O estado da arte da legislação brasileira sobre a criminalidade cibernética

Danielle Novaes de Siqueira Valverde[1], José de Siqueira Silva[2]

[1]Centro de Informática – Universidade Federal de Pernambuco (UFPE)

[2]Departamento de Ciências Jurídicas – Faculdade de Olinda (FOCCA)

dnsv@cin.ufpe.br, jsiqueirajr@yahoo.com.br

Abstract. *This paper presents a study about Brazilian criminal laws and rules on prosecution a computer-related crime, focus on the classification offered by the International Telecommunication Union. The first computer-related conduct to be criminalized in Brazil was the software piracy, in 1987, by the Law nº 7.646. The fight against child pornography gained more effectiveness when the Laws nº 10.764/2003 and n° 11.829/2008 became approved and entered into force. More recently, the Law nº 12.737/2012 criminalized the first purely computer-related offense. The prosecution, however, still lacks rules to provide legal mechanism to both investigators and forensics, in their respective works, to collect evidences that help to prove the crime and to identify the offenders.*

Resumo. *Este artigo apresenta um estudo sobre os tipos penais e as normas processuais penais brasileiras relativas ao crime cibernético, sob o enfoque da classificação oferecida pela International Telecommunication Union. A primeira conduta relacionada à informática a ser criminalmente tipificada foi a pirataria de software, no ano de 1987, por força de Lei nº 7.646. O combate à pornografia infantil ganhou maior efetividade com a edição das Leis nº 10.764, de 2003 e n° 11.829, de 2008. Mais recentemente, a Lei nº 12.737, de 2012 tipificou criminalmente os primeiros delitos puramente informáticos. O processo penal ainda carece de normas que ofereçam à investigação e à perícia forense mecanismos que facilitem a construção probatória e a identificação do autor do delito.*

1. Introdução

Muitas condutas inequivocamente lesivas ao interesse da sociedade em preservar os bens jurídicos mais fundamentais ao equilíbrio e a harmonia da coexistência social, ainda ocorrem atualmente sem perspectiva de prevenção geral ou especial à falta de tipificação como ilicitude na lei penal.

A tecnologia da informação possibilita, nos dias atuais, a perpetração de dano ou de perigo de dano contra o patrimônio moral e material dos indivíduos e, com frequência, da própria coletividade, que, pela sua gravidade teria de ser objeto da incidência penal.

Os fatos, como sempre, anteciparam-se à previsão legal. Qual o legislador que preveria, há trinta anos, os recursos de que hodiernamente dispomos, graças à tecnologia da informação, para gerir nosso patrimônio, movimentar nossas contas bancárias à distância, declarar impostos e fazer pagamentos sem ir a banco ou repartição fazendária, retirar ou depositar dinheiro em caixas eletrônicos, em autoatendimento, com a segurança (relativa, claro) dos cartões magnéticos, que utilizamos correntemente em substituição aos cheques e ao papel moeda em espécie?

As facilidades e o conforto decorrentes da evolução tecnológica trouxeram consigo a fragilidade da insegurança que seu indevido uso acarreta.

Surgiram, assim, as fraudes, as invasões ilegítimas de privacidade, os atentados e danos na esfera do público e do privado.

Crime organizado, espionagem, interferência na segurança estatal e na prestação de serviços públicos, o próprio estado, em nome de princípios justificados sob sua ótica, mas de legitimidade duvidosa ou de ilegitimidade induvidosas, como no caso recente dos Estados Unidos, bisbilhotando a privacidade dos cidadãos em nome do combate ao terrorismo, são algumas das ofensas graves com utilização da satisfação tecnológica.

Muitas dessas condutas de ofensas graves aos direitos fundamentais do ser humano já estão tipificadas como crime na lei penal. Outras estão em estudo para tipificação.

A prova dessas condutas ocorre, ainda, em terreno movediço, à falta de uma legislação processual apropriada, de uma hermenêutica no tocante aos princípios constitucionais garantistas que equilibre mais claramente o predomínio da proporcionalidade dos valores atinentes aos indivíduos e à sociedade. O Supremo Tribunal Federal já decidiu que as garantias constitucionais não podem ser transformadas em escudo protetor da delinquência contra a sociedade.

Em nível internacional, é preciso avançar relativamente à incidência da extraterritorialidade da lei penal, efetivamente, nos casos em que as ofensas resultem de condutas praticadas fora do território nacional ou no (indefinido) espaço virtual cibernético.

O presente artigo visa contribuir com o estudo sobre a legislação penal e processual penal brasileira, concernente à criminalidade cibernética, através de uma breve revisão de literatura, com o objetivo maior de apresentar, num só lugar, o estado da arte em que se encontra o tema no cenário jurídico nacional.

2. O crime cibernético no ordenamento jurídico brasileiro

As expressões crime cibernético, crime digital, crime de informática, ou simplesmente cibercrime, são usadas para se referir a um conjunto de condutas delituosas que, de certa forma, estão relacionadas à tecnologia da informação. Para Ferreira (2005), trata-se de toda

ação típica, antijurídica e culpável cometida contra ou pela utilização do processamento automático de dados ou sua transmissão.

Atendendo a fins meramente didáticos e para melhor estruturar a exposição do objeto deste artigo, tomar-se-á por empréstimo a classificação proposta pela *International Telecommunication Union* [ITU 2012], que organiza as ofensas em:

a) relacionadas a direitos autorais;
b) relacionadas a conteúdos;
c) contra confidencialidade, integridade e disponibilidade de sistemas computacionais;
d) relacionadas a computadores.

