

Douglas Ferreira Magalhães*
Luiz Henrique Borges de Azevedo**

ESTUDO DA EFICIÊNCIA JURISDICIONAL NO DIREITO CIBERNÉTICO

STUDY OF JUDICIAL EFFICIENCY IN CYBER LAW

ESTUDIO DE LA EFICIENCIA JUDICIAL EN EL DERECHO
CIBERNÉTICO

Resumo:

Na segunda metade do século XXI a humanidade conheceu um avanço tecnológico jamais visto: os novos meios de comunicação e a manipulação de dados, a internet. Porém, tais recursos podem ocasionar sérios problemas devido ao seu mal uso e ao obsolescimento jurisdicional acerca do modo ilícito com que a internet está sendo usada, como para praticar crimes como calúnia, difamação, violação ao direito autoral, incitação ao crime, apologia de crime ou criminoso, inserção de dados falsos em sistema de informações, adulteração de dados em sistema de informações, pedofilia, pirataria de software, dentre outros. Essas ações lesam direitos de terceiros, apresentam aparato legal no ordenamento jurídico pátrio, mas causam embaraço aos operadores do direito, por assim dizer, tipificação penal, cabendo-nos fazer distinção quanto aos novos tipos de crimes, que trazem a tecnologia computacional em seu corpo e que passaram comumente a ser chamados de crimes eletrônicos e informáticos.

Abstract:

In the second half of the twenty-first century humanity has known an unprecedented technological advances: new media and data

* Especialista em Auditoria Ambiental pela FMB. Especializando em Direito Processual Civil Contemporâneo e Direito Constitucional pela FMB. Bacharel em Direito. Secretário Auxiliar do MP-GO.

** Especialista em Direito Público pela FESURV, Direito Penal e Direito Constitucional pela UFG. Docente do curso de Direito da FMB. Técnico Judiciário do Tribunal Regional Eleitoral, Chefe de Cartório - São Luis de Montes Belos - GO.

manipulation, the Internet, but such features can cause serious problems due to misuse, obsolescence the court about the way the unlawful internet is being used, which use to commit crimes such as libel, defamation, infringement of copyright, incitement to crime, crime of condoning or criminal, inserting false data into information system, tampering of data in information systems, child pornography, software piracy, among many others. Such actions harm the rights of others, present the legal framework international legal system but cause embarrassment to law enforcement officers, so to speak, criminal classification, leaving us to distinguish for new types of crimes that bring computing technology into your body and that now commonly being referred to as electronic and computer crimes.

Resumen:

En la segunda mitad del siglo XXI la humanidad ha conocido un avance tecnológico sin precedentes: nuevos medios de comunicación y la manipulación de datos, la Internet. Sin embargo, tales características pueden causar serios problemas a causa de su mal uso y a la obsolescencia judicial acerca del modo ilegal con el que se usa la Internet, utilizada para practicar delitos como calumnia, difamación, violación de los derechos de autor, la incitación a la delincuencia, apología del delito o penal, la inserción de datos falsos en el sistema de información, la manipulación de los datos en el sistema de información, la pedofilia, la piratería de software, entre otros. Esas acciones en detrimento de los derechos de los demás tienen el aparato legal de las leyes nacionales, no obstante causar vergüenza a los agentes del orden, por así decirlo, la clasificación penal, lo que nos hace distinguir a los nuevos tipos de delitos, que traen a la tecnología informática en su cuerpo y llegan a ser comúnmente llamados delitos informáticos y electrónicos.

Palavras-chaves:

Direito penal, direito eletrônico, crimes na informática, obsoletismo.

Keywords:

Criminal law, electronic law, computer crimes, obsolescence.

Palabras clave:

Derecho penal, derecho electrónico, delitos informáticos, obsolescencia.

INTRODUÇÃO

A Internet é uma rede na qual todos os pontos se equivalem e não há comando central (BARAN, 2001).

As características técnicas e operacionais da Internet, notavelmente descentralizada, fazem com que não exista uma sede geográfica definida (território) para as operações que a rede, na totalidade, propicia. Daí surgir o conceito de ciberespaço ou de realidade virtual (FILHO, 1999).

Estamos diante da revolução do controle, da possibilidade de se tornar senhor de um mundo próprio (SHAPIRO apud MARZOCHI, 2005).

Isso pode ser observado pelo número crescente de “hacktivistas”. O “hacktivismo” consiste em usar as técnicas do *hacking* em causas políticas, numa guerra cibernética. Por exemplo, em 1999, sites do governo brasileiro foram substituídos por páginas de protestos (MARZOCHI, 2005).

O computador e a Internet são os elementos mais perceptíveis dessa nova realidade pelo lugar de destaque que ocupam na vida humana, seja na realização de tarefas ou no entretenimento. É o símbolo dessa nova era. Enquanto o símbolo da Guerra Fria era um muro, que separava, a Internet é o símbolo que une (FRIEDMAN, 1999).

