DELITOS INFORMÁTICOS: CONVENÇÃO DE BUDAPESTE

Denise Tanaka dos Santos[1]

Resumo: O objetivo deste artigo é avaliar o impacto da criação da Convenção de Budapeste na modificação da legislação penal dos diversos Estados-membros. O surgimento da citada convenção reflete-se como forma de combate à nova criminalidade, advinda de novos paradigmas apresentados no panorama internacional, notadamente no que tange aos delitos informáticos.

Palavras-chave: Convenção. Budapeste. Delitos. Cibernéticos. Informáticos. Direito penal.

Abstract: This article attempts to draw attention to what has been cybercrime and evaluate the impact of the Budapest Convention on the Brazilian criminal law.

Keywords: Convention. Budapeste. Cybercrimes. Criminal Law.

1 Mestranda em direito pela Pontifícia Universidade Católica de São Paulo (PUC-SP), mestranda em direito pelas Faculdades Metropolitanas Unidas, especialista em direito público e direito processual civil, cursou propedêutico de direito internacional na Universidade de Amsterdã e direito internacional na Corte Internacional de Haia. É Defensora Pública Federal.

1 Os Tratados Internacionais

O estudo da Convenção de Budapeste requer, de forma preliminar, uma breve inserção na compreensão do direito internacional público. Nesse sentido, Accioly e Silva[2] destacam que esse ramo do direito aborda o conjunto de regras jurídicas e rege a relação entre sujeitos de direito internacional: Estados, organizações internacionais e indivíduos no seio da comunidade internacional.

A origem desse arcabouço jurídico foi a necessidade de estabelecer a paz entre Estados soberanos. É importante mencionar que o estabelecimento de regras internacionais não abala a soberania dos Estados; ao contrário, ratifica-a sobremaneira. Assim, somente os Estados soberanos podem firmar tais instrumentos, criados por eles. Em suma, os tratados são reflexos da soberania.

Podem-se pontuar como fontes do direito internacional, ao lado das convenções, os costumes, os princípios gerais de direito e as decisões judiciais. No que se refere aos tratados, a Convenção de Viena, assinada em 1969 e fonte de direito, codificou regras consuetudinárias sobre o assunto, sendo posteriormente complementada pela Convenção de 1986.

Com base nessas convenções, no que tange à terminologia, tratado é um acordo regido pelo direito internacional e, conforme Accioly e Silva, "qualquer que seja sua denominação".[3] Assim, trata-se de expressão genérica, constituindo um acordo escrito de vontades, entre dois ou mais sujeitos de direito internacional, de direitos e deveres vinculantes e regido pelo direito internacional.

Nesse contexto, a relação entre o direito interno e o direito internacional trata de um tema vasto e controverso. No Brasil, a incorporação dá-se pela

2 ACCIOLY, Hildebrando; SILVA, Geraldo Eulalio Nascimento e. **Manual de direito internacional público**. 15. ed. São Paulo: Saraiva, 2002.
3 Ibid., p. 29.

aplicação dos arts. 49, I, e 84, VIII, ambos da Constituição Federal;[4] além disso, envereda-se pelas teorias monistas e dualistas. Kelsen,[5] por exemplo, defende a primeira teoria: há duas normas em um mesmo ordenamento jurídico, sendo que a antinomia utiliza a hierarquia do direito internacional. Já a segunda teoria, a dualista, trata da existência de dois ordenamentos diferentes, porque são fontes diversas. Logo, a norma internacional precisa ser internalizada, de modo que a lei é inconstitucional, não o tratado.

Há, ainda, teorias intermediárias, como o monismo moderado, segundo o qual não há a necessidade de lei para a incorporação de normas internacionais, mas decreto; e o dualismo moderado, no qual se precisa de decreto quando for válido fora. Além disso, há o disposto na Emenda Constitucional nº 45/04,[6] para a qual os tratados internacionais serão incorporados em nível constitucional quando forem aprovados segundo as regras formais das emendas.

Nesse sentido, o Supremo Tribunal Federal entende que os tratados de direito internacional ingressam no ordenamento interno em forma de lei ordinária, adotando-se, assim, a teoria dualista. Ocorre que, no caso de direito humanos, há outros entendimentos. Flávia Piovesan, notadamente, entende que as normas de direitos humanos oriundas de tratados internacionais ingressam no ordenamento jurídico brasileiro como normas constitucionais.[7] Para ela, os direitos insertos nos tratados internacionais de direitos humanos são direitos constitucionalmente consagrados.

---

4 BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília: Senado Federal, 1988.

5 KELSEN, Hans. **Teoria pura do direito**. 6. ed. São Paulo: Martins Fontes. 1988.

6 BRASIL. Constituição (1988). Emenda Constitucional nº 45, de 30 de dezembro de 2004. Altera dispositivos dos arts. 5º, 36, 52, 92, 93, 95, 98, 99, 102, 103, 104, 105, 107, 109, 111, 112, 114, 115, 125, 126, 127, 128, 129, 134 e 168 da Constituição Federal, e acrescenta os arts. 103-A, 103B, 111-A e 130-A, e dá outras providências. **Diário Oficial da União**, Brasília, DF, 31 dez. 2004a.