2.1 Ofensas relacionadas a direitos autorais

A história da tipificação dos crimes cibernéticos no Brasil tem início com matéria relacionada à proteção da propriedade intelectual sobre programas de computador. Em dezembro de 1987, o Congresso Nacional aprovou a Lei nº 7.646, criminalizando as condutas de violação de direitos do autor (art. 35) e a importação, exposição, manutenção em depósito, para fins comerciais, de programas de computador, de origem externa, não cadastrados (art. 36). Essa lei foi revogada pela de nº 9.609, em 1998, que manteve o primeiro tipo penal (agora no art. 12) com a mesma pena, e aboliu o segundo.

2.2 Ofensas relacionadas a conteúdos

Nessa categoria, agrupam-se os ilícitos relacionados a material erótico, pornografia, pornografia infantil, racismo, discurso de ódio, incitação à violência, ofensas religiosas, jogos *online* ilegais, difamação ou falsa informação, *spam* e outras formas de conteúdo ilegal.

2.2.1 Pornografia infantil

O crime de pornografia infantil é disciplinado pelo Estatuto da Criança e do Adolescente (Lei nº 8.069, de 1990), nos arts. 240, 241 e 241-A a 241-E.

A primeira alteração no texto original do Estatuto, nas questões referentes à pornografia infantil, ocorreu em 2003, por força da Lei nº 10.764, de 2003, que deu outro teor aos termos dos arts. 240 e 241. No entanto, as mudanças mais significativas foram trazidas pela Lei nº 11.829, de 2008, que além de alterar, mais uma vez, os citados artigos, acrescentou novos tipos penais (241-A a 241-E), com a finalidade, segundo Nucci (2009), de acompanhar os passos da modernidade e da tecnologia, cada vez mais disseminada entre os jovens, com livre e fácil acesso aos mais variados conteúdos.

Nesses termos, a referida lei ampliou a possibilidade de punição, agravou a pena, bem como buscou penalizar a conduta de manter fotos e outros registros de menores de 18 (dezoito) anos envoltos em cenas pornográficas ou de sexo explícito. Passou a punir também o comportamento daqueles que trocam, transmitem, disponibilizam publicam ou divulgam, por qualquer meio, qualquer registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. Visou ainda punir montagens e edições de filmes, em geral, contendo imagens sexuais de jovens. Quem simula sexo explícito ou pornografia envolvendo crianças e adolescentes, por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual também estará sujeito aos rigores da lei. Finalmente, o Estatuto ampliou a criminalização dos agentes que buscam jovens em programas de comunicação, com o fim de praticar ato libidinoso, mormente em sites específicos da internet, como salas de bate-papo, redes sociais e outros sistemas de interações.

2.2.2 Atuação de grupos racistas e outras organizações criminosas

Os crimes referidos neste item constam originalmente da Lei n° 7.716, de 1989, que recebeu alterações sucessivas pelas Leis nº 8.081, de 1990; Lei nº 8.882, de 1994; Lei nº 9.459, de 1997; Lei nº 10.741, de 2003; Lei nº 12.735, de 2012. O Código Penal tipifica, no §3º do art. 140, a injúria racial contra uma ou várias pessoas, por força de inclusão da Lei nº 9.459, de 1997 e posterior alteração provocada pelo Estatuto do Idoso (Lei nº 10.741, de 2003).

As manifestações de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional cometidas por meio da internet tendem a repercutir mais intensamente do que as ofensas proferidas verbalmente, em razão da abrangência da grande rede. Em geral, esse crime envolve a veiculação de imagens, comentários, vídeos ou outras formas de manifestações discriminatórias.

As condutas de praticar, induzir ou incitar a discriminação de raça, cor, etnia, religião ou procedência nacional (art. 20 da Lei nº 7.716, de 1989) tornam-se mais gravosas quando cometidas por intermédio dos meios de comunicação social ou publicação de qualquer natureza (§ 2º do art. 20 da Lei nº 7.716, de 1989), podendo, nesses casos, o juiz determinar, ouvido o Ministério Público ou a pedido deste, sob pena de desobediência, a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio e a interdição das respectivas mensagens ou páginas de informações na internet.

2.2.3 *Cyberbullying*

O *bullying* compreende atitudes agressivas, intencionais e repetidas, que ocorrem sem motivação evidente, adotadas por um ou mais estudantes contra outro(s), causando dor e angústia, e executadas dentro de uma relação desigual de poder [Nogueira 2009]. Trata-se de palavra originada da língua inglesa que significa valentão e caracteriza-se pela prática de agressões físicas ou psicológicas de forma habitual, traumática e prejudicial às vítimas [Wendt e Jorge 2012].

Ciberbullying é a expressão utilizada quando o *bullying* ocorre por meio da internet. No Brasil, não é crime, mas as condutas que o constituem, via de regra, são enquadráveis penalmente ou constituem ato infracional, quando quem o pratica sujeita-se às normas do Estatuto da Criança e do Adolescente.

Assim, dentre as principais práticas, destacam-se a calúnia, difamação, injúria, ameaça, constrangimento ilegal, falsa identidade, molestar ou perturbar a tranquilidade. Neste último caso, não há crime, e sim uma contravenção penal que permite punir aquele que passa a molestar ou perturbar a tranquilidade alheia por acinte ou motivo reprovável.

