados.

Poderia existir violação à privacidade se os dados de tráfego fossem armazenados, pois estes se referem ao conteúdo navegado pelo internauta: sites que acessou, quais downloads foram efetuados, qual o teor dos emails enviados, dentre outros elementos.

Ao sabermos quem acessou a Internet ou qualquer sistema eletrônico, em que hora e data, estamos simplesmente identificando a pessoa. Neste momento, é quebrado o anonimato. Tendo em vista que nossa Constituição Federal veda o anonimato, a identificação do usuário da Internet ou de qualquer ambiente eletrônico é legal e válida.

5) Que melhorias você considera como necessárias para o desenvolvimento desse ramo em nosso direito?

GT: É necessária a implantação da disciplina de Direito Digital nas faculdades de Direito, para que o profissional já tenha contato com o assunto, estando mais bem preparado para o mercado de trabalho.

Também entendo como medida necessária a inserção de aulas sobre “Cidadania Digital” no currículo escolar dos jovens, a fim de conscientizarmos o cidadão quanto ao uso ético, seguro e legal das novas tecnologias.

Gisele Truzzi

Advogada especialista em Direito Digital e Direito Criminal.

www.truzzi.com.br

gisele@truzzi.com.br