Cibercriminalidade e crimes informáticos: uma aproximação entre a legislação italiana e brasileira

Cybercrime and computer crimes: a comparison between Italian and Braszilian legal systems

Fernando Brandini Barbagalo[1]

RESUMO: O presente artigo busca, em estudo comparativo, identificar e analisar a evolução da legislação italiana e brasileira sobre crimes de informática e cibercriminalidade, suas fontes, formas e abrangência. O Brasil aderiu, recentemente, à Convenção de Budapeste, enquanto a adesão da Itália foi ratificada em 2008, promovendo alterações legislativas significativas. O estudo comparado permite reconhecer o atual panorama legislativo da Itália e do Brasil referente à cibercriminalidade e identificar aspectos relevantes que possam auxiliar no desenvolvimento de políticas públicas orientadas a aumentar a segurança no ambiente digital.
Palavras-chave: direito penal; crimes de informática; cibercriminalidade; direito digital; meio ambiente digital; convenção sobre cibercriminalidade.

ABSTRACT: The aim of this comparative study was to identify and to analyze the evolution of both italian and brazilian legislation, along with their sources, forms and scope on computer crimes and cybercrime. Brazil recently acceded to the Budapest Convention, while Italy´s accession was ratified in 2008, promoting significant legislative changes. The comparative study allows us to recognize the current legislative overview in Italy and Brazil in regard to cybercrime and identify relevant aspects that can help in the development of public policies oriented to increasing security in digital environment.
Keywords: criminal law; digital law; computer crimes; cybercrime; digital enviroment; convention on cybercrime.

1. Introdução

[1] Juiz de Direito (TJDFT), Professor da Escola da Magistratura do Distrito Federal e da Universidade Paulista, campus Brasília-DF.

A cibercriminalidade é uma realidade relativamente recente, decorrência da globalização, do aumento exponencial do uso da informática, da evolução das linguagens de programação e do fluxo de dados realizado através da rede mundial de computadores: a internet.[2]

Conforme esclarece a Comissão sobre Prevenção ao Crime e Justiça Criminal da Organização das Nações Unidas, a criminalidade é influenciada pela globalização e todo o processo que facilita o comércio e a integração entre os povos também implica mudanças radicais nas dinâmicas dos crimes e da violência, pois "as tecnologias que possibilitam melhorias substantivas nas vidas das pessoas também são utilizadas por aqueles que burlam as leis, cometem crimes e desafiam a justiça.[3]

A utilização massiva de dispositivos como computadores, *tablets* e *smartphones* que processam e armazenam dados, juntamente com a difusão e a democratização do acesso à *internet*, permitiu que pessoas mal-intencionadas passassem a utilizar as ferramentas da informática e o acesso à rede mundial de computadores para se aproveitar, de diversas formas, do despreparo e do desconhecimento da imensa maioria dos usuários e obter algum tipo de proveito indevido através do acesso furtivo às informações de usuários, dados financeiros, fotografias e vídeos armazenados ou compartilhados.

Os dispositivos de informática e seus diversos aplicativos de comunicação passaram a ser utilizados, largamente, como instrumentos na prática de crimes tradicionais como estelionato, ameaça, furto, difamação, incitação, racismo etc.

Além da utilização dos dispositivos de informática e internet para pratica de crimes comuns, os denominados crimes de informática também evoluíram em gravidade e consequência. Se no início deste século a preocupação residia em atos de pedofilia compartilhados pela internet e no acesso indevido a dados pessoais por *spywares* ou *malwares* encaminhados por e-mails ou outro tipo de mensagem eletrônica, atualmente, o aumento do número de casos de *ransomware*, ou extorsão informática, assusta as corporações[4] e os governos ao redor do globo terrestre.[5]

---

[2] Ao que consta a expressão "cybercrime" foi utilizada pela primeira vez em 1977, na tese de doutorado do professor alemão Ulrich Sieber, ***Computerkriminalität und Stafrecht***.

[3] ONU/UNDOC. Disponível em < https://www.unodc.org/lpo-brazil/pt/crime/index.html > Acesso em 02 de março de 2022.

[4] A empresa alimentícia JBS pagou US$ 11 milhões para não ter seus dados eliminados por *hackers*. ***World's biggest meat producer JBS pays $11m cybercrime ransom***, The Guardian, 10.06.2021. Disponível <https://www.theguardian.com/business/2021/jun/10/worlds-biggest-meat-producer-jbs-pays-11m-cybercrimeransom > acesso em 17.02.2022.

[5] Em novembro de 2020, o Superior Tribunal de Justiça sofreu um ataque que bloqueou a base de dados dos processos em andamento e paralisou todo sistema de informática, provedor e servidor de e-mail do Tribunal. Os

Essas ações perniciosas, mesmo antes da criação de leis específicas, passaram a ser chamadas de "delitos informáticos" ou "cibercrimes", expressões que restaram publicamente consagradas. [6]

Nos últimos anos, especialmente em decorrência do isolamento físico imposto pela Pandemia da Covid-19, aumentou a ação de pessoas especializadas (ou nem tanto) que buscam angariar, indevidamente, algum tipo de vantagem ou mesmo satisfação sexual, utilizando seus computadores ou *smartphones* no conforto de suas casas ou em qualquer outro local provido de acesso à internet.[7]

Esta realidade está impondo uma nova orientação e interpretação da legislação penal. Os delitos de informática ou cibercrimes, consequência do mundo contemporâneo, diferem daqueles de outrora. O *iter criminis* com delimitação temporal e espacial restou ultrapassado. Os estudiosos ainda procuram estabelecer parâmetros hermenêuticos para esta forma de criminalidade e a ciência jurídica, sempre a reboque da realidade, adequa-se para fazer frente a este novo fenômeno.