A prática de *bullying* constitui dano moral, passível de indenização à vítima, conforme dispõe o inc. X do art. 5º da Constituição Federal.

Iniciativas de prevenção à prática de *bullying* no ambiente escolar são encontradas em alguns estados brasileiros. Em Pernambuco, por exemplo, a Lei Estadual nº 13.995, de 2009, publicada no Diário Oficial do Estado de 23 de dezembro de 2009, dispõe sobre a inclusão de medidas de conscientização, prevenção, diagnose e combate ao *bullying* escolar no projeto político pedagógico das escolas públicas e privadas de educação básica do estado.

2.3 Ofensas contra confidencialidade, integridade e disponibilidade de sistemas computacionais

Essa categoria descreve as ações que atentam contra a confidencialidade, a integridade e a disponibilidade dos sistemas computacionais. A invasão de sistemas, espionagem eletrônica,

interceptação ilegal, ataques a sistemas de bancos de dados, a interferência em sistemas computacionais são alguns exemplos de ofensas subsumidas a essa categoria.

2.3.1 Interceptação telemática ilegal

A interceptação telemática, como forma legal de investigar delitos cibernéticos, pode extrapolar os limites da licitude e ser considerada crime, nos termos do art. 10 da Lei nº 9.296, de 1996. De acordo com esse dispositivo, constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

2.3.2 Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

A Lei nº 12.737, de 2012 criminalizou a interrupção e perturbações a serviço telemático ou de informação de utilidade pública, com a inclusão dos § 1º e 2º no art. 266 do Código Penal. Esse crime situa-se no Título VIII do Código Penal, Capítulo II, atentando contra a incolumidade pública no tocante à segurança dos meios de comunicação, classificando-se, no entender de Capez (2010), como crime de perigo comum, sendo imprescindível que as condutas típicas causem perigo a todo o sistema referido. Portanto, se apenas a comunicação ou conversação entre duas pessoas for interrompida o delito será do art. 151, §1º, III do Código Penal.

Tutela-se a incolumidade pública no particular aspecto da regularidade do funcionamento dos serviços telegráficos, telefônicos, informático, telemático ou de informação de utilidade pública. Protege-se, portanto a normalidade dos serviços de telecomunicações.

2.3.3 Invasão de dispositivo informático

O tipo penal de invasão de dispositivo informático alheio, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita, foi inserido no ordenamento jurídico brasileiro por força da Lei nº 12.737, de 2012.

É considerado dispositivo informático o computador pessoal, o computador em formato de prancheta (*tablet*), o telefone celular (em especial os que possuem acesso à internet), dispositivos de armazenamento externo, como CD-ROM, DVD e outras mídias assemelhadas, conforme expressa o legislador na justificativa apresentada no projeto de lei nº 2.793, de 2011, que originou a citada lei. É condição essencial que o dispositivo informático seja de pessoa distinta do autor do delito, sob pena de tornar atípica a conduta.

A violação indevida de mecanismo de segurança é elemento normativo da antijuridicidade e pressupõe a obrigatoriedade da vítima em zelar pela segurança dos seus dados, indicativo de sua pretensão de privacidade.

O elemento subjetivo do tipo é o dolo, representado pela vontade livre e consciente do autor em obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

O referido tipo penal apresenta também elemento subjetivo do injusto ou dolo específico, caracterizado pelo intuito do autor de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

A produção, oferta, venda ou difusão de vírus de computador ou dispositivo com o intuito de permitir a invasão do dispositivo informático, seja para obter, adulterar ou destruir dados ou informações seja para instalar vulnerabilidades para obter vantagem ilícita, sujeitará o autor a mesma pena do *caput* do art. 154-A, constituindo crime assemelhado. Em se tratando do elemento subjetivo que expressa o fim de instalar vulnerabilidades para obter vantagem ilícita, é necessário que o autor tenha consciência de que obtém uma vantagem indevida, visto que, se for devida, legal ou justa, não se cuidará o tipo penal.

Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido, a pena será de reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, caso não configure crime mais grave.

A pena será majorada se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos ou se o crime for praticado contra o Presidente da República, governadores e prefeitos; Presidente do Supremo Tribunal Federal; Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Trata-se de crime formal, pois, apesar de descrever um resultado, este não precisa verificar-se para ocorrer a consumação. Basta a ação do autor e a vontade de concretizá-lo, configuradora do dano pessoal.

2.3.4 Alteração de sistemas de informações

No ano 2000, modificações no Código Penal trazidas pela lei n° 9.983 fizeram inserir novos tipos penais relacionados ao uso indevido de sistemas de informações, como o peculato eletrônico (art. 313-A) e a modificação ou alteração não autorizada de sistemas de informações (art. 313-B), além de alterar os termos dos crimes de violação de sigilo funcional (§1° do art. 325) e de divulgação de segredo (§1°-A do art. 153).

Essas alterações foram motivadas pela necessidade de coibir fraudes na previdência social, que, em diversos casos, eram perpetradas pelo uso indevido da tecnologia da informação.

O art. 313-A tipifica penalmente a conduta de inserir ou facilitar 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.

O art. 313-B criminalizou as condutas de modificar ou alterar sistema de informações ou programa de computador, sem autorização ou solicitação de autoridade competente. Embora aparentemente sejam consideradas palavras sinônimas, Prado (2002) afirma que, no sentido do texto, a ação de modificar expressa uma transformação radical no programa ou no sistema de informações, enquanto na alteração, embora também se concretize uma mudança no programa, ela não chega a desnaturá-lo totalmente.