7 PIOVESAN, Flávia. **Direitos humanos e o direito constitucional internacional**. São Paulo: Max Limonad, 2002.

Por sua vez, a Emenda Constitucional nº 45/04, que alterou o art. 5º, § 3º, da Constituição Federal,[8] institui que os tratados e convenções internacionais sobre direitos humanos que forem aprovados em cada Casa do Congresso Nacional, em dois turnos, por três quintos dos votos dos respectivos membros, serão equivalentes a emendas constitucionais. Por fim, o Ministro Sepúlveda
Pertence, todavia em decisão isolada, compatibilizou a questão, com uma solução hermenêutica, segundo a qual as normas de direitos humanos originadas em tratados internacionais têm natureza de norma supralegal.

Já para fins de sistematização do tema inserido na Convenção de Budapeste, é importante destacar a Convenção das Nações Unidas para o combate contra os crimes de organizações transnacionais – a Convenção de Palermo.

Há parte da doutrina que entende configurar verdadeira atipicidade. Nesse contexto, a organização criminosa no Brasil, por falta de elementos típicos, restaria impune, podendo ser aplicada, no caso, a norma referente à quadrilha ou bando (art. 288 do Código Penal).[9] Por outro lado, há entendimento no sentido de que o Decreto nº 5.015, de 12 de março de 2004,[10] que promulgou a Convenção de
Palermo contra organizações criminosas transnacionais, é suficiente para tipificar a conduta de um grupo estruturado com três ou mais pessoas, reunido em algum tempo, para cometimento de um ou mais infrações graves para obter, direta ou indiretamente, benefício econômico.

É certo que tal entendimento, cuja visão é ampla e de cunho internacional, pode, após a assinatura da Convenção de Budapeste pelo Brasil, dirimir certos conflitos referentes a lacunas legislativas, a depender do caso concreto.

8 BRASIL, op. cit.
9 BRASIL. Decreto-lei nº 2.848, de 7 de dezembro de 1940. Código Penal. **Diário Oficial da União**, Rio de Janeiro, 31 dez. 1940.
10 BRASIL. Decreto nº 5.015, de 12 de março de 2004. Promulga a Convenção das Nações Unidas contra o Crime Organizado Transnacional. **Diário Oficial da União**, Brasília, DF, 15 mar. 2004b.

2 A Convenção de Budapeste

2.1 A origem

A Convenção de Budapeste, de 21 de novembro de 2001, foi o primeiro trabalho internacional sobre crime no ciberespaço, tendo surgido devido ao novo panorama internacional e aos novos paradigmas enfrentados.

A título de exemplo, menciona-se o surgimento de delitos transnacionais, os quais ultrapassam os limites territoriais do direito penal interno, formando verdadeiros paraísos de informação. Ademais, são crimes de alta tecnologia, tanto pela necessidade de equipamentos e conexão, quanto pelo conhecimento dos programas e dos acessos, tratando-se de bens jurídicos difusos e imateriais, relacionados ao computador e à internet.

Recorde-se que a internet surgiu nos centros acadêmicos e no ambiente militar, em nível de Estados, tendo passado com grande rapidez aos meios corporativos industriais e econômicos, chegando com a mesma velocidade aos indivíduos particulares. Foi com o eclodir do 11 de setembro que os países, notadamente os Estados Unidos e os países da Europa, iniciaram uma série de trabalhos, que culminou na promulgação da Convenção de Budapeste.

Essa Convenção foi criada pelo Conselho da Europa, Estados Unidos, Canadá, Japão e África do Sul – o Brasil, todavia, não assinou tal tratado; de toda a forma, há projetos de lei tramitando, que tratam do assunto em pauta. Em seu preâmbulo, destaca-se a importância da unidade entre os membros, bem como da sua cooperação, sendo que os Estados-membros buscam perseguir uma política criminal comum direcionada à proteção da sociedade contra o cibercrime, por meio de uma legislação apropriada, pela alteração causada pela digitalização e pela contínua globalização das redes de computador.

Nesse item, estampa-se a preocupação dos Estados no sentido de que há preocupação com o risco de as redes de computadores e as informações eletrônicas poderem ser usadas para o cometimento de crimes e de provas relativas a essas ofensas poderem ser armazenadas e transferidas por essas redes. Assim, concordou-se que a Convenção de Budapeste é necessária para prevenir ações diretas contra os bens jurídicos tutelados, como, à guisa de exemplo, a confidencialidade, a integridade e a disponibilidade de sistemas de computador, redes e dados de computador, assim como a má utilização destes, provendo a criminalização de cada conduta.