Como esclarece Spencer Sydow:[8]

> O Direito Penal e o Direito Processual Penal sofreram e sofrem impactos fortes e diretos da informática diuturnamente, porém ainda sem a devida adequação da dogmática tradicional, existindo espaço até mesmo para princípios basilares serem repensados. A tecnologia modifica a forma com que enxergamos a teoria da ciência criminal posto que transforma conceitos de dentro para fora. A imaterialidade torna-se circunstância padrão, assim como a criptografia e a anonimidade; a existência de dispositivos eletrônicos afasta fisicamente o agente da conduta, gerando uma sensação de distância e de prática indireta.

À guisa de conceito, os cibercrimes compreendem as condutas descritas e punidas com sanção penal previstas legalmente que: *i*) acarretem prejuízo nos equipamentos ou sistemas de

---

trabalhos na Corte ficaram paralisados por mais de uma semana, mas o acesso completo ao sistema só foi possível depois de meses. ***Hackers* invadem sistema do STJ e site está fora do ar**. Olhar Digital, 04.11.2020. Disponível em < https://olhardigital.com.br/2020/11/04/seguranca/hackers-invadem-sistema-do-stj-site-esta-fora-do-ar/ > acesso em 16.02.2022.

[6] As dificuldades conceituais dos fatos criminosos praticados com uso de instrumentos de informática ou com auxílio da internet começam quanto às definições utilizadas para se referir a esse tipo de delito. É possível encontrar uma série de denominações na doutrina, jurisprudência e veículos de notícias para esses fatos. Assim, foram criadas expressões como "crimes virtuais", "crimes digitais", "crimes eletrônicos", "crimes cibernéticos", "crimes de internet", "crimes de computador", "crimes de informática", "crimes telemáticos", "cibercrimes" entre outros (CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. Saraiva, 2011, pp. 47-62). A doutrina italiana, igualmente, diferencia os crimes de informática (em sentido estrito) dos cibercrimes (SBORDONI, Stefano. ***Web, Libertà e Diritto, aspetti di dirito positivo nella comunità virtuale***. Istituto poligráfico e zecca dello Stato, Libreria dello Stato, 2014, p. 03.

[7] Segundo dados da Central Nacional de Denúncias de Crimes Cibernéticos foram registradas 156.692 denúncias em 2020, um aumento de 87% em relação a 2019 < https://indicadores.safernet.org.br/ > acesso em 02.02.2022.

[8] **Princípio da Dupla Presunção de Inocência no Direito Penal Informático**. São Paulo: Revista dos Tribunais, Vol. 975, janeiro de 2017, p. 02.

informática, *ii*) que permitam o acesso clandestino a dados armazenados em dispositivos de informática diretamente ou com a utilização da internet *e iii*) condutas criminosas que se valem de equipamentos de informática ou da internet como instrumento ou meio para sua execução, embora, nesta última hipótese, o crime pudesse ser praticado de forma diversa.[8]

Neste sentido, os cibercrimes e crimes de informática podem ser classificados como puros ou próprios quando buscarem prejudicar os sistemas de informática de pessoas físicas ou de empresas. Os chamados delitos de "risco informático" integram esta categoria, pois objetivam o acesso indevido aos dados armazenados ou digitados em equipamentos de informática, o acesso a dados armazenados em discos rígidos ou em "nuvens", diretamente ou utilizando a disseminação de "vírus" (*spyware, malware*) com o consequente prejuízo ao funcionamento de sistemas de informática.[9] Os crimes mistos, impuros ou impróprios seriam as condutas sujeitas a pena criminal que utilizam os equipamentos de informática e internet durante o *iter criminis*, nos atos preparatórios ou como meio de execução em crimes cujos objetos jurídicos não possuam relação com sistema informático ou internet. Assim, atualmente é comum a utilização de aplicativos de mídias sociais com troca de mensagens e dados para prática de crimes que podemos considerar "tradicionais", como os crimes de furto e estelionato, contra a honra, sexuais, incitação e apologia, racismo e até mesmo crimes contra a vida, como o induzimento ou incitação ao suicídio.

Numa rápida distinção, os cibercrimes e crimes de informática puros ou próprios somente podem ser cometidos por meio de recursos tecnológicos e afetam principalmente os dispositivos informáticos e os sistemas de informação ou telemático; enquanto os impuros ou impróprios se utilizam da informática como um *modus operandi* delitivo, porém podem ser praticados por outros meios.[10]

Diante do aumento exponencial desses tipos de crimes, os países não puderam permanecer inertes e engendraram alterações no plano legislativo, tanto no direito privado quanto no direito público, em especial no direito penal, com adaptações e inovações referentes ao novo fenômeno.