O objeto material refere-se a sistema de informações ou programa de informática utilizados pela administração pública, ambos elementos normativos de valoração extrajurídica.

Os dois tipos penais descritos acima são classificados como crimes próprios, uma vez que o sujeito ativo do delito é obrigatoriamente servidor público ou equiparado vinculado ao ente público, vilipendiado com a ação delituosa, sendo admissível a prática do crime através

do concurso com particular, desde que este conheça a qualidade de servidor público exigida do agente.

Ao crime de violação de sigilo funcional acrescentou-se o §1º ao art. 325, que criminalizou a conduta do funcionário que se utiliza indevidamente do acesso restrito aos sistemas, bem como permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública.

Segredo funcional, elemento normativo do tipo, é tudo o que não é nem pode ser conhecido senão por determinadas pessoas ou por certa categoria de pessoas, em razão de ofício [Prado 2002].

O bem jurídico a ser protegido é o normal funcionamento da administração pública, resguardando o seu interesse de que não sejam divulgados determinados segredos de relevância para a perfeita atuação funcional do estado e demais entes descritos no art. 327 §1º do Código Penal, protegendo-se ainda o interesse próprio particular, que poderia ser lesado com a devida publicidade de dados sigilosos que estão ao alcance restrito do ente público.

Na figura penal de divulgação de segredo, divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública não é pré-requisito para configurar o tipo ser o autor do delito funcionário público, como nos tipos descritos anteriormente. A infração penal é de médio potencial ofensivo, já que, embora a pena máxima cominada ultrapasse dois anos de detenção, a mínima não é superior a um ano.

2.3.5 Espionagem

Tipos penais relacionados à espionagem são descrito no ordenamento jurídico pátrio pelo Código Penal Militar (Decreto-Lei nº 1.001, de 1969) e pela Lei de Segurança Nacional (Lei nº 7.170, de 1983). No contexto desse artigo, várias condutas descritas nesses dispositivos legais são facilitadas pelo uso da tecnologia da informação, em especial da internet.

2.4. Ofensas relacionadas a computadores

Nessa categoria estão inseridas as ofensas que necessariamente são cometidas por meio de sistemas computacionais, tais como fraude eletrônica, *phishing*, falsificação eletrônica .

2.4.1 O estelionato e as fraudes eletrônicas em sistemas bancários

A figura do estelionato eletrônico não é encontrada no ordenamento jurídico brasileiro, sendo uma denominação utilizada por alguns autores, como Plantullo (2010), para referenciar fraudes cometidas por meio de sistemas computacionais.

O crime de estelionato é tipificado pelo art. 171 do Código Penal (1940), e consiste em obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.

Segundo Bitencourt (2005), a característica fundamental do estelionato é a fraude, utilizada pelo agente para induzir ou manter a vítima em erro, com a finalidade de obter vantagem patrimonial ilícita.

Para configurar o crime, é indispensável que a vantagem seja ilícita, decorra de erro produzido pelo agente, ou seja, que aquela seja consequência deste. Não basta a existência do erro decorrente da fraude, sendo necessário que da ação resulte vantagem ilícita e prejuízo

patrimonial. Sendo assim, são requisitos apontados pelo autor para a configuração do crime de estelionato: o emprego de artifício, ardil ou qualquer outro meio fraudulento; induzimento ou manutenção da vítima em erro; obtenção de vantagem patrimonial ilícita, em prejuízo alheio.

O projeto de lei nº 5.485, de 2013, que tramita no Congresso Nacional, propõe a tipificação criminal do estelionato eletrônico, configurado pelo envio mensagens digitais de qualquer espécie, fazendo-se passar por empresas, instituições ou pessoas a fim de induzir outrem a revelar informações pessoais, de identidade, ou senhas de acesso.

A rigor, o que está sendo proposto é a criminalização do *phishing*, punindo com a mesma pena do estelionato o simples envio de mensagens que buscam atingir vítimas que forneçam seus dados pessoais a pessoas mal-intencionadas. Em se consumando a obtenção da vantagem indevida, em prejuízo alheio, ou seja, se o falso se exaure no estelionato, sem mais potencialidade lesiva, é por este absorvido, conforme dispõe a Súmula 17 do Superior Tribunal de Justiça [STJ 1990].

As fraudes eletrônicas em sistemas bancários podem ocorrer com utilização de cartão de débito, cartão de crédito, via acesso à conta bancária pela internet (*home banking*) e centrais de atendimento (*call centers*).

As fraudes via *home banking*, em geral, procedem mediante a disseminação de programas maliciosos que capturam informações confidenciais do usuário, remetendo-as ao criminoso cibernético através da própria internet.

Nesses casos, é importante identificar que programa malicioso foi utilizado ou que outra estratégia de ataque foi empregada, de forma a estabelecer a melhor forma de abordar o problema, planejando adequadamente os procedimentos investigativos [Wendt and Jorge 2012].

Por fim, a Lei nº 12.737, de 2012 equiparou a documento particular o cartão de crédito ou débito, no intuito de contribuir com o combater a fraude bancária.

3. Os instrumentos legais para a investigação dos crimes cibernéticos

3.1 A interceptação telemática

A inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas é protegida pela Constituição Federal, de 1988, através do inc. XII do seu art. 5º, cuja parte final é disciplinada por meio da Lei nº 9.296, de 1996, que trata a interceptação de comunicações telefônicas e do fluxo de comunicações em sistemas de informática e telemática, de qualquer natureza, para prova em investigação criminal e em instrução processual penal.