Trouxe para todos nós, mesmo para os menos atentos aos fatos históricos, a visão de que uma nova sociedade estava se formando: um mundo no qual os indivíduos, conectados entre si, começaram apenas “navegando” em busca do conhecimento universal, mas que depois passou a ser o ambiente em que tudo o mais passou a ser realizado. De fato, não se poderia pretender que o Direito ficasse indiferente a esse magnífico fenômeno humano. As normas

de estudos físicos se assemelham à realidade jurisdicional, como relatado na terceira lei de Newton, na qual toda ação está associada a uma reação, a todo impacto nas relações humanas corresponde igual reação no Direito. O avanço das tecnologias da informação na verdade está provocando o obsolescência de muitos institutos jurídicos e a necessidade de reformulação em tantos outros. A necessidade de ajustamento dos sistemas jurídicos nacionais para enfrentar a realidade do mundo "on line" vem sendo o grande desafio para o direito (FILHO, 2006).

A ciência do direito deve acompanhar os avanços tecnológicos para que não exista margem a dúvidas e incertezas capazes de dificultar a expansão brasileira em campos atualmente fundamentais, como se caracteriza a troca de informações por meio da grande rede. O Direito existe para regulamentar ou organizar os fatos sociais com o fito de garantir a harmonia social, evitando os conflitos entre as pessoas (FONTES, 2009).

Os benefícios da modernidade e da rapidez alcançados com a rede mundial trazem, na mesma proporção, a prática de ilícitos penais que vêm confundindo não só as vítimas como também o responsável pela persecução penal. Tem-se que enfrentar os problemas que decorrem do comércio eletrônico, tais como legislação aplicável nas transações, além das fronteiras territoriais dos países, a proteção do consumidor e garantia de privacidade, o regime jurídico, a validade e a eficácia dos contratos eletrônicos (DAOUN, 1999).

Nos últimos cinco anos, o crescimento exponencial de novos usuários conectados à rede já acarreta questões e controvérsias jurídicas relevantes (FILHO, 1999).

Os vírus representam um dos maiores problemas para usuários de computador. Consistem em pequenos programas criados para causar algum dano ao computador infectado, seja apagando dados, seja capturando informações ou alterando o funcionamento normal da máquina. Esses "programas maliciosos" receberam o nome de vírus porque possuem a característica de se multiplicar facilmente, assim como ocorre com os vírus reais, ou seja, os vírus biológicos. Eles se disseminam ou agem por meio de falhas ou limitações de determinados programas, se espalhando como uma infecção e causando, portanto, danos ao usuário (ALECRIM, 2003).

Diante do exposto, será apresentado o tema proposto para que seja possível a construção de conhecimentos formadores de opinião sobre a forma da atual legislação brasileira que abrange o direito no ciberespaço, ramificada em várias áreas do direito, inclusive internacional, apresentando e discutindo casos e decisões jurídicas.

NOVAS TENDÊNCIAS DOS TRIBUNAIS

Na última década, o Poder Judiciário brasileiro vem se preparando para fazer uma das mais relevantes mudanças da história: implementar o processo eletrônico em todas as instâncias. Para especialistas, a nova modalidade é um caminho sem volta, cujo objetivo é assegurar a celeridade processual tão aclamada por aqueles que buscam a prestação jurisdicional, além de propiciar uma economia processual sem precedentes.

De acordo com a Gazeta do Advogado, recentemente o Superior Tribunal de Justiça (STJ) entrou na Era Virtual. Dos 32 Tribunais de Justiça do país, 29 já aderiram à rede implantada, permitindo o envio de peças à Corte. Os Tribunais de Justiça de São Paulo, Minas Gerais e Rio Grande do Sul, por questões orçamentárias e operacionais, ainda estão de fora.

No entanto, ainda que a era virtual se concretize como novo paradigma do processamento e acompanhamento dos litígios, a modalidade para gerenciar o andamento dos feitos também sofre resistências, não só por conta da preocupação com relação à segurança do sistema, como também pela compreensão daquilo que será o futuro do cotidiano do Judiciário brasileiro. Existem, na atualidade julgados sobre restituição do prazo, conflito entre a informação prestada por meio eletrônico e a informação por meio tradicional, portanto, a relação jurisdicional quanto a confiabilidade:

Processual Civil. Informações. Prazo de Recurso. **Uso do computador. A informação computadorizada há de ser plenamente confiável e não pode ser levada a descrédito porque**

do contrário seria preferível desativar o serviço. Havendo conflito entre a informação eletrônica e a tradicional, restitui-se o prazo recursal. Tribunal de Justiça do Distrito Federal. Agravo de Instrumento; AGI 20010020054563/ DF, Segunda Turma Cível. Relator: Getúlio Moraes Oliveira, 26 de novembro 2001.