E mais, não se esqueceram dos ditames insertos para a proteção aos direitos humanos e liberdades fundamentais.

2.2 O objetivo da Convenção de Budapeste

A Convenção assinalada recomenda a tipificação de delitos. Nesse sentido, é interessante lembrar que não se trata tão somente de crimes, pois há, na mesma linha, contravenções penais, como o jogo do bicho por meio do computador; por isso, recomenda a tipificação de delitos. Além disso, sugere e não obriga, uma vez que não tem vinculação coercitiva, servindo de parâmetro a ser observado pelos Estados, a fim de uniformizar as várias legislações internas.

Também, traz recomendações acerca da cooperação internacional e de aspectos relacionados à investigação criminal e a procedimentos de processo penal. Apesar da grande importância do tema, este trabalho restringir-se-á aos aspectos de direito penal material inseridos na Convenção de Budapeste.

2.3 As definições

Com o precípuo objetivo de uniformizar as várias legislações dos mais diversos Estados envolvidos, a presente Convenção trouxe definições acerca dos delitos praticados no ciberespaço e relacionados ao computador, podendo-se destacar os seguintes termos:

> • sistema de computador: equipamentos conectados, que, viabilizados por um programa, realizam processamento automático de dados;
>
> • dados de computador: qualquer representação de fatos, informações ou conceitos em uma forma adequada para o processamento em um sistema de computador, incluindo um programa apropriado que possibilite ao sistema de computador realizar uma função;
>
> • provedor de serviços: qualquer entidade pública ou privada que proporcione aos usuários de seus serviços a possibilidade de se comunicar por meio de um sistema de computador ou qualquer outra entidade que processe ou armazene dados de computador em benefício de tal serviço de comunicação ou dos usuários desse serviço;
>
> • tráfego de dados: qualquer dado de computador relacionado a uma comunicação, gerado por um sistema de computador e que forma uma parte de uma cadeia de comunicação, indicando a origem da comunicação, destino, rota, tempo, data, tamanho,duração ou tipo de base de serviço.

2.4 As diretrizes para a tipificação

A doutrina traz o conceito de delitos informáticos. Para Ferreira, por exemplo, crime de informática é "toda a ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão."[11]

11 FERREIRA, Ivette Senise. A criminalidade informática. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coords.). **Direito & internet:** aspectos jurídicos relevantes. Bauru: Edipro, 2000. p. 207-237. p. 209.

Já na lição precisa de Rossini,

> a denominação 'delitos informáticos' alcança não somente aquelas condutas praticadas em que haja relação com sistemas informáticos, quer de meio, quer de fim, de modo que essa denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta, sem a imprescindível conexão à rede mundial de computadores, ou a qualquer outro ambiente telemático.[12]

Em remate, o percuciente autor entende que o delito classificado como informático poderia ser

> a conduta típica e ilícita, constitutiva de crime ou contravenção penal, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem elementos a integridade, a disponibilidade e a confiabilidade.[13]

Ainda, o ilustre autor destaca a importância da Convenção de Budapeste – Convenção sobre cibercrime –, no sentido de que ela traz

> condutas praticadas em ambiente de rede, não as fora dele, abarcando, desta forma, apenas os fatos típicos ocorridos exclusivamente no Ciberespaço, podendo, receber a denominação de 'delito telemático', dada a peculiaridade de ocorrer no e a partir do inter-relacionamento entre os computadores em rede telemática usados na prática delitiva.[14]

Assim, conclui o doutrinador que "delito informático é gênero, do qual delito telemático é espécie."[15]

---

12 ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004. p. 110.

13 Ibid., p. 110. 14

Ibid., p. 110.

15 ROSSINI, 2004, p. 110.

Sobre as classificações, Rossini classifica os delitos de informática em puros e mistos. Os delitos puros ocorrem quando o sujeito ativo objetiva o sistema de informática; já nos impuros, o computador é simples instrumento para a ofensa a outros bens jurídicos, que não exclusivamente os do sistema informático.[16] Nessa esteira, vale a pena discorrer brevemente sobre o bem jurídico analisado pela

Convenção de Budapeste, que deve ser verificado segundo as teorias humanistas ou de direito penal mínimo.

O ser humano pratica condutas hodiernamente e, de acordo com o pacto social, despoja-se de parte de sua liberdade em favor da ordem social. Assim, a sociedade na qual está inserido o homem individual escolhe quais condutas devem ser punidas com mais rigor, e assim sucessivamente. Dessa forma, as condutas mais graves serão abarcadas pelo direito penal e, para as condutas intermediárias, podem-se aplicar sanções de natureza civil ou administrativa. Ainda, para a maioria da doutrina, as condutas praticadas por meio da internet geram o seu uso indevido, com a criação de condutas que espelham a necessidade de sua tipificação diante da sociedade de risco.