Em sentido estrito, interceptar significa interromper, cortar ou impedir. No entanto, a interceptação tratada na lei em comento tem o significado de interferência, com o fito de colheita de informes [Nucci 2009].

É vedada a interceptação quando não houver indícios razoáveis da autoria ou participação em infração penal; quando a prova puder ser feita por outros meios disponíveis; quando o fato investigado constituir infração penal punida, no máximo, com pena de detenção.

Diferentemente da interceptação de comunicações telefônicas, que é regida pela mesma lei e já se encontra sedimentada, a interceptação telemática apresenta uma série de desafios técnicos e jurídicos.

Enquanto a utilização dos serviços de telefonia apresenta bem definida as obrigações inerentes às concessionárias e aos usuários, na internet essa relação inexiste, pois se trata de tecnologia cuja exploração não é disciplinada ou normatizada pelo estado brasileiro.

Na seara jurídica, a constitucionalidade dos dispositivos legais atinentes à interceptação do fluxo de comunicações em sistemas de informática e telemática foi questionada por meio da Ação Direta de Inconstitucionalidade nº 1.488 [STF 2001], proposta pela Associação dos Delegados de Polícia do Brasil. Integra o pleito um pedido de concessão de medida cautelar liminar, visando a suspensão da eficácia da norma questionada.

Alega a requerente que o parágrafo único do art. 1º e o art. 10 da referida lei atentam contra os incisos XII e LVI do art. 5º da Constituição Federal de 1988, ao instituir a possibilidade de interceptação do fluxo das comunicações em sistemas de informática e telemática.

Os argumentos apresentados margeiam o texto do dispositivo constitucional que prevê a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (art. 5º inc. XII da Constituição Federal de 1988).

Segundo a interpretação dos requerentes, apenas as comunicações telefônicas seriam passíveis de serem violadas, desde que obedecidas as formalidades legais.

Como consequência direta dessa impossibilidade, os laudos de degravação das comunicações telemáticas seriam inadmissíveis como prova, por afrontar o inc. LVI do art. 5º da Constituição Federal ("são inadmissíveis, no processo, as provas obtidas por meios ilícitos").

O Supremo Tribunal Federal conheceu a ação direta em face da relevância de seus fundamentos, mas indeferiu o pedido de liminar por considerar a inocorrência de *periculum in mora* a justificar a suspensão da vigência do dispositivo impugnado.

No mérito, a ação não foi analisada, pois teve o seu seguimento negado pelo relator, no ano de 2001, por ilegitimidade ativa ad causam da requerente.

A despeito do não pronunciamento formal do Supremo Tribunal Federal, o Superior Tribunal de Justiça vem demonstrando reconhecimento à constitucionalidade do parágrafo único do art. 1º da Lei nº 9.296, de 2006, amparando suas decisões, a partir do Habeas Corpus nº 15.026/SC [STJ 2002], no qual reconhece que "a legislação integrativa do *canon* constitucional autoriza, em sede de persecução criminal, mediante autorização judicial, [...] a interceptação do fluxo de comunicações em sistemas de informática e telemática".

Após esse julgado, outros se sucederam no mesmo sentido, como o Acórdão no Habeas Corpus nº 101.165/PR [STJ 2008], que reconheceu a legalidade na interceptação telemática quando ela é, aliada a presença de indícios de autoria, devido à peculiaridade do *modus operandi* do delito, o único meio de prova a esclarecer os fatos.

Outra norma atinente à interceptação telefônica e telemática é a Resolução nº 59, editada em 2008 pelo Conselho Nacional de Justiça [Poder Judiciário 2008], com o objetivo de disciplinar e uniformizar as rotinas visando ao aperfeiçoamento do procedimento de interceptação de comunicações telefônicas e de sistemas de informática e telemática nos órgãos jurisdicionais do Poder Judiciário, a que se refere a Lei nº 9.296, de 1996. Tal normativa trata aspectos relacionados à movimentação de documentos para garantir o sigilo das medidas judiciais e estabelecimento de controle a fim de coibir abusos no uso desse meio de prova.

3.2 A quebra do sigilo telemático

Uma inovação trazida pela Lei nº 12.683, de 2012 foi a possibilidade de o Ministério Público e a Polícia Judiciária requisitarem diretamente, sem intermediação judicial, os dados cadastrais de investigados, mantidos em bases da Justiça Eleitoral, das companhias telefônicas, das instituições financeiras, dos provedores de internet e das administradoras de cartões de crédito

A norma harmoniza-se com a Constituição Federal de 1988, pois a requisição direta de dados cadastrais de telefonia e telemática não se confunde com a interceptação de comunicações telefônicas, medida de investigação criminal regulada na Lei nº 9.296, de 1996, para a qual o artigo 5º, inciso XII da Constituição Federal de 1988 exige autorização judicial. Tampouco se confunde com a quebra de sigilo bancário, prevista na Lei Complementar nº 105, de 2001, segredo cujo afastamento revela a vida financeira do investigado e pode sugerir outros elementos de sua personalidade.

Os dados cadastrais não estão protegidos pelo direito à intimidade (art. 5º, X, Constituição Federal), conforme demonstram decisões exaradas em diversos julgados do Superior Tribunal de Justiça, como na Carta Rogatória nº 000297 [STJ 2006], no Habeas Corpus nº 83.338/DF [STJ 2009], nos Embargos de Declaração em Recurso no Mandado de Segurança nº 25.375/PA [STJ 2008].