Recurso Especial. Divergência. Precedente do STJ. Diário da Justiça. Site na internet. Indicado como paradigma acórdão do próprio STJ, com referência ao Diário da Justiça da União, órgão de publicação oficial, e com a reprodução do inteiro teor divulgado na página que o STJ mantém na Internet, tem-se por formalmente satisfeita a exigência de indicação da fonte do acórdão que serve para caracterizar o dissídio. Superior Tribunal de Justiça. Recurso Especial 2001/0057873-6; RESP 327687/SP. Quarta Turma. Relator: Min. Ruy Rosado de Aguiar, 21 de fevereiro 2002. (grifos nossos)

Processual – Prazo – Justa Causa – **Informações prestadas via Internet – Erro – Justa Causa – Devolução de prazo – CPC, art. 182. Informações prestadas pela rede de computadores operada pelo Poder Judiciário são oficiais e merecem confiança.** Bem por isso, eventual erro nelas cometido constitui "evento imprevisto, alheio à vontade da parte e que a impediu de praticar o ato". Reputa-se, assim, justa causa (CPC, Art. 183, § 1º), fazendo com que o juiz permita a prática do ato, no prazo que assinar (Art. 183, § 2º). Superior Tribunal de Justiça. Recurso Especial 2001/0181499-7; RESP 390561/PR. Primeira Turma. Relator: Min. Humberto Gomes de Barros, 18 de junho 2002. (grifos nossos)

Ações judiciais para resolver problemas causados por malfícios por vírus, um dos primeiros julgados a falar sobre programas maliciosos:

Processo Civil e Civil – Apelo adesivo – Amplitude – Indenização por danos morais – Cadastro negativo do SPC – **Vírus de computador** – Caso fortuito – Inexistência – Conduta previsível e evitável – Majoração da condenação ante as peculiaridades do caso em apreço. O apelo adesivo, a teor do posicionamento do colendo STJ, não está adstrito ao recurso principal quanto às questões devolvidas ao Tribunal, podendo suscitar outras

matérias diversamente daquelas levantadas no apelo principal. **A infecção de computador por vírus, ante o rápido desenvolvimento tecnológico da informática, inclusive com o aparecimento da rede de computadores "internet", é hipótese bastante previsível e também evitável, com os modernos mecanismos de defesa, os quais devem ser empregados por todos aqueles que trabalham com referidas máquinas e com grandes bases de dados, sendo a inexistência de tal proteção, derivando de tal infecção o irregular cadastro negativo do SPC, conduta negligente, afastada, assim, a hipótese de caso fortuito.** Deve-se majorar a verba de ressarcimento, tendo em vista a hipótese em análise, observando o binômio punição/compensação, quando se nota que a atitude ilícita da instituição perdurou por mais de dois anos, com a imputação indevida ao cadastro do autor de mais de 500 protestos. Tribunal de Justiça de Minas Gerais. AC 281.733-6, 3.º C. Civ., Rel. Juiz Dorival Guimarães Pereira, 16 de junho 1999. (grifos nossos)

A possibilidade da remessa dos autos via Internet traz uma série de vantagens e benefícios. Segundo dados do próprio STJ, um processo físico, que pode demorar até oito meses para chegar à Corte, dependendo da região, chegará em poucos minutos. Aqueles que têm certificação eletrônica poderão peticionar e consultar o processo de qualquer lugar e a qualquer momento do dia. O espaço físico para o armazenamento dos inúmeros volumes também poderá ser redesenhado e aproveitado para outras finalidades. Há julgados quanto à legalidade da entrega de peças processuais via meio eletrônico:

Processual civil. Agravo no agravo de instrumento. Petição original. Intempestividade. Petição recursal enviada por correio eletrônico (e-mail). Inadmissibilidade. - O prazo para interposição de agravo contra decisão unipessoal que negou provimento a agravo de instrumento é de 5 (cinco) dias. - **Não se admite a interposição de recurso por meio de correio eletrônico, que não é considerado similar ao fac-símile para efeito de incidência do disposto no art. 1º da Lei n. 9.800/99.** Agravo no agravo de instrumento não conhecido. Superior Tribunal de Justiça. Agravo Regimental no Agravo de Instrumento; AGA 549345/SP. Terceira Turma. Relator: Min. Nancy Andrighi, 01 de abril 2004. (grifos nossos)

Agravo regimental. Recurso especial intempestivo. E-mail. Ausência de perfeita concordância com o original. 1. **Mesmo que se admita o envio da petição de recurso especial por e-mail, não cumpriu a recorrente as normas regulamentadoras de utilização de tal sistema na instância de origem, já que transmitido o recurso após o expediente forense, sendo protocolado no dia subsequente, quando já decorrido o prazo legal.** 2. Descumprido o disposto no artigo 4º, parágrafo único, da Lei nº 9.800/99, invocada pela própria agravante, já que o original não guarda perfeita concordância com o e-mail, distintos os nomes dos advogados constantes das petições. Ressalto que o dispositivo exige perfeita concordância entre as peças e a alteração dos nomes dos advogados responsáveis pela interposição do recurso constitui, inequivocamente, modificação da petição, o que contraria mencionado dispositivo legal. 3. No Estado de São Paulo, o "protocolo integrado" está regulado no artigo 1º, § 3º, do Provimento 462/91, do Conselho Superior da Magistratura, que estabelece que as petições de recursos dirigidas ao Superior Tribunal de Justiça somente poderão ser apresentadas no protocolo do Tribunal *a quo*. Conta-se o prazo, portanto, a partir do momento em que a petição ingressou na Secretaria do Primeiro Tribunal de Alçada Civil do Estado de São Paulo, razão por que o original também teria sido protocolado a destempo, fora do quinquídio previsto no artigo 2º da Lei nº 9.800/99. A série de irregularidades evidenciadas impede afastar o decreto de intempestividade do recurso especial. 4. Agravo regimental desprovido. Superior Tribunal de Justiça. Agravo Regimental no Agravo de Instrumento; AGA 561145/SP. Terceira Turma. Relator: Min. Carlos Alberto Menezes Direito, 06 de maio 2004. (grifos nossos)