Na linha de análise do bem jurídico, Smanio pondera que

> trata-se de um bem jurídico-penal de natureza difusa. Isto porque, além de atingir um número indeterminado de pessoas, gera conflituosidade entre o interesse dos usuários da Internet, os *hackers* e os *crackers*, bem como das grandes corporações quer de fornecedores, quer de provedores de acesso.[17]

Para o citado autor, há bens jurídico-penais individuais, dos quais se tem disponibilidade; bens de natureza coletiva, referentes à coletividade; e bens de natureza difusa, que, da mesma forma, referem-se à sociedade e são indisponíveis, porém com uma conflituosidade inerente a vários grupos sociais, notadamente o

16 Ibid.
17 SMANIO, Gianpaolo Poggio. **Tutela penal dos direitos difusos**. São Paulo: Atlas, 2000. p. 108.

meio ambiente, o consumidor e a saúde pública.[18] Além disso, na lição lapidar de Rossini, há um bem jurídico absolutamente permanente: a segurança da informática, independentemente dos bens jurídicos individuais ou coletivos.[19]

Após a breve análise do conceito de delito informático, de sua classificação e da natureza do bem jurídico envolvido, parte-se para a abordagem das disposições sobre delitos no ambiente de rede, subdivididas em nove infrações, enquadradas, por sua vez, em quatro categorias: a primeira diz respeito à proteção da confiabilidade, integridade e disponibilidade dos sistemas de computador; a segunda, aos danos relacionados a computador; a terceira, aos danos relacionados ao conteúdo; e a última, à transgressão de direitos autorais e correlatos.

Nesse contexto, vale a pena sublinhar alguns tópicos referentes a essas categorias de delitos em ambiente de rede. Assim, a confiabilidade, a integridade e a disponibilidade de dados dizem respeito ao acesso e interceptação ilegais, cujo elemento subjetivo é o dolo – aliás, há influente doutrina que sustenta a necessidade da tipificação de condutas sob o manto da culpa –; nesse item, ressaltem-se a interferência de dados e sistemas e o mau uso de equipamentos. Aqui, há a punição dos atos preparatórios, como no crime de quadrilha ou bando (art. 288 do Código Penal brasileiro)[20] e em algumas contravenções penais.

Já a segunda categoria refere-se a danos relacionados a computador e à verdade das informações nele contidas, sendo que tais condutas estão diretamente ligadas à falsificação e à fraude, comprometendo, sobremaneira, a veracidade dos dados inseridos em ambiente de rede.

A terceira categoria de delitos informáticos sugerida pela Convenção de Budapeste é sobre o conteúdo dos dados apresentados pelo computador, sendo o ponto crucial a pornografia infantil. É importante destacar que a Convenção define

18 Ibid., p. 108. 19 ROSSINI, 2004. 20 BRASIL, 1940.

o termo vago de pornografia infantil como o oferecimento e a disponibilidade desse material, em ambiente aberto ou fechado, desde os atos preparatórios, além de estabelecer que as imagens com cenas pornográficas podem designar menores ou os que aparentem menoridade.

Dessa forma, tipifica-se a conduta de imagens pornográficas de pessoas que já atingiram a maioridade. Explica-se: as imagens de um jovem captadas há muito tempo restariam atípicas se, no presente momento, essa vítima houvesse atingido a maioridade. Assim, a Convenção ampliou o campo de punibilidade penal. Ainda, cabe ressaltar que pornografia infantil difere de pedofilia, que, além de ter abrangência maior, abarca as condutas, notadamente, de estupro envolvendo menores, atentado violento ao pudor, prostituição infantil, drogas, distribuição de material pornográfico etc.

Por fim, a quarta categoria de diretrizes para tipificação contida na Convenção de Budapeste recai sobre a transgressão a direitos autorais e correlatos. Significa dizer que se trata de condutas dolosas, lembrando a posição da respeitada doutrina sobre a tipificação de condutas culposas e com escala comercial. Isso porque a abrangência deve ser ampla, o que destaca a escala comercial e por sistema de computador.

Nesse tópico, há interesses particulares envolvidos, o que sustenta o empenho individual na persecução penal. Contudo, ocorre que há outros interesses envolvidos, de forma que o Estado, de maneira singular, tem interesse na arrecadação de tributos, os quais, com a conduta delituosa, restariam sonegados.

3 A Responsabilidade

A Convenção de Budapeste sugere a tipificação tanto da pessoa física quanto da pessoa jurídica. No sistema jurídico atual, a responsabilidade da pessoa física já traz contornos seguros e doutrina pacificada. O problema da tipificação, portanto, recai sobre a responsabilidade da pessoa jurídica.