Sendo assim, doravante os Ministérios Públicos, a Polícia Judiciária (a Federal e as Civis dos Estados) e a Polícia Militar (quando da realização de Inquéritos Policiais Militares) poderão, com base no art. 17-B da Lei nº 9.613, de 1998, expedir requisições diretamente às pessoas jurídicas detentoras dos dados cadastrais, ordens estas que deverão ser cumpridas sob pena de desobediência (art. 330 do Código Penal).

O abuso dessa atribuição pelo membro do Ministério Público ou pela autoridade policial pode caracterizar os delitos de prevaricação (art. 319 do Código Penal), ou violação de sigilo funcional (art. 325, §1º, Código Penal), e ainda ato de improbidade administrativa e falta disciplinar a ser apurada.

4. Aspectos relacionados aos provedores de internet

4.1 A responsabilidade penal dos provedores de internet

Atualmente, inexiste lei específica estabelecendo a responsabilidade criminal dos provedores de acesso e dos provedores de conteúdo e de armazenamento.

A complexidade do tema está relacionada à dificuldade do provedor de acesso e de conteúdo de identificar a natureza do conteúdo que trafega e que é armazenado, respectivamente, em seus servidores. Caso o provedor venha a ter ciência comprovada do conteúdo prejudicial de um *site* por ele hospedado, terá que imediatamente suspender a publicação daquela página, para não vir a ser responsabilizado civilmente ou até criminalmente. Assim está previsto no Estatuto da Criança e do Adolescente (Lei nº 8.609, de 13 de julho de 1990), por força das alterações introduzidas pela Lei nº 11.829, de 2008.

De acordo com o § 2ª do art. 241-A do referido Estatuto, as condutas tipificadas nos incisos I e II do § 1º do art. 241-A são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o *caput* desse artigo.

Os Estados Unidos tratam de forma diferenciada os provedores de acesso e os de serviços de armazenamento de conteúdo. Os primeiros não são responsabilizados por

conteúdo ilegal transmitido em suas redes, desde que mantenham política de cancelar o acesso de usuários que reincidam em conduta proscrita em lei. Os provedores de serviços relacionados à armazenamento de conteúdo, por sua vez, são obrigados a remover material divulgado na internet por seus clientes, mediante requisição do detentor de direito autoral do mesmo. Caso o usuário comprove que não está infringindo a lei de direitos autorais, ou caso o detentor do direito não leve adiante processo judicial sobre o caso, o serviço de armazenamento deve restaurar o conteúdo, mediante pedido do usuário, decorrido o prazo de 10 a 14 dias. O anonimato, entendido como a proteção da fonte de certa manifestação ou expressão on-line, não se aplica ao usuário da internet, para fins de execução e investigação legal. Ademais, o ordenamento jurídico do país não veda o monitoramento de comunicação na internet [Vieira 2010].

4.2 A obrigatoriedade de guarda dos registros de acesso à internet pelos provedores de acesso

A obrigatoriedade da guarda dos registros (*logs*) de acesso à internet não é procedimento regulamentado por qualquer lei ou norma de abrangência nacional, restringindo-se a iniciativas locais de governos estaduais e municipais, o que enseja limitação na investigação criminal.

Em nível estadual, exigem dos provedores internet a guarda dos *logs* ou dos estabelecimento que disponibilizam acesso oneroso ou gratuito à grande rede o cadastro dos usuários: Alagoas (Lei nº 6.891, de 2007), Amapá (Lei nº 1.047, de 2006), Amazonas (Lei nº 3.173, de 2007 e Lei nº. 3.351, de 2008), Bahia (Lei nº 11.608, de 2009), Espírito Santo (Lei nº 8.777, de 2007), Paraíba (Lei nº 8.134, de 2006), Paraná (Lei n.º 16.241, de 2009), Pernambuco (Lei nº 14.001, de 2009), Piauí (Lei nº 5.747, de 2008), Rio de Janeiro (Lei nº5.132, de 2007), Rio Grande do Sul (Lei nº 12.698, de 2007), Santa Catarina (Lei nº 14.890, de 2009), São Paulo (Lei nº 12.228, de 2006).

Em nível distrital e municipal, destacam-se iniciativas como a do Distrito Federal, com a Lei Distrital nº 3.437, de 2004 e a do Município do Recife, com a Lei Municipal nº 17.572, de 2009.

Criar obrigação para os provedores de acesso registrarem *logs* não exaure os recursos necessários a identificar o autor de um delito cometido por meio da internet, mas pode contribuir sobremaneira na identificação dos mesmos.

5. A cooperação internacional

5.1 Abrangência

Grande parte das normas internacionais existentes teve origem na conclusão de tratados e convenções internacionais entre os estados. Desde a antiguidade, os tratados têm servido aos mais diferentes fins, entre os quais se destacam a constituição de alianças militares de caráter defensivo, celebração de paz, o estabelecimento de linhas fronteiriças entre os países, a intensificação do intercâmbio econômico e cultural [Amaral Junior 2011].

Segundo o art. 38 do Estatuto da Corte Internacional de Justiça, promulgada pelo Brasil, por meio do Decreto nº 19.841, de 1945, são fontes do direito internacional as convenções internacionais; o costume internacional; os princípios gerais do direito, reconhecidos pelas nações civilizadas; sob ressalva da disposição do art. 59, as decisões judiciárias e a doutrina dos juristas mais qualificadas das diferentes nações, como meio auxiliar para a determinação das regras do direito.