Agravo Regimental. Agravo de Instrumento. Intempestividade. Interposição via correio eletrônico. Inadmissibilidade. 1 - **É inadmissível a interposição de recurso por correio eletrônico (e-mail), porquanto não é considerado similar ao fac-símile para efeito de incidência da Lei 9.800/99.** Precedentes. 2 - Agravo regimental improvido. Superior Tribunal de Justiça. Agravo Regimental no Agravo Regimental no Agravo de Instrumento; AGRAGA 504012/RJ. Quarta Turma. Relator: Min. Fernando Gonçalves, 08 de junho 2004. (grifos nossos)

Tamanha é a importância da informática no meio social que já há julgados garantindo alguns fatores como impenhorabilidade do computador por se tratar de bem que garante a residência:

Processual Civil – Embargos à execução – Nulidade do Título executivo inexistente – não caracterizada cobrança de capitalização de juros – Matéria de prova – **Impenhorabilidade dos bens móveis** e utensílios que garantem a residência, incluindo televisores, aparelhos de som, vídeo cassete, microondas e **computador** – precedentes. I - As instâncias ordinárias concluíram que o título executivo é apto a embasar a execução, necessitando para a apuração do quantum devido, apenas, a realização de cálculos aritméticos, o que não o descaracteriza. Deixou consignado, também, a inexistência de capitalização de juros. Matéria de prova e interpretação de contrato insuscetível de reexame nesta instância especial (Súmulas 5 e 7/STJ). II - **A Lei 8009/90 fez impenhoráveis, além do imóvel residencial próprio da entidade familiar, os equipamentos e móveis que o garantem**, excluindo veículos de transporte, objetos de arte e adornos suntuosos. O favor compreende o que usualmente se mantém em uma residência e não apenas o indispensável para fazê-la habitável. Devem, pois, em regra, ser reputados insuscetíveis de penhora aparelhos de televisão e de som, microondas e vídeo-cassete, **bem como o computador, que, hoje em dia, corriqueiro e largamente adquirido como veículo de informação, trabalho, pesquisa e lazer, não pode igualmente ser considerado adorno suntuoso**. III - Recurso conhecido em parte, e nessa parte provido. Superior Tribunal de Justiça. Recurso Especial: RESP 150021/MG, Terceira Turma. Relator: Ministro Waldemar Zveiter, 23 de fevereiro 1999. (grifos nossos)

OS CRIMES DE INFORMÁTICA E SUAS CLASSIFICAÇÕES

Apesar de alguma discrepância doutrinária, são denominados “crimes de informática” as condutas descritas em tipos

penais realizadas por meio de computadores ou voltadas contra computadores, sistemas de informática ou os dados e as informações neles utilizados (armazenados ou processados).

Em face das lacunas oriundas do avanço nas relações sociais, no que tange aos novos crimes virtuais que afloram em nosso meio deverá acatar o princípio da reserva legal, conquanto verificada no artigo 1º do Código Penal Brasileiro e consagrada pelo artigo 5º, XXXIX, da Constituição Federal de 1988: “Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal”. Portanto, precisa-se urgentemente de uma legislação específica quanto aos crimes virtuais, sendo, assim, uma legislação específica para tais casos.

Há ilícitos perfeitamente enquadráveis no Código Penal pátrio e legislação extravagante, quais sejam, aqueles em que a internet, ou outro ambiente eletrônico, informático ou computacional, é somente o seu meio de execução, estando a tipificação perfeita ao ato proferido; são estes os crimes eletrônicos, que recebem também as nomenclaturas de “crimes da Internet”, “crimes digitais”, “crimes cibernéticos” ou “cibercrimes”.

Com propriedade, ao se falar de ilícito eletrônico ou informático, a conduta, mesmo não prevista em lei penal, pode ensejar reparação cível, com multas variáveis de acordo com o resultado obtido, a ser estipulada pelo juiz. Assim, aqueles que se sentirem lesados por atos de terceiros advindos da Internet podem intentar ações judiciais cíveis, em que se requer a devida reparação.