---

[8] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. Saraiva, 2011, p. 63. Não obstante, o mesmo autor esclarece: "tecnicamente o mais correto é considerar como crime informático apenas a conduta que vise atingir sistema informático ou de telecomunicações ou ainda, a informação".

[9] WENDT, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos: ameaças e procedimentos de investigação**. 1ª Ed., São Paulo: Editora Brasport, 2012. p. 65.

[10] SYDOW, Spencer Toth. **Princípio da Dupla Presunção**. Obra citada, p. 03.

Neste sentido, Itália e Brasil promoveram alterações e adaptações em suas legislações penais e processuais penais que apresentam, cada qual, contextos, formas e alcances diversos. O escopo do presente trabalho é o estudo da evolução normativa sobre o tema na Itália e no Brasil, identificando os instrumentos legais criados por estes países para prevenção e combate à chamada cibercriminalidade.

2. Os atos normativos italianos sobre a cibercriminalidade

2.1. A influência das normativas do Conselho da Europa na legislação italiana sobre cibercriminalidade

O Conselho da Europa é integrado por 47 (quarenta e sete) países e foi o principal incentivador da modernização da legislação penal e processual penal dos seus Estadosmembros para combater a cibercriminalidade. Por intermédio do Conselho da Europa, foram realizadas conferências, debates e estudos sobre cibercriminalidade, buscando soluções legais para as ações potencialmente criminosas que se iniciaram a partir do desenvolvimento das tecnologias de informática e dos sistemas de telecomunicações e telemática.[11]

Algumas Recomendações[12] foram criadas para que as autoridades dos Estados-membros do Conselho da Europa adotassem determinadas definições de crimes de informáticas em suas legislações. As Recomendações tratavam de aspectos normativos com orientação para criação de crimes específicos e instrumentos legais para investigação, além de mecanismos genéricos de cooperação.

Com o passar dos anos, percebeu-se a necessidade de um empenho maior para conseguir uma padronização da legislação dos Estados-membros sobre cibercriminalidade, crimes

[11] No ordenamento jurídico do Conselho da Europa existem as seguintes espécies de atos normativos: as Diretivas e as Recomendações que não possuem aplicabilidade imediata e, apesar de vincular o Estado-membro quanto ao resultado (futuro), deixam às instâncias nacionais a competência quanto a forma e os meios para sua realização. Enquanto as Diretivas e as Recomendações permitem a harmonização das leis e não possuem aplicabilidade direta, os Regulamentos têm por finalidade a uniformização da legislação e possui aplicabilidade direta, vinculando os Estados-membros e seus respectivos cidadãos. O Regulamento é a "Lei da União (Europeia)". Os Tratados compõem o direito originário, sendo a base da ordem jurídica comunitária, igualmente, com força obrigatória. (ACCIOLY, Elizabeth. **Mercosul e União Europeia Estrutura Jurídico-Institucional**. 4ª Ed, 2010. Curitiba: Juruá, pp. 106-9).

[12] Especialmente as Recomendações R 81-12, R 89-9 e R 95-13.

informáticos e medidas legais para investigação desta espécie de delito, buscando ainda formar uma estrutura de cooperação internacional eficaz contra esta nova espécie delitiva.

Paulatinamente, os Estados-membros do Conselho da Europa adotaram, em maior ou menor medida, as orientações das Recomendações sobre delitos de informática e cibercriminalidade, mas ainda numa velocidade reduzida e com algumas adaptações individuais que debilitava a harmonização das legislações internas.

Prudente destacar que no ordenamento jurídico comunitário da União Europeia, as Recomendações não possuem eficácia vinculativa para os países membros que possuem certa flexibilidade para adotar, em maior ou menor extensão, as suas orientações.

A segunda medida normativa adotada pelo Conselho da Europa sobre crimes de informática, a Recomendação 89, possuía apenas um caráter sugestivo e trazia uma "lista mínima" de delitos apontando que seria "apropriado" aos Estados-membros a criminalização de tais condutas, tais como fraude e sabotagem informáticas e danos em programa ou dados informáticos, com referências ainda a conduta de menor gravidade com intervenção administrativa. O Parlamento italiano acolheu a solicitação e editou a Lei 547, de 23 de dezembro de 1993.[13]

Ainda assim, rapidamente, formou-se um consenso sobre a existência de um défice na maioria das legislações internas dos Estados-membros do Conselho da Europa em relação à cibercriminalidade. Diante disso, a partir da Recomendação R-95-13, em 11 de setembro de 1995, adotada pelos Conselhos de Ministros do Conselho da Europa, houve um incremento das reuniões e discussões para encontrar um ato normativo que vinculasse todos os países integrantes do Conselho da Europa para permitir uma padronização de suas legislações internas.[14]

Como deixa claro seu preâmbulo, a Recomendação R 95-13 manifestou clara preocupação com o direito penal e o processo penal:

> ante o notável desenvolvimento da tecnologia da informação e sua aplicação em praticamente todos os setores da sociedade contemporânea, enfatizando os risco de sua utilização para a prática de crimes e a dificuldade de encontrar e manter as evidências de tais crimes em razão de estarem armazenadas ou mesmo terem sido transmitidas por meios dos sistemas de informação e telemática.[15]

---

[13] CONTRAFATTO, Vania. ***I reati informatici.*** Collana Direta da Gianni Reynaud. *Diritto Penale Dell'Impresa*. 2017, Key Editore, pp. 19-20.