Tratado é o acordo formal, concluído entre sujeitos de direito internacional público e destinado a produzir efeitos jurídicos. São variantes terminológicas de tratado concebíveis em português: acordo, ajuste, arranjo, ato, ata, código, corte, estatuto, declaração, memorando, pacto, protocolo, regulamento [Rezek 2010]. Para o crime cibernético, registre-se a Convenção sobre o Cibercrime [Council of Europe 2001], assinada 23 de novembro de 2001, na cidade de Budapeste/Hungria, ainda não ratificada pelo Brasil.

Em virtude do fenômeno da globalização, crimes eminentemente internos, nos quais o princípio da territorialidade aplica-se na sua integralidade, podem necessitar, para sua apuração, de adoção de mecanismos de cooperação internacional.

Segundo Weber (2011), a cooperação penal internacional engloba o conjunto de mecanismos que propicia a interação dos estados na efetivação da justiça penal, em atenção a procedimentos ou processos específicos. Nesse contexto, não se confunde com a cooperação internacional administrativa, que é destinada ao aprimoramento tecnológico, à troca de informação, estratégias de atuação entre os órgãos envolvidos.

A discussão sobre os fundamentos da cooperação penal internacional dissocia-se, cada vez mais, do paradigma da territorialidade ou extraterritorialidade na punição de delitos. A regra geral é a territorialidade, podendo haver a persecução de crimes cometidos fora do território nacional em virtude da nacionalidade do autor (princípio da personalidade ativa), nacionalidade da vítima (princípio da personalidade passiva), bem jurídico afetado (princípio da defesa ou real), local onde foi praticado o ilícito (princípio da representação) e características do delito, hábil a afetar ou não valores da comunidade internacional (princípio da justiça universal). Havendo elementos de extraneidade (como fases do seu cometimento no exterior, vítima ou autor estrangeiros) a necessidade de cooperação internacional afigura-se em regra mais evidente.

Weber (2011) entende que a cooperação penal internacional fundamenta-se, no estado brasileiro, pela necessidade de cooperação entre os povos para o progresso da humanidade, pelo respeito aos direitos humanos, a serem protegidos via aparato penal, e pela observância do devido processo internacional.

5.2 Procedimentos operacionais

No caso de cooperação jurídica internacional em matéria penal, as solicitações de assistência devem ser intermediadas pelo Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional, vinculado à Secretaria Nacional de Justiça do Ministério da Justiça, com sede no Distrito Federal.

A Assistência Judiciária em Matéria Penal entre o Brasil e os Estados Unidos da América é disciplinada por meio do Decreto nº 3.810, de 2001. Com o Japão, fundamenta-se por meio da Portaria Interministerial n° 26, de 14 de agosto de 1990, Ministério das Relações Exteriores e do Ministério da Justiça.

Com o Reino Unido, as bases legais da cooperação internacional são a Convenção das Nações Unidas contra o Crime Organizado Transnacional (Convenção de Palermo), promulgada por meio do Decreto nº 5.015, de 2004; Convenção das Nações Unidas contra a corrupção (Convenção de Méridas), promulgada pelo Decreto nº 5.687, de 2006; Convenção contra o Tráfico Ilícito de Entorpecentes e Substâncias Psicotrópicas (Convenção de Viena), promulgada pelo Decreto n° 154, de 1991. Refere-se ainda ao Memorando de Entendimento entre o Governo da República Federativa do Brasil e o Governo do Reino Unido da Grã-Bretanha e Irlanda do Norte para Aprofundar a Cooperação nas Áreas de Segurança e Combate ao Crime [Brasil 2011], com o objetivo de desenvolver e fortalecer a cooperação em diversas áreas, inclusive relacionada a crimes cibernéticos, conforme letra b do item 1.1.

Com a Alemanha, as bases legais da cooperação são a Convenção das Nações Unidas contra o Crime Organizado Transnacional (Convenção de Palermo) e a convenção contra o tráfico ilícito de entorpecentes e substâncias psicotrópicas.

Com a China, destaca-se o Acordo de Cooperação Internacional para o Combate à Criminalidade Organizada Transnacional e Outras Modalidades Delituosas [Brasil 2004], cujo escopo inclui o crime cibernético (letra k do Artigo 1).

6. Conclusão

É relativamente nova a problemática da criminalidade cibernética com os graves danos e riscos de dano que acarreta, exigindo que o estado tutele urgentemente os bens jurídicos afetados por lesões efetivas ou perigo delas. O desafio é compreender como as condutas danosas ou potencialmente danosas lesionam o interesse das pessoas e da coletividade e aparelhar os órgãos investigativos, entre eles a Polícia Judiciária e o Ministério Público, e o estado-juiz, com a legislação apropriada a coibir o uso desvirtuado e lesivo da internet e das tecnologias correlatas, com a complementação das normas penais e processuais penais já existentes e a dotação dos recursos tecnológicos para comprovar a ilicitude dos comportamentos, sua autoria e participação, com observância do devido processo legal e do respeito às demais garantias dos direitos fundamentais não apenas das pessoas ofendidas, mas daquelas que são imputadas das práticas desses tipos de ilicitude penal.

Referências

Amaral Junior, A (2011) “Curso de Direito Internacional Público”, Atlas, São Paulo.