A norma que trata do peculato eletrônico (Lei 9.983/2000), que acresce à parte especial do código penal o art. 313-A:

Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano.

Caso haja alteração de um dado ou informação da administração pública em troca de vantagem indevida, o servidor pode pegar de dois a doze anos de prisão. Esta lei nasceu depois da violação do placar do Plenário do Senado. O Legislativo discutiu e

aprovou rapidamente a legislação depois do episódio. Conseguiu fechar algumas lacunas dentro da administração pública. Nesse ponto houve evolução, mas também é preciso evoluir na esfera privada para que haja uma proteção mínima.

Também constituem exemplos de crimes eletrônicos a exposição em sites de Internet de fotos pornográficas com crianças ou adolescentes – enquadrando-se no art. 241 do Estatuto da Criança e do Adolescente – pedofilia.

APLICABILIDADE JURISDICIONAL

Renato Opice Blum, um dos poucos advogados especializados em Direito Eletrônico no país, Revista Consultor Jurídico, revela que depois das acusações de calúnia e difamação online as principais ações do chamado Direito Eletrônico no Judiciário tratam de invasões de sistemas e vazamento de informações, dois tipos de ilícito sem tipificação específica na legislação penal brasileira.

Se o hacker (nomenclatura utilizada para indivíduos que elaboram e modificam software para invadir sistemas eletrônicos) invadir um sistema privado sem causar prejuízo, não há crime. Trata-se de um fato atípico. No caso de vazamento de dados, a pena é de um ano, não proporcional ao efeito multiplicador quando o vazamento se dá na internet.

Em entrevista à Consultor Jurídico, o advogado diz que o Judiciário brasileiro tem suprido as lacunas da legislação com muita imaginação e sabedoria jurídica. Segundo ele, o Brasil não tem leis como os Estados Unidos, a União Europeia e mesmo os vizinhos Argentina, Chile e Colômbia. Contudo, tem muito mais casos e decisões judiciais. Em suas contas, já chegam a dezesseis mil os julgados em matéria de Direito Eletrônico no país.

Em 2009, os jornalistas Gláucia Milício e Mauricio Cardoso entrevistaram Renato Opice Blum que, ao ser indagado sobre os casos em que não há qualquer previsão legal no direito eletrônico e a importância de legislação específica, respondeu:

Uma pessoa que invade um sistema (que não seja na administração pública) só para olhar e não faz nada, não pode ser condenada. Este é um fato atípico. Mas existe previsão para os casos em que o sujeito entra no sistema e vaza uma informação. A Lei de Propriedade Intelectual (Lei 9.279), em seu artigo 195, trata da situação de vazamento de informação sigilosa a que uma pessoa teve acesso indevido. A pena é de um ano de prisão. No entanto, há uma distorção. Se alguém quebrar o IP [Internet Protocol, o número de identidade de cada computador que acessa a rede] de 20 milhões de pessoas, a pena é a mesma. Ele será condenado a pagar cestas básicas. Esse é um caso em que há previsão parcial. Outra situação preocupante é a pena para a pessoa que colocar vírus em uma urna eletrônica: 5 a 10 anos de prisão. É uma punição extremamente severa, maior que para homicídio. A falta de legislação específica é apenas um dos elementos que fazem com que a Era da Tecnologia possa ser considerada a Era da Insegurança. Um clique em falso e, em minutos, todos os seus vizinhos, colegas de trabalho e amigos com acesso à internet poderão ver, ouvir e comentar o seu segredo. Anos de investimento na segurança do sistema vão por água abaixo depois de alguns esforços de um hacker, que quebra as barreiras e senhas e tem acesso a todas as informações sigilosas da empresa.

Indagado da necessidade de legislação específica para tratar da internet e da realidade brasileira, respondeu:

O Direito Eletrônico merece atenção especial, porque tem muitas peculiaridades. É uma área que já existe na prática, com reflexos importantes para a sociedade como um todo. O Brasil vive uma situação *sui generis*. Não tem legislação específica, mas tem muitos casos interessantes julgados, o que não acontece em países que já têm legislação para a internet. Há alguns anos, crimes que aconteciam lá fora, aqui não existiam. Hoje, também acontecem dentro do Brasil. Os Estados Unidos e a União Europeia têm legislação específica prevendo a coleta, o tratamento, a guarda e o eventual compartilhamento de dados pessoais coletados pelo governo, por empresas e no comércio eletrônico. Sem dúvida, tem de haver leis próprias para isso. Cada vez mais fornecemos os nossos dados e não percebemos os riscos disso. Todo mundo tem cartão de crédito, e-mail,

Twitter, Orkut, Flickr, MSN. Nossos dados estão disponíveis para estas empresas quando fazemos o cadastro. Estamos aceitando perder nossa privacidade sem perceber. Aqui usamos uma legislação genérica. Temos de nos concentrar no detalhamento dessas situações e dar mais atenção aos projetos relacionados com tecnologia, Direito Eletrônico, internet. São questões muito sensíveis [...] no Brasil, apesar de ainda não existir, temos em torno de 17 mil decisões judiciais relacionadas às novas tecnologias, o que despertou o interesse de quem estava no congresso.