Berenguer e Torres afirmam que há lacunas para a responsabilização da pessoa jurídica, especialmente dos provedores de serviços em ambiente de rede, e sustentam que o ato desses provedores vai muito além do apoio técnico; de fato, trata-se de verdadeira colaboração. Mas, indagam eles: qual seria a abrangência dessa responsabilidade dos provedores de acesso? Além disso, apresenta-se o dilema dos limites territoriais restritos do direito penal interno de cada Estado-membro.[21]

A solução, para os autores, recai sobre a criação de tratados internacionais, referências legais, bem como normas jurídicas globais, como, por exemplo, a Convenção de Palermo, de 2000, que determinou a obrigação universal de combate a tal conduta.[22]

Também, esclarecem os renomados doutrinadores que os Estados Unidos optaram por uma regulação mais restrita, no que tange à responsabilização da pessoa jurídica, no campo da delituosidade informática. Assim, a responsabilidade recai na omissão de controle para evitar a circulação de dados com conteúdos proibidos.[23] Nesse sentido, importante foi o caso do C*ommunications Decency Act*, de 1996; ocorre que tal ato foi declarado inconstitucional, haja vista a sua incompatibilidade com a 1ª Emenda estadunidense, que declara a liberdade de expressão.

De outra banda, na Europa, a preocupação com a responsabilização da pessoa jurídica, no campo da delituosidade informática, ocorreu após o processo judicial, na Alemanha, em face da empresa Compuserve, em 1997. O provedor foi condenado, em primeira instância, por difundir material pornográfico infantil, advindo dos Estados Unidos; sublinhe-se, porém, que tal decisão foi reformada no tribunal germânico. De toda forma, a doutrina alemã ressaltou a atipicidade

21 BERENGUER, Enrique Orts; TORRES, Margarita Roig. **Delitos informáticos y delitos comunes cometidos a través de la informática**. Valencia: Tirant lo Blanch, 2001.
22 Ibid.
23 BERENGUER; TORRES, 2001.

da responsabilidade do provedor. A solução foi a implementação de reformas legislativas, tanto em nível estadual quanto federal, a partir de agosto de 1997. Entretanto, as reformas referidas são limitadas, ou seja, implicam o conhecimento do conteúdo proibido por parte dos provedores, a respectiva omissão na prevenção e na circulação e seu subsequente bloqueio.

Entre nós, Rossini comenta que, para a implantação do mandamento da Convenção de Budapeste, no sentido da responsabilidade da pessoa jurídica, é necessária a edição de emenda constitucional, no mesmo formato da responsabilidade da pessoa jurídica no campo do meio ambiente e nos crimes financeiros.[24] Além disso, a responsabilidade do provedor recairia na falha da supervisão e controle, atuando como verdadeiro garante diante de uma conduta omissiva. Assim, hodiernamente, no Brasil, comina-se a participação da pessoa física, restando atípica a conduta delituosa praticada pelo provedor de serviços no ambiente de rede.

Impende observar, nesse tópico, que o Brasil, todavia, não assinou a Convenção de Budapeste, porém nada impede a construção hermenêutica sugerida por parte da doutrina, como na tipificação de organização criminosa, nos termos da Convenção de Palermo.

4 As Sanções

O art. 11 da Convenção de Budapeste estabelece que cada Parte criará medidas legislativas, em conformidade com o seu direito interno, estabelecendo como infração penal a cumplicidade, quando dolosa, ou seja, com a intenção de que as condutas tipificadas na referida Convenção sejam cometidas. Além disso, demonstra a necessidade de se estabelecer como infração penal a tentativa, segundo os parâmetros do direito interno de cada Estado-membro.[25]

24 ROSSINI, 2004.
25 CONSELHO DA EUROPA. **Convenção sobre o cibercrime**. Budapeste: Conselho da Europa, 2001.

Já seu art. 13 sugere que cada Parte adotará medidas legislativas e outras que se revelem necessárias para assegurar que as infrações penais dos arts. 2º a
11 verificadas em aplicação sejam passíveis de sanções efetivas, proporcionais e dissuasivas, inclusive com privação de liberdade. Ademais, pontifica a necessidade da responsabilização da pessoa jurídica, nos termos do art. 12. Assim, esses sujeitos ativos seriam punidos com sanções ou medidas, penais ou não penais, eficazes, proporcionais e dissuasivas, incluindo sanções pecuniárias.[26]

5 O Direito Comparado

A erudita tese de Rossini sobre o direito comparado afirma que, mesmo antes da Convenção, houve vários encontros internacionais; notadamente, o Conselho da Europa (Mercado Comum Europeu) adotou a Recomendação nº 9 da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), a qual sugeria a criação de 8 tipos. Por sua vez, a Convenção adotou a tipificação de tais condutas por força do 11 de setembro.[27]

Nessa linha, antes mesmo da Convenção, vários Estados já tentavam criminalizar condutas informáticas em ambiente de rede, como Portugal, Itália, Espanha e Venezuela. Inicialmente, Portugal preocupou-se com o tema e enfrentou o desafio, alterando as normas legislativas por intermédio da edição de legislação específica: a Lei nº 109, de 17 de agosto de 1991 – Lei da Criminalidade
Informática –, dispõe de forma expressa que aos crimes previstos na presente lei são subsidiariamente aplicáveis as disposições do Código Penal. Além disso, utiliza a definição de termos técnicos, como a Convenção de Budapeste; a título de ilustração, definem-se rede, sistema e programa informático.[28]

---

26 CONSELHO DA EUROPA, 2001. 27
ROSSINI, 2004.
28 PORTUGAL. Lei nº 109, de 17 de agosto de 1991. Lei da Criminalidade Informática. **Diário da República**, Lisboa, 17 ago. 1991.