Bitencourt, Cezar Roberto (2005) “Tratado de Direito Penal”, Saraiva, São Paulo.

Brasil (2004) “Acordo de Cooperação Entre o Governo da República Federativa do Brasil e o Governo da República Popular da China para o Combate à Criminalidade Organizada Transnacional e Outras Modalidades Delituosas”, http://dai-mre.serpro.gov.br/atos-internacionais/bilaterais/2004/b_109.

Brasil (2011) “Memorando de Entendimento entre o Governo da República Federativa do Brasil e o Governo do Reino Unido da Grã-Bretanha e Irlanda do Norte para Aprofundar a Cooperação nas Áreas de Segurança e Combate ao Crime”, http://dai-mre.serpro.gov.br/atos-internacionais/bilaterais/2011/memorando-de-entendimento-entre-o-governo-da-republica-federativa-do-brasil-e-o-governo-do-reino-unido-da-gra-bretanha-e-irlanda-do-norte-para-aprofundar-a-cooperacao-nas-areas-de-seguranca-e-combate-ao-crime.

Capez, Fernando (2010) “Curso de Direito Penal: Parte Especial”, Saraiva, São Paulo.

Council of Europe (2001) “Convenção de Budapeste sobre o Cibercrime”. http://dre.pt/pdf1sdip/2009/09/17900/ 0635406378.pdf.

Ferreira, Ivette Senise (2005) “A criminalidade informática”. In: DE Lucca, Newton; Simão Filho, Adalberto (coord). “Direito & Internet”, Quartier Latin, São Paulo.

ITU - International Telecommunication Union (2012) “Understanding cybercrime: Phenomena, challenges and legal response”. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

Nogueira, S.D´Amato (2009) “Crimes de Informática”, Leme, Belo Horizonte.

Nucci, Guilherme de Souza (2009) "Leis Penais e Processuais Penais Comentadas", Revista dos Tribunais, São Paulo.

Plantullo, Vicente L. (2010) "Estelionato eletrônico: Segurança na Internet". Juruá, Curitiba.

Poder Judiciário (2008) "Conselho Nacional de Justiça. Resolução Nº 59, de 09 de setembro de 2008. Disciplina e uniformiza as rotinas visando ao aperfeiçoamento do procedimento de interceptação de comunicações telefônicas e de sistemas de informática e telemática nos órgãos jurisdicionais do Poder Judiciário, a que se refere a Lei nº 9.296, de 24 de julho de 1996", http://www.cnj.jus.br/atos-administrativos/atos-da-presidencia/resolucoespresiden cia/12174-resolu-no-59-de-09-de-setembro-de-2008.

Prado, Luiz Regis (2002) "Curso de Direito Penal Brasileiro", Revista dos Tribunais, São Paulo.

Rezek, Francisco (2010) "Direito Público Internacional:curso elementar", Saraiva, São Paulo.

STF (2001) "Ação Direta de Inconstitucionalidade nº 1488", Relator: Ministro Néri da Silveira,http://www.stf.jus.br/portal/diarioJustica/verDiarioProcesso.asp?numDj=55&dataPublicacaoDj=20/03/2001&incidente=1648295&codCapitulo=6&numMateria=32&codMateria=2.

STJ (1990) "Súmula 17. Quando o falso se exaure no estelionato, sem mais potencialidade lesiva, e por este absorvido", http://www.dji.com.br/normas_inferiores/regimento_interno_e_sumula_stj/stj__0017.htm.

STJ (2002) "Habeas Corpus nº 15.026/SC", Relator: Ministro Vicente Leal, data do julgamento: 24/09/2002, https://ww2.stj.jus.br/revistaeletronica/ita.asp?registro=200001264931&dt_publicacao=04/11/2002.

STJ (2006) "Carta Rogatória nº 000297", Relator: Ministro Barros Monteiro, data de publicação: 18/12/2006, http://www.stj.jus.br/SCON/decisoes/toc.jsp?livre=(CR+e+000297).nome.

STJ (2008) "Habeas Corpus nº 101.165/PR", Relator: Ministra Jane Silva, data do julgamento: 01/04/2008, https://ww2.stj.jus.br/revistaeletronica/ita.asp?registro=200800454698&dt_publicacao=22/04/2008.

STJ (2008) "Embargos de Declaração em Recurso no Mandado de Segurança nº 25.375/PA", Relator: Ministro Felix Fischer, data do julgamento: 18/11/2008, https://ww2.stj.jus.br/revistaeletronica/ita.asp?registro=200702410579&dt_publicacao=02/02/2009.

STJ (2009) "Habeas Corpus nº 83.338/DF", Relator: Ministro Hamilton Carvalhido, data do julgamento: 29/09/2009, https://ww2.stj.jus.br/revistaeletronica/ita.asp?registro=200701161721&dt_publicacao=26/10/2009

Vieira, Mauro Luiz Iecker (2010) "Resposta do embaixador do Brasil nos EUA a consulta sobre o uso da Internet naquele país", Cultura Digital, 24/05/2010, http://culturadigital.br/marcocivil/2010/05/24/contribuicao-de-washington-para-o-marco-civil/.

Weber, Patrícia Núñez (2011) "A cooperação jurídica internacional em medidas processuais penais", Verbo Jurídico, Porto Alegre.

Wendt, Emerson and Jorge, Higor Vinicius Nogueira (2012) "Crimes cibernéticos: Ameaças e procedimentos de investigação", Brasport, Rio de Janeiro.