[14] GNOSIS. ***Rivista Italiana di Intelligence***, n. 8. Disponível em < http://gnosis.aisi.gov.it/sito/Rivista8.nsf/servnavig/14 > acesso em 22.02.2022.

[15] Disponível em < https://rm.coe.int/16804f6e76 > Acesso em 10 de fevereiro de 2022.

A partir de então, foram incentivadas alterações na legislação dos países membros do Conselho da Europa com o objetivo de definir claramente os meios de buscas em sistemas de informação, de apreensão dos dados de interesse e de interceptação do fluxo de dados. Ainda houve determinação para que a legislação sobre interceptação de comunicação fosse revista periodicamente, de modo a garantir aplicabilidade às novas tecnologias de informação e a imposição de obrigatoriedade de cooperação dos operadores de redes de informação pública ou privada com as autoridades estatais responsáveis pela investigação desta nova modalidade delitiva.

Por fim, a mesma Recomendação estipulava cuidados para armazenamento e exibição das "provas eletrônicas" de modo a garantir sua integridade, além de estabelecer necessidade realizar pesquisas e treinamento para minimizar o risco de cometimento de crimes com o uso das tecnologias da informação e desenvolver contramedidas técnicas adequadas e estimular a cooperação internacional, autorizando, em casos urgentes, fossem as medidas legais estendidas a outros sistemas informáticos mesmo que localizados em países diversos de onde se iniciou a investigação. Para tanto, foi proposta a criação de uma base legal uniforme com a adoção de instrumentos transnacionais para evitar alegações de violações da soberania interna ou de regras do direito internacional.

Apesar do rigor técnico e da abrangência, havia preocupação de, se acaso algum Estadomembro não adotasse as orientações da Recomendação em sua integralidade, poderem ser criados "paraísos informáticos". Por outro lado, a referida Recomendação desconsiderou a circunstância de que muitos países do bloco já haviam, recentemente, realizado alterações em sua legislação.[16] Essas questões, naquele momento, dificultaram a implementação das novas diretrizes, pois muitos países membros resistiram em alterar sua legislação nos termos integralmente propostos, aguardando a constituição de um ato normativo mais efetivo.[17] Um desses países foi a Itália.

Na época, a Itália havia acabado de alterar a sua legislação penal em razão de uma Recomendação anterior do Conselho Europa. Em resumo, antes da Recomendação 95 (R-9513), de 11 de setembro de 1995, havia sido editada, no fim dos anos oitenta uma outra

---

[16] LA GRECA, Federico Tavassi. ***Hacking e criminalità informática***. *La Rivista* ADIR, 2003. Disponível em < http://www.adir.unifi.it/rivista/2003/tavassi/cap3.htm > acesso em 02 de março de 2022.

[17] O "Informe Kaspersen" elaborado pelo Conselho da Europa, referente à Implementação da Recomendação R (89-9), já continha a ideia de se constituir um ato normativo mais efetivo que as Recomendações e apontava para necessidade de uma Convenção internacional. (Eilberb, Daniela Dora e outros. **Os cuidados com a Convenção de Budapeste**. Revista Eletrônica JOTA, 08.7.2021. Disponível em < https://www.jota.info/opiniao-e-

Recomendação sobre Crimes de Informática (R 89-9), adotada em 09 de setembro de 1989. Assim, a Itália, passou a adaptar sua legislação interna, especialmente, a penal, no sentido de tipificar algumas condutas envolvendo fraude por meios de informática, danos a dados e programas de informática, acesso e interceptação indevida de sistema informática e violação autoral de programas de computadores.[19]

Como fruto desta Recomendação de 1989 (R-89-9), em 23 de dezembro de 1993, foi aprovada a Lei n. 547 que alterou o Código Penal e de Processo Penal italianos.[20]

Na ocasião, o Parlamento italiano adotou um método evolutivo e adaptou a legislação preexistente e fez inserir novos tipos penais nos diversos capítulos do código penal com base em alguma semelhança existente.[21] Assim, foram tipificadas as condutas de danificar ou destruir sistemas informáticos ou telemáticos de utilidade pública (art. 420), o acesso abusivo aos sistemas informáticos ou telemáticos (art. 615-*ter*), a detenção e difusão abusiva de código de acesso de sistema informático ou telemático (art. 615-*quater*), a difusão e entrega de programa para danificar sistema informático ou telemático (art. 615-*quinquies*), interceptar, impedir ou interromper indevidamente a comunicação informática ou telemática (art. 617-*ter*), instalar dispositivos para interceptação (art. 617-*quinquie*), falsificar, alterar ou suprimir o conteúdo de comunicação informática ou telemática (art. 617-*sexies*), destruir ou deteriorar ou tornar inútil sistemas informáticos ou telemáticos, programas, informações ou dados de terceiros (art. 635-*bis*), de fraude por meio de informática (art. 640-*ter*), ainda ampliou o conceito de correspondência para incluir aquelas realizadas por meio informáticos, telemáticas, ou por qualquer outra forma de comunicação à distância (art. 616), assim como definir que, para fins de criminalização do crime de revelação de conteúdo de documento, inclui qualquer suporte informático que contenha dados, informações ou programas (art. 621) e ampliar o conceito de comunicação e conversas para incluir a transmissão de sons imagem ou outros dados (art. 623-*bis*).

analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/os-cuidados-com-a-convencao-de-budapeste08072021 > acesso em 09 de março de 2022).

[19] TADDEI, Sara. ***Le norme vigente sui reati telematici***. Filo Diritto, 04 de agosto de 2015. Disponível em < https://www.filodiritto.com/le-norme-vigenti-sui-reati-telematici > Acesso em 15 de fevereiro de 2022.

[20] Disponível em < https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1993-12-23;547 > Acesso em 10 de fevereiro de 2022.

[21] CONTRAFATTO, Vania. ***I reati informatici.*** Obra citada, p. 20.

Por meio da mesma lei, foram alterados dois artigos do Código de Processo Penal italiano sobre interceptação telefônica de modo a abranger a interceptação de fluxo de comunicações

por meio de sistemas de informática ou telemática, nos mesmos casos admitidos para interceptação telefônica, além de estender a medida para os crimes cometidos com uso de sistema de informática ou telemática (art. 266) e ainda regulamentar o acesso e exame da prova produzida por meio de interceptação de fluxo de dados (art. 268, 3-*bis*).

Como visto, passado menos de dois anos, foi elaborada uma nova Recomendação (R-95-13) pelo Conselho da Europa, mas houve resistência na sua adoção. Ainda assim, ocorreram alguns avanços na legislação interna italiana relacionados ao tema da cibercriminalidade e temas correlatos, como, por exemplo, o Decreto Legislativo n. 169, de 06 de maio de 1999, relativo à tutela jurídica dos bancos de dados que conferia maior proteção jurídica aos dados pessoais armazenados em sistemas informáticos. Outro exemplo, específico no campo penal, foi a Lei n. 269, de 03 de agosto de 1998 que tipificou a pornografia infantil distribuída, divulgada ou publicada "por qualquer meio, inclusive por via telemática" (art. 600-ter Código Penal).

A resistência aos termos da Recomendação 95-13 intensificou, por parte do Conselho da Europa, a realização de reuniões, grupos de estudos e discussões sobre o tema da cibercriminalidade, envolvendo a Organização das Nações Unidas e culminando com a realização da Convenção de Budapeste no ano de 2001.

2.2. A legislação italiana sobre a cibercriminalidade a partir da Convenção de Budapeste

A Convenção de Budapeste é o primeiro acordo internacional sobre cibercrime. Como anteriormente mencionada, foi precedida de diversas reuniões e estudos ocorridos entre os anos 1997 e 2000, tanto no Conselho da Europa como na ONU, sendo aberto para assinaturas em novembro de 2001 e com entrada em vigor em julho de 2004, após a ratificação por cinco países. Conforme exposto em seu preâmbulo, o seu objetivo é um avanço na busca de uma política criminal comum que objetiva a proteção da sociedade contra a cibercriminalidade e

crimes de informática, principalmente através da adoção de uma legislação adequada ao combate desta espécie de crime e do fomento da cooperação internacional entre os países signatários ou convidados.

A Convenção é composta por 48 (quarenta e oito) artigos com orientações sobre Direito

Penal, Processo Penal e Cooperação Internacional e foi suplementada por um Protocolo Adicional sobre atos racistas e xenofóbicos cometidos por meio de sistemas de computador e internet.

Os principais aspectos jurídicos da Convenção, que devem ser adotados pelos países signatários são: *i*) a determinação da criminalização das condutas de acesso indevido a dados, interferência fraudulenta nos sistemas de informática, violação de direitos autorais e pornografia infantil; e *ii*) a criação de instrumentos processuais para investigar cibercrime e obter provas eletrônicas em relação a qualquer crime; *iii*) o compromisso com a cooperação internacional.

Ao estabelecer um rol de infrações penais, pretendeu-se simplificar a persecução penal pela harmonização das legislações, de modo a evitar que o delito informático cometido em um país não encontrasse tipificação em outro. A adoção da Convenção não impede, porém, a criação de outros crimes distintos na legislação de cada país subscritor.[18]

Apesar de sua extensa regulamentação normativa, considera-se como principal aspecto positivo da Convenção, a política de incentivo à cooperação internacional entre os países signatários com compartilhamento de informações e tecnologias referentes ao combate a cibercriminalidade.