O art. 3º da referida lei trata da responsabilidade penal das pessoas coletivas e equiparadas, as quais são penalmente responsabilizadas quando os atos tipificados forem cometidos em seu nome e no interesse coletivo pelos seus órgãos ou representantes. Observe-se que tal responsabilização não exclui a responsabilidade individual dos respectivos agentes.[29]

Por fim, a lei tipifica condutas, como a falsidade informática, o dano a dados ou a programas informáticos, a sabotagem e o acesso ilegítimo, a interceptação e reprodução ilegítima, e comina penas às pessoas coletivas: admoestação, que pode ser cumulativa com pena acessória de caução, multa e dissolução.[30]

Por sua vez, a Itália editou, em 23 de dezembro de 1993, lei sobre modificações e integrações das normas do Código Penal e do Código de
Processo Penal em tema de crime de computador. Tal lei faz uma adequação aos tipos penais já existentes, alterando-os no sentido de tipificar as condutas que a sociedade considera lesivas ao sistema penal como um todo, incluindo o sistema informático ou telemático. Assim, não há diferenciação na criação de tipos penais extravagantes, mas a adequação do próprio Código Penal, tais como: dano a equipamento de utilidade pública, falsidade a documentos informáticos públicos ou privados, acesso indevido, entre outros.

É interessante sublinhar que essa lei especificou o conceito de correspondência, como sendo a epistolar, telegráfica, telefônica, informática ou telemática, ou qualquer outra forma de comunicação à distância, além de fazer, inclusive, adequações na parte processual penal, como sobre os procedimentos de interceptações de comunicações informáticas ou telemáticas.

Já a Espanha traz um panorama interessante. Sobre essa nação, analisam-se artigos do Código Penal relacionados às infrações penais informáticas, valendo a pena trazer à colação alguns tipos penais:

29 Ibid.
30 Ibid.

- art. 169 – das ameaças: as penas são aumentadas quando forem por escrito, por telefone ou por qualquer outro meio de comunicação ou de reprodução, ou em nome de entidades ou grupos reais ou supostos;
- art. 189 – dos delitos de exibicionismo e provocação sexual: será punido aquele que utilizar menores de idade ou incapazes para fins de espetáculos exibicionistas ou pornográficos, tanto públicos quanto privados, ou para elaborar qualquer tipo de material pornográfico, ou financiar qualquer dessas atividades; bem como aquele que produzir, vender, distribuir, exibir ou facilitar a produção, venda, difusão ou exibição por qualquer meio de material pornográfico em cuja elaboração tenham sido utilizados menores de idade ou incapazes, ainda que o material tenha sua origem no exterior ou no desconhecido. Ainda, pune quem possui esse material para a realização de qualquer uma dessas condutas, com pena reduzida em metade, além de cuidar da violação e divulgação de segredos e de crimes contra a honra. Nesse item, a punição recai quando realizadas as condutas com propagação por meio de imprensa, radiodifusão ou por qualquer outro meio de eficácia semelhante;
- art. 473 – dos delitos contra a Constituição: traz à baila o crime de rebelião, quando, notadamente, cause estrago em propriedades de titularidade pública ou privada e sejam cortadas as comunicações telegráficas, telefônicas e por ondas.[31]

Por fim, a Venezuela, como Portugal, tratou do tema com a edição de lei especial contra delitos informáticos, em 6 de setembro de 2001. Nesse caso, o objeto da lei é a proteção integral dos sistemas que utilizem tecnologias de informação, bem como a prevenção e sanção dos delitos cometidos contra tais sistemas ou quaisquer de seus componentes, ou os cometidos com uso de tecnologias.

Da mesma forma que a Convenção de Budapeste, essa lei traz definições de termos, como tecnologia da informação, sistemas e dados, e, inclusive, define mensagem de dados como qualquer pensamento, ideia, imagem, áudio, dado ou informação, expressa em uma linguagem conhecida, que pode ser explícita ou secreta (encriptada), preparada dentro de um formato adequado para ser transmitido por um sistema de comunicações.

31 ESPANHA. Ley Orgánica nº 10, de 23 de noviembre de 1995. Código Penal. **Boletín Oficial del Estado**, Madri, 23 nov. 1995.