Por isso, é necessário criar mecanismos de proteção aos dados pessoais, que integram milhares de cadastros feitos por empresas, sites, cartões de crédito. No Estado de Nevada, nos Estados Unidos, regulamentou-se uma lei em que todos os dados devem ser criptografados assim que coletados. Já que a possibilidade de vazamento não pode ser descartada, que eles se tornem incompreensíveis aos serem repassados inadvertida ou ilegalmente.

No mês de agosto de 1999, a imprensa em geral publicou matérias noticiando misteriosos desaparecimentos de dinheiro de contas bancárias movimentadas pela internet, mas o interessante disso é que os golpistas não roubaram cartões magnéticos e tampouco suas senhas. Em Americana (SP), a Polícia Civil investiga ações de hackers que teriam furtado R\$ 50 mil de duas contas correntes via internet, transferindo o produto do crime para contas distintas em cidades do Nordeste. O registro de ocorrência do "estelionato eletrônico", como foi denominado referido golpe, desperta no meio jurídico extensa discussão quanto à configuração do ocorrido como ilícito penal.

A emblemática é que alguns sustentam que condutas similares às descritas, verificadas as peculiaridades de cada caso, não podem ser enquadradas, por exemplo, como crime de furto, previsto no art. 155 do Código Penal Brasileiro (subtrair para si ou para outrem coisa alheia móvel), vez que emergem dúvidas quanto à conceituação e à aplicabilidade ao caso do objeto penalmente protegido, qual seja, a 'coisa alheia móvel'. Apesar das considerações de que a lei material penal deve ser interpretada restritivamente, proibida a extensão analógica, o revés de tal interpretação, para o direito de informática, ausente qualquer traço análogo, o

dinheiro rapinado de uma conta corrente via internet é furto como outro qualquer, diferenciando-se apenas quanto à maneira e ao agente que pratica o delito (hacker). Portanto o que se difere não é o tipo penal, nem mesmo os conceitos incidentes sobre este: a inovação está no *modus operandi*. O resultado alcançado com a conduta depende da abrangência jurídica atribuída a 'res'.

Em face das lacunas oriundas da modernidade, a reprimenda aos novos crimes virtuais que afloram em nosso meio deverá acatar o princípio da reserva legal, conquanto verificado no artigo 1º do Código Penal Brasileiro e consagrado pelo artigo 5º, XXXIX, da Constituição Federal de 1988: "Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal".

ATUALIZAÇÃO DAS NORMAS JURISDICIONAIS

Foi proposta, em 2000 e 2003, a votação de projetos de lei para regulamentação da internet, mas um bombardeio de críticas provenientes de vários setores do Governo, de parlamentares e de segmentos da sociedade civil organizada provocou o adiamento da votação, na Comissão de Constituição e Justiça do Senado, do substitutivo do Senador Eduardo Azeredo (PSDB-MG) para três projetos de lei que tramitam em conjunto no Congresso Nacional (PLC n. 89, de 2003, do Dep. Luiz Piauhyllino PLS n. 76, de 2000, do Sen. Renan Calheiros e PLS n. 137, de 2000, do Sen. Leomar Quintanilha), que tratam da regulamentação e repressão aos crimes de informática no Brasil.

O ponto polêmico é a obrigação que cria para os provedores de acesso à Internet (ou qualquer rede de computadores), de identificar os usuários de seus serviços, mediante cadastramento prévio. Nos termos exatos do substitutivo, "todo aquele que desejar acessar uma rede de computadores deverá identificar-se e cadastrar-se naquele que torne disponível este acesso". Essa regra vem complementada pelo artigo seguinte de tal legislação proposta, segundo o qual "todo aquele que torna disponível o

acesso a uma rede de computadores somente admitirá como usuário pessoa que for autenticado conforme validação positiva dos dados cadastrais previamente fornecidos pelo contratante de serviços". O parágrafo 1º desse último dispositivo elenca os tipos de dados do usuário que devem fazer parte do cadastro aberto pelo provedor (nome, senha, endereço, número de identidade, número de CPF ou similar). Cria-se, ainda, a obrigação de o provedor manter, pelo prazo de três anos, os dados de conexões e comunicações realizados pelos seus usuários. A Omissão do provedor em identificar seus usuários, mediante cadastro prévio, e conservar os dados de tráfego na Internet é considerada crime, punido com detenção e multa (artigo 154 do Código Penal).

Mostrando que é possível regulamentar atos na internet, Portugal apresenta legislação própria contra crimes informáticos – a chamada Lei de Criminalidade Informática, datada de agosto de 1991 –, estando, dessa forma, muito à frente do Brasil, que tem alguns projetos de lei em trâmite no Congresso e esperando por aprovação quer do Senado, quer da Câmara dos Deputados.