A partir da Convenção, no âmbito do Conselho da Europa, foi criado um Comitê da Convenção sobre Crimes Cibernéticos (T-CY), que monitora a implementação da Convenção pelos países signatários, o Programa Escritório para Crimes Cibernéticos (C-PROC), localizado em Bucareste, Romênia, que permite aos profissionais dos países signatários (e convidados) o compartilhamento de experiências e a criação de relacionamentos que facilitam a cooperação internacional, além de desenvolver programas para capacitação profissional, como o projeto GLACY (Ação Global contra Cibercrimes).[19]

Com a Convenção de Cibercrime concluída e assinada pela Itália, foram iniciados os trabalhos internos no Parlamento italiano para alteração de sua legislação, adotando-se quase que integralmente os conceitos e definições trazidos no acordo internacional.

O principal fruto deste trabalho foi a Lei n. 48, de 18 de março de 2008 (publicada em 04 de abril do mesmo ano), executiva da Convenção da Budapeste, que introduziu significativas

---

[18] CRESPO, Marcelo. **Crimes Digitais**. Obra citada, p. 132.

[19] **A Convenção de Budapeste sobre Cibercrime: benefícios e impacto na prática –** Relatório do Conselho da Europa – disponível em < https://www.coe.int/en/web/cybercrime/the-budapest-convention > acesso em 10 de fevereiro de 2022.

modificações no Código Penal e Processo Penal italianos; no Decreto Legislativo n. 231, de 08 de junho de 2001 (Responsabilidade Administrativa das Empresas) e no Decreto Legislativo n. 196, de 30 de junho de 2003 (Código de Privacidade).[20]

No Código Penal italiano foram criados ou aprimorados tipos penais para inserir, por exemplo, a falsidade nas declarações para assinaturas eletrônicas juntos aos serviços de certificação digital (art. 3). Além de aprimorar a legislação penal sobre acesso indevido, danos informáticos ou aos sistemas de informação e telemáticos, bem como aos programas e tratamento ilícito de dados públicos ou privados armazenados ou em fluxo de informações, com a alteração das penas aplicáveis a diversos delitos (arts. 4, 5, 6 e 7).

Posteriormente, houve complementação pela Lei n. 12, de 15 de fevereiro de 2012 (com entrada em vigor em 09 de março de 2012) com a adoção de medidas cautelares privadas referente ao combate à cibercriminalidade. A referida lei modificou o art. 240 do Código Penal italiano, tornando obrigatório o confisco de bens de informática ou telemática utilizado no cometimento de crimes informáticos específicos, sendo que os artigos seguintes disciplinaram a autorização judicial para faculdade de uso e a destinação de tais bens pela polícia ou outros órgãos estatais em casos de investigações sobre cibercrimes. Em 29 de outubro de 2016, foi publicado o decreto legislativo nº 202, com nova alteração do art. 240, sobre a obrigação de congelamento e confisco de bens, dinheiro ou rendimentos que possam caracterizar proveito de crimes informáticos específicos praticados dentro da União Europeia.

A legislação italiana possui previsão de responsabilidade administrativa para pessoa jurídica por crimes de informática cometidos por seus funcionários ou diretores em seu benefício. A disciplina da matéria encontra-se no decreto legislativo nº 231, de 08 de junho de 2001 que prevê as hipóteses de responsabilização, as punições, inclusive a interdição da atividade da empresa envolvida, além de algumas hipóteses de exclusão da responsabilidade.[21] Alvo de algumas críticas, especialmente em razão da carência de definições técnicas mais precisas, a legislação italiana sobre cibercriminalidade é abrangente e atende as diretrizes da Convenção de Budapeste.[22]

---

[20] Disponível em < https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2008-03-18;48!vig= > Acesso em 12 de fevereiro de 2022.

[21] FOLTRAN, Francesco. ***Reati informatici del dependente: quando è responsabile anche il datore di lavoro?*** Disponível em < https://www.smartius.it/data-it-law/guida-reati-informatici-azienda/reati-informaticidipendente-responsabile-datore-lavoro/ > Acesso em 12 de março de 2022.

[22] BUCCINI, Alfonso. ***La Legge 48/2008 a dieci anni dalla pubblicazione***. 2018. Centro Studi Informatica

3. Os atos normativos brasileiros sobre a cibercriminalidade

3.1. A ausência de normas regionais sobre cibercriminalidade na América do Sul

Diferentemente do que ocorre na Europa, inexiste um bloco continental coeso unindo os países que compõem a América do Sul. Diferenças político-ideológicas momentâneas, desconfianças históricas e assimetria entre as economias dos países impedem a formação ou continuidade de um bloco continental na região.[23] Nos últimos trinta anos, foram formados três grupos na região. O mais longevo é o MERCOSUL (Mercado Comum do Sul), bloco econômico, formado inicialmente por Brasil, Argentina, Paraguai e Uruguai em 1991, através do Tratado de Assunção. Os outros são a UNASUL e o PROSUL.

Em 2008, foi criada a UNASUL (União das Nações Sul-Americanas), por doze países sul-americanos. A UNASUL foi formada quando vários dos países eram governados por políticos liberais. Com a posterior alteração do quadro político nesses países, em 2018, o grupo se desintegrou com um pedido conjunto de suspensão da participação por vários países, inclusive do Brasil que iria assumir a presidência do grupo.