Além disso, pune, em seu art. 5º, a pessoa jurídica nos casos em que o fato punível tenha sido cometido por decisão de seus órgãos, no âmbito de sua atividade, com seus recursos sociais ou em seu interesse exclusivo ou preferente. Como ilustração, a citada lei pune, no Capítulo IV – Dos delitos contra crianças e adolescentes, o ato de difusão ou exibição de material pornográfico e a exibição pornográfica de crianças e adolescentes.

Como vaticinado, destaca Rossini os critérios metodológicos para o estudo das infrações penais telemáticas no Brasil. Para o ilustre doutrinador, admitem-se a classificação das infrações penais informáticas em próprias e impróprias, a colocação em tipos no Código Penal e na legislação extravagante, bem como a escolha dos tipos segundo sua ocorrência concreta, com base em pesquisas de mídia. Ademais, reconhece-se a participação do art. 29 do Código Penal na forma material ou moral.[32]

5 As Três Reformas Legislativas

Albuquerque pondera que houve três reformas penais. A primeira, referente à privacidade, aconteceu na década de 1970, como ocorreu na Alemanha, Canadá, Estados Unidos, França, Israel, Japão e Holanda, por intermédio de leis específicas para proteger o cidadão do armazenamento, coleta e transmissão arbitrários de dados pessoais.[33]

A segunda tipificação de condutas informáticas delituosas, datada da década de 1980, recaiu sobre a ocorrência de natureza econômica, com projeção patrimonial. Nesse contexto, ao invés de estender as infrações já existentes, haja vista a estrita observância ao princípio da legalidade e, além disso, a proibição da

32 ROSSINI, 2004.

33 ALBUQUERQUE, Roberto Chacon de. **A criminalidade informática**. São Paulo: Juarez de Oliveira, 2006.

aplicação da analogia em desfavor do réu, em matéria penal material, vários países editaram leis específicas. Aqui, segundo o referido autor, induzia-se em erro um computador e não uma pessoa, pois os objetos eram intangíveis.[34]

Finalmente, a terceira onda de reforma penal ocorreu ao longo da década de 1980, tendo como objeto jurídico a propriedade intelectual, com a exclusão dos programas de computador da proteção do direito das patentes, dos anos 1970. Assim, o *software* passou a ser uma obra intelectual em países como Alemanha, Estados Unidos, Índia, México e Japão.

Essa doutrina afirma que o Brasil atendeu parcialmente a segunda e terceira ondas de reformas penais. O autor fundamenta tal posicionamento na promulgação da Carta de 1988; na edição da Lei nº 9.507/97, sobre *habeas data*; e na edição da Lei nº 9.983/00, sobre a reforma do Código Penal, e da Lei nº 9.609/98, sobre a proteção da propriedade intelectual de programas de computador e sua comercialização no país.[35]

Albuquerque estabelece, ainda, que existem preponderantemente dois mé-todos para a reforma penal anteriormente descrita.[36] O primeiro estampa a reforma do Código Penal, com a introdução de novos artigos para oferecer proteção contra condutas ilícitas denominadas pela sociedade especificada; esse é o caso da Holanda e da Alemanha. O segundo, por sua vez, determina que os Estados adotem legislação específica, entendimento que encontra fundamento no processo de descodificação da legislação e na verticalização do direito constitucional. Ressalte-se que tais leis específicas restam desprendidas do Código Penal. À guisa de exemplo, citam-se Portugal e Inglaterra.

O referido doutrinador entende que o Brasil deveria adotar a primeira opção, determinando-se as condutas consideradas crimes, para posterior inserção

34 Ibid.
35 Ibid.
36 Ibid.

no Código Penal vigente. Dessa forma, analisam-se quais condutas podem ganhar características novas em artigos já existentes e quais podem ser atualizadas para enquadrar condutas com novos métodos para os crimes tradicionais e a respectiva proteção a bens jurídicos imateriais.[37] Além disso, os tipos penais devem seguir a sistemática consagrada em artigos já vigentes, porém com outros elementos constitutivos, com a roupagem de artigos independentes.

De toda forma, a maioria da doutrina concorda com o fato de que a colaboração penal internacional é fundamental, haja vista a transnacionalidade dos crimes informáticos em ambiente de rede.

6 Perspectivas e Conclusão

Parte da doutrina entende que o direito informacional é um novo ramo do direito, com objeto e método de estudo próprios. Dessa forma, pode-se defini-lo como um conjunto de instituições jurídicas que converge para a tutela da informação. Indaga-se, no entanto, se é possível, hodiernamente, falar em delitos informáticos como um novo ramo do direito.

Diante dessas revoluções, a Convenção da União Europeia apresenta-se como paradigma para que a comunidade internacional, notadamente o Brasil, estabeleça modificações legislativas relativas à matéria penal, bem como à matéria processual penal e para a cooperação internacional, uma vez que essas medidas são importantes para combater a nova criminalidade transnacional, contra paraísos informáticos criados pela territorialidade do direito penal interno de cada Estado-membro.