Com esse caos na internet brasileira já se tem reflexos na visão internacional sobre o Brasil, tendo a NASA proibido o acesso de internautas brasileiros a seus links, alegando que o Brasil é o maior celeiro de hackers do mundo.

Tem que haver, na nova legislação, a preocupação com a falta de regimento jurídico, tais como o regime jurídico aplicável ao "correio eletrônico", dando ênfase ao enquadramento penal no mal uso de tal; o regime da venda à distância no que respeita às normas que regem as condições de oferta pública na venda de produtos e serviços aos consumidores, acrescentando ao código comercial novas leis para que não haja brechas jurídicas que ocasionalmente existam; às questões de segurança, de criptografia e de proteção de dados; às violações do direito à imagem e à vida privada; às questões de responsabilidade relativas à difusão de informação ou de imagens, principalmente aquelas que são difamatórias (contra a ordem pública e os bons costumes); ao controle e às sanções de criminalidade específicas em crimes na informática, dando lugar a novos tipos de delito; e, por fim, às questões da propriedade intelectual e, em particular, dos direitos de autor.

CONCLUSÃO

Pela natureza jurídica do direito brasileiro não há mecanismos, sobretudo legais, capazes de outorgar satisfatória proteção nas relações cibernéticas. Em vista do princípio da legalidade, insculpido no artigo 5º, inciso II, da Constituição Federal de 1988, se faz necessário o objeto de criação de norma específica sobre o tema, capaz de definir limites, regular condutas e aplicar penas aos infratores em casos específicos da realidade na internet e nos meios eletrônicos.

Se versa no sentido de que as legislações devem definitivamente acompanhar as irreversíveis mudanças trazidas pela internet, bem como serem flexíveis para englobar as novas relações interpessoais do século XXI, tem-se a lição do eminente jurista Felipe Eluf Creaz:

Sabe-se que, para o acompanhamento de modificações sociais relevantes, a criação doutrinária é de longe mais rápida do que a atividade legislativa, isto acontecendo em todos os países de cultura jurídica fundada no Direito Romano, ou seja, países nos quais o princípio da legalidade é base sobre a qual se manifesta o Direito.

A falta de normatização compromete a própria sobrevivência da Internet, a exigência de identificação, o cadastramento e a autenticação dos usuários dos serviços de conexão à Internet, e mesmo a retenção dos dados de tráfego, podem ser necessárias para garantir a segurança dos serviços de comunicação eletrônica e viabilizar o combate, a investigação e a punição de crimes informáticos.

Não se trata, portanto, de criar mecanismos de “controle de acesso à Internet”, como alguns têm pensado erroneamente, mas de adotar medidas que possam identificar o usuário de um sistema de comunicação específico (que é o serviço de conexão à Internet, fornecido pelos provedores de acesso). É o mesmo processo que se faz, por exemplo, quando uma pessoa se dirige a uma operadora de telefonia e contrata a utilização de um aparelho telefônico (fixo ou celular). Nesse momento da contratação,

a pessoa (usuário) é identificada, apresenta documentos que atestam a sua identidade e é feito um cadastro com os seus dados pessoais. A mesma coisa se pretende seja feita na contratação do serviço de conexão à Internet. Não se estará jamais, com esse tipo de medida, autorizando o próprio provedor ou o estado ou quem quer que seja a monitorar o conteúdo de nossas mensagens eletrônicas, a bloquear o acesso de cidadãos à rede, a censurar o teor de websites ou de qualquer forma de violar o sigilo das comunicações eletrônicas. O que se quer apenas é garantir que, no caso da eventualidade da prática de um crime na Internet, a investigação criminal ou instrução processual possa ser viabilizada mediante requisição judicial (como prevê a Constituição) ao provedor para identificação do usuário suspeito.

Por outro lado, não é sensato o argumento de que a obrigação de identificação prévia do usuário não terá eficácia, já que os criminosos podem acessar a rede mediante provedores situados em outros países nos quais não exista essa obrigação. Deve ser observado que a maioria dos países desenvolvidos já adotou ou está em processo de adotar medida semelhante.

No caso brasileiro, temos verdadeiro vácuo legal, cuja razão de ser somente se pode explicar por meio do normal atraso legislativo frente à morosa velocidade com que se implementaram as transformações sociais advindas com a internet. Ressalva-se então a necessidade de criações legislativas com o fito de regulamentação de áreas tecnológicas impregnadas por relações jurídicas, dentre estas as relações existentes nos sítios de internet, principalmente no que tange à proteção de direitos intelectuais e de valor social do indivíduo.

REFERÊNCIAS

ALECRIM, Emerson. *Vírus de computador: o que são e como agem*. Publicado em 30 jun. 2003. Disponível em: < <http://www.in-fowester.com/virus.php> >. Acesso em: 19 nov. 2011.

BARAN, Paul. O fundador. *Amanhã*, São Paulo, n. 165, p. 30-34, abr. 2001.

CREAZ, Felipe Eluf. *Jurisdiction over cyber space: a new approach for "cybersecurities" transactions*. Disponível em: www.jus.com.br.