Os mesmos países que deixaram de pertencer formalmente a UNASUL criaram outro grupo continental, o PROSUL (Foro para o Progresso da América do Sul), formalizado por meio da Declaração de Santiago, em 22 de março de 2019, assinada por oito países: Brasil, Argentina, Chile, Colômbia, Equador, Guiana, Paraguai e Peru.

Um dos países que não assinou a Declaração de Santiago para criação do PROSUL foi o Uruguai. Na ocasião, retratando a dificuldade de integração entre os países sul-americanos, o vice-chanceler Ariel Bergamino afirmou:[24]

> Não assinaremos porque não acreditamos realmente que os problemas colocados pelos processos de integração sejam resolvidos com a criação de novos órgãos (...) foi dito que a UNASUL sofre de 'ideologização extrema', quando se pode realmente perguntar: o PROSUL também não tem uma conotação ideológica.

Giuridica – Observatorio di Bologna (CSIG Bologna). Disponível em < https://www.csigbologna.it/referenze/giurisprudenza/la-legge-48-2008-a-dieci-anni-dalla-pubblicazione/ > Acesso em 02 de março de 2022.

[23] Fabeiro. Valentina e outros. **Segurança Regional no Mercosul**. *Revista de La Facultad de Derecho (online)*, Montevideo: Uruguai, nº 50, jan-jul. 2021, p. 14.

[24] **PROSUL: Entenda o novo bloco sul-americano**. Politize! Disponível em < https://www.politize.com.br/prosul/ > Acesso em 20 de fevereiro de 2022.

A ausência de um compromisso estável retrata a dificuldade de realizar a integração política e social dos países sul-americanos.

Diante desse quadro, o MERCOSUL prevalece como principal elo de cooperação entre os países da América do Sul. Inspirado no Mercado Comum da União Europeia,[25] o Mercosul foi formado inicialmente por Brasil, Argentina, Paraguai e Uruguai em 1991, através do Tratado de Assunção. Posteriormente, em 2006, a Venezuela aderiu ao tratado constitutivo, mas, em dezembro de 2016, com base no Protocolo de Ushuaia, foi suspensa – com prazo indeterminado – por descumprir compromisso da plena vigência das instituições democráticas. Integram ainda o MERCOSUL, na condição de associados, os demais países da América do Sul: Bolívia, Chile, Peru, Colômbia, Equador, Guiana e Suriname.

Apesar de constituir um bloco econômico, o MERCOSUL passou a assumir outras agendas, constando inclusive com Reuniões de Ministros e Altas Autoridades sobre temas como Desenvolvimento Social, Educação, Meio Ambiente, Direitos Humanos, Justiça entre outros. Além disso, possui Grupos de Trabalhos, vinculado ao Conselho do Mercado Comum, sobre Cooperação Internacional e até um Grupo de Agenda Digital. Com o tempo, o Mercosul assumiu a interlocução política e, atualmente, trata de assuntos que vão além das questões econômicas e aduaneiras.

Durante os anos de sua existência foram editados mais de duas centenas de acordos intergovernamentais sobre diversos temas, mas apenas sete são sobre matéria criminal e nenhum deles aborda o tema da cibercriminalidade.[26] Apenas em 2015, por ocasião da XLIX Reunião Ordinária do Conselho do Mercado Comum do Mercosul, foi destacada a importância de reuniões de autoridades sobre privacidade e segurança da informação, visando a proposição de políticas de iniciativas comum na área de segurança cibernética, privacidade, proteção de dados pessoais, confiança no uso da *internet*, prevenção e combate à cibercriminalidade, mediante estratégias e políticas de promoção de coordenação local e regional respeitando a particularidade dos Estados Parte. Não obstante, essas reuniões, denominadas RAPRISIT,

---

[25] Accioly, Elizabeth. **Mercosul e União Europeia Estrutura Jurídico-Institucional**. Juruá Editora, 2010, 4ª ed, p. 114.

[26] Fabeiro. Valentina e outros. **Segurança Regional no Mercosul**. *Revista de La Facultad de Derecho (online)*, Montevideo: Uruguai, nº 50, jan-jul. 2021, p. 12-3.

embora importantes, possuem características mais voltadas a questões técnicas com alcance jurídico inexistente.[27]

Além disso, o arranjo político institucional de alguns países do MERCOSUL, inclusive do Brasil, impede a criação de um poder supranacional, permitindo apenas a implementação de modelos intergovernamentais, dificultando a internalização das normativas regionais e inviabilizando a plena integração entre os países.[28]

Sem uma imposição supranacional, o Brasil demorou para regulamentar as questões envolvendo os crimes informáticos e a cibercriminalidade. O Código Penal brasileiro, até o ano de 2012, não fazia qualquer referência a computadores, rede de computadores, internet etc.

Como recordou Vladimir Aras em artigo escrito nos idos de 2001: [29]

> A Internet, na sua feição atual, é uma 'criança' em fase de crescimento bastante acelerado. Sua principal *interface*, a *WWW — World Wide Web* surgiu na década de 1990. Sucede, porém, que o Código Penal em vigor no Brasil (parte especial) data de 7 de dezembro de 1940. Naquela época, mal havia telefones e rádios nas residências. A televisão ainda não havia sido inventada. Como pretender, então, que essa legislação criminal se adeque aos novíssimos crimes de informática?