Nesse sentido, entende-se, como a melhor doutrina, que a maioria dos tipos já consta no direito brasileiro, restando poucas equiparações legais: coisa e documento digital para crimes patrimoniais e falsificação, tipos abertos para

37 Ibid.

acompanhar rapidez na tecnologia etc., por portarias do Ministério da Ciência e Tecnologia; e responsabilidade da pessoa jurídica, por emenda constitucional, para provedores de acesso e empresas de telecomunicações com capital transnacional, com regulamentação pelo Estado de tais atividades.

Denota-se, também, um novo sujeito ativo no meio informático, que é mais rico e com conhecimento técnico; ainda, o crime é plurilocal e a distância, com várias condutas já tipificadas pelo sistema penal brasileiro. Assim, as condutas não incluídas podem ser colocadas por equiparações e acrescidas ao Código Penal, como ocorrido na Holanda, Alemanha e Espanha.

Em remate, destaca-se que a Convenção de Budapeste ainda não foi ratificada pelo Brasil, porém nada impede que esse Estado utilize os princípios e as normas ali inseridos, como parte das fontes à disposição do aplicador do direito.

Entretanto, sublinhe-se que, para a tipificação de condutas delituosas, é necessária a observação do princípio constitucional da legalidade, ficando tal trabalho a cargo do Poder Legislativo.

Referências

ACCIOLY, Hildebrando; SILVA, Geraldo Eulalio Nascimento e. **Manual de direito internacional público**. 15. ed. São Paulo: Saraiva, 2002.

ALBUQUERQUE, Roberto Chacon de. **A criminalidade informática**. São Paulo: Juarez de Oliveira, 2006.

BERENGUER, Enrique Orts; TORRES, Margarita Roig. **Delitos informáticos y delitos comunes cometidos a través de la informática**. Valencia: Tirant lo Blanch, 2001.

BRASIL. Decreto-lei nº 2.848, de 7 de dezembro de 1940. Código Penal. **Diário Oficial da União**, Rio de Janeiro, 31 dez. 1940.

_____. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília: Senado Federal, 1988.

_____. Constituição (1988). Emenda Constitucional nº 45, de 30 de dezembro de 2004. Altera dispositivos dos arts. 5º, 36, 52, 92, 93, 95, 98, 99, 102, 103, 104, 105, 107, 109, 111, 112, 114, 115, 125, 126, 127, 128, 129, 134 e 168 da Constituição Federal, e acrescenta os arts. 103-A, 103B, 111-A e 130-A, e dá outras providências. **Diário Oficial da União**, Brasília, DF, 31 dez. 2004a.

_____. Decreto nº 5.015, de 12 de março de 2004. Promulga a Convenção das Nações Unidas contra o Crime Organizado Transnacional. **Diário Oficial da União**, Brasília, DF, 15 mar. 2004b.

CONSELHO DA EUROPA. **Convenção sobre o cibercrime**. Budapeste: Conselho da Europa, 2001.

ESPANHA. Ley Orgánica nº 10, de 23 de noviembre de 1995. Código Penal. **Boletín Oficial del Estado**, Madri, 23 nov. 1995.

FERREIRA, Ivette Senise. A criminalidade informática. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coords.). **Direito & internet:** aspectos jurídicos relevantes. Bauru: Edipro, 2000. p. 207-237.

KELSEN, Hans. **Teoria pura do direito**. 6. ed. São Paulo: Martins Fontes. 1988.

PIOVESAN, Flávia. **Direitos humanos e o direito constitucional internacional**. São Paulo: Max Limonad, 2002.

PORTUGAL. Lei nº 109, de 17 de agosto de 1991. Lei da Criminalidade Informática. **Diário da República**, Lisboa, 17 ago. 1991.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

SMANIO, Gianpaolo Poggio. **Tutela penal dos direitos difusos**. São Paulo: Atlas, 2000.

Bibliografia consultada

ASUÁ, Luis Jiménez. **Crônica del crimen**. Buenos Aires: Pannedille, 1970.

GOUVEIA, Sandra. **O direito na era digital**. Crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997.

LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coords.). **Direito & internet:** aspectos jurídicos relevantes. Bauru: Edipro, 2000.

PAESANI, Liliana Minardi. **Direito da informática**. 3. ed. São Paulo: Atlas, 2001.

PLANTULHO, Vicente Lentini. **Estelionato eletrônico**. Curitiba: Juruá, 2003.

SILVA, Rita Cássia Lopes da. **Direito penal e sistema informático**. São Paulo: RT, 2003.

VERDELHO, Pedro; BRAVO, Rogério; ROCHA, Manuel Lopes. **Leis do crime cibernético**. Portugal: Centro Atlântico, 2003. v. 1.