DAOUN, Alexandre Jean. Os novos crimes de informática. *Jus Navigandi*, Teresina, ano 4, n. 37, dez. 1999. Disponível em: <<http://jus2.uol.com.br/doutrina/texto.asp?id=1827>>. Acesso em: 19 nov. 2011.

FILHO, Demócrito Reinaldo. *A internet e o obsolescimento das leis*. 2006. Disponível em : <<http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile/5902/5471>>. Acesso em: 12 dez. 2011.

FILHO, Eury Pereira Luna. *Internet no Brasil e o Direito no Ciberespaço*. 1999, p. 1. Disponível em: <<http://www.ibdi.org.br/site/artigos.php?id=189>>. Acesso em: 11 nov. 2011.

FONTES, Felipe Costa. *Natureza e Proteção Jurídica dos Websites no Direito Brasileiro*. 2009, p. 5. Disponível em: <<http://jusvi.com/artigos/557>>. Acesso em: 03 dez. 2011.

FRIEDMAN, Thomas. Manifesto para o mundo veloz. *O Estado de São Paulo*, São Paulo, 23 de maio 1999. Caderno 2, p. D-4 a D-7.

GAZETA DO ADVOGADO. *Processo eletrônico: evolução sem precedentes*. 28 out. 2009. Disponível em: <<http://www.original123.com.br/assessoria/2009/10/28/processo-eletrnico-evoluo-sem-precedentes/>>. Acesso em: 12 dez. 2011.

MARZOCHI, Marcelo de Luca. Globalização, Internet e Direito. *Revista Ciências Humanas*, Taubaté-SP, UNITAU, v. 11, p. 95-101, jul-dez. 2005.

REVISTA CONSULTOR JURÍDICO. *A Era da tecnologia é também a era da insegurança*. Lilian Matsuura - Extraído de: OAB - Bahia -

22 de Março de 2009. Disponível em: <[www.jus.brasil.com.br/busca?q=peculato%20eletrônico&s=noticias peculato eletronico](http://www.jus.brasil.com.br/busca?q=peculato%20eletr%C3%B4nico&s=noticias%20peculato%20eletronico)>. Acesso em: 06 dez. 2011.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. RESP 2001/0181499-7. Disponível em: <[http://www.stj.jus.br/webstj/processo/Justica/detalhe.asp?numreg=200101814997&pv=0 00000000000](http://www.stj.jus.br/webstj/processo/Justica/detalhe.asp?numreg=200101814997&pv=00000000000)>. Acesso em: 06 dez. 2011.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. AGA 504012. Disponível em: <https://ww2.stj.jus.br/processo/ita/listarAcordaos?classe=&num_processo=&dt_publicacao=08/07/2004&num_registro=504012>. Acesso em: 11 dez. 2011.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. AGA 549345. Disponível em: <https://ww2.stj.jus.br/processo/ita/listarAcordaos?classe=&num_processo=&dt_publicacao=01/04/2004&num_registro=549345>. Acesso em: 11 dez. 2011.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. AGA 561145. Disponível em: <[http://www.stj.jus.br/webstj/processo/Justica/detalhe.asp?numreg=200301938064&pv=01 0000000000&tp=51](http://www.stj.jus.br/webstj/processo/Justica/detalhe.asp?numreg=200301938064&pv=01000000000&tp=51)>. Acesso em: 11 dez. 2011.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. RESP 2001/0057873-6. Disponível em: <<http://www.stj.jus.br/webstj/processo/Justica/detalhe.asp?numreg=200400286032&pv=010000000000&tp=51>>. Acesso em: 02 dez. 2011.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. RESP 150021 (1997/0069361-9 - 02/08/1999). Disponível em: <https://ww2.stj.jus.br/processo/ita/listarAcordaos?classe=&num_processo=&dt_publicacao=02/08/1999&num_registro=199700693619>. Acesso em: 22 dez. 2011.

STJ. SUPERIOR TRIBUNAL DE JUSTIÇA. RESP 198370 (1998/0091891-4 - 05/02/2001). Disponível em: <<https://ww2.stj>>.

jus.br/processo/ita/listarAcordaos?classe=30%23|%23RESP&num_processo=198370&dt_publicacao=&num_registro=>. Acesso em: 10 dez. 2011.

TJ/MG. TRIBUNAL DE JUSTIÇA DE MINAS GERAIS. AC 281.733-6, 3.º C. Civ. Disponível em: <http://www.tjmg.jus.br/juridico/sf/proc_nome.jsp?comrCodigo=24&numero=20>. Acesso em: 01 dez. 2011.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS - TJDFT. AGI 20010020054563. Disponível em: <http://tjdf19.tjdft.jus.br/cgi-bin/tjcg1?NXTPGM=plhtml02&ORIGEM=INTER&TitCabec=2%AA+Inst%E2ncia+%3E+Consulta+Processual&CHAVE=20010020054563&SELECAO=1&pesquisa=Enviando...>>. Acesso em: 01 dez. 2011.