O desenvolvimento da informática e das tecnologias de fluxo de informação e comunicação impactou a sociedade brasileira com mais intensidade no início dos anos 1990, tornando necessária a criação de leis penais sobre o tema.

Ocorre que a tramitação legislativa é tradicionalmente lenta em razão da sua ritualística procedimental e muitas vezes esta lentidão, no Brasil, é agravada por fatores políticos. Ainda assim, em 1997, foi criada a primeira lei (extravagante) que tratava de forma precária e indireta das novas tecnologias.[30] A Lei 9.459, de 13 de maio de 1997, criava uma causa de aumento para o crime de racismo, caso a conduta fosse praticada "por intermédio dos meios de comunicação social ou publicação de qualquer natureza" (art. 20, § 2º). No mesmo ano, a Lei 9.504, de 30 de setembro, sobre o processo eleitoral, criou os primeiros crimes informáticos

---

[27] Deluca, S; Del Carril, E. ***Cooperación Internacional em Materia Penal en el MERCOSUR: El Cibercrimen***. Revista da Secretaria do Tribunal Permanente de Revisão: Ano 5, nº 10; outubro de 2017, Assunção: República do Paraguai, p. 24-6.

[28] Accioly. Elizabeth. **Mercosul e União Europeia**. Obra citada, p. 148. A autora recorda: "Nos Estados-membros da União Europeia, as Constituição contêm dispositivos que aceitam a delegação do exercício de certas competências para um poder supranacional, e isso é necessário porque, como vimos, o Direito da União prima sobre o Direito Nacional, donde se conclui que os Estados-membros devem ter mecanismos para recepcionar e acatar as leis comunitárias, que atuam nos limites por eles delegados" (p. 146).

[29] ARAS, Vladmir. **Crimes de informática: Uma nova criminalidade**. Disponível em < https://jus.com.br/artigos/2250/crimes-de-informatica > acesso em 17 de fevereiro de 2022

[30] SYDOW. Spencer Toth. **Curso de Direito Penal Informático – Parte Geral e Especial**. 2ª Ed. Salvador: Editora JusPodivm, p. 253.

próprios na legislação brasileira. A redação do art. 72, incisos I e II, fez referência expressa a "sistema de tratamento automático de dados (usado pelo sistema eleitoral)" e "programa de computador" (capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral)".

Não deixa de ser curioso o fato de a primeira tipificação penal sobre acesso ilegítimo à sistema ou programa de computador no Brasil esteja relacionada, não à proteção dos interesses individuais dos cidadãos, mas sim do pleito político-eleitoral.

Em continuidade, a Lei 9.983/2000, acrescentou os artigos 313-A e 313-B no Código Penal que pune a exclusão ou alteração indevida de dados em sistemas informatizados ou bancos de dados da administração pública e a alteração do próprio sistema de informações ou programas de informática. Os crimes em comento foram inseridos na parte do Código Penal em capítulo referente aos crimes praticados por funcionários públicos, portanto, com alcance restrito.

Em 2008, a Lei 11.829 alterou a redação do Estatuto da Criança e do Adolescente (Lei 8.069/1990) para criminalizar diversas condutas, inclusive divulgar "através de sistema informático ou telemático" registro contendo sexo ou pornografia envolvendo criança ou adolescente (art. 241-A). Inclusive a "armazenagem" do conteúdo foi criminalizada, o que foi considerado um grande avanço no combate à pedofilia no Brasil.[31]

Após um início tímido no tratamento aos crimes de informática, com a publicação da Lei 12.737/2012, que entrou em vigor no ano seguinte, foi finalmente alterado o Código Penal com a criminalização do acesso indevido a dispositivo informático (art. 154-A). Nesse aspecto, foram consideradas típicas várias condutas relacionadas a dispositivos ou programas de computador e a idealização e desenvolvimento de programas ou dispositivos que permitissem a invasão de dispositivos informáticos (art. 154-A, § 1º). A mesma lei alterou o art. 266 do Código Penal para incluir, no crime de perturbação ou interrupção de serviço telegráfico e telefônico, os serviços informático, telemático e de informação. Além de alterar o art. 298, para equiparar o cartão de crédito ou débito a documento particular, no crime de falsidade.

A Lei 12.737/2012 foi aprovada com alguns anos de atraso em relação a outros países da América do Sul[32] e frustrou uma parte dos estudiosos que aguardavam um texto mais preciso e

---

[31] PECK, Patrícia. **Direito Digital**. 7ª Ed. 2021. São Paulo: Saraiva, p. 398.

[32] A Argentina possui lei específica sobre os crimes informáticos desde 2008, Lei 26.388, de 24 de junho; a Colômbia desde 2009, Lei 1273, de 05 de janeiro; o Chile desde 1993, Lei 19.223, de 07 de junho.

técnico. A tramitação de um dos projetos de lei sobre o tema foi acelerada, o que impediu um maior debate. Na época, houve uma pressão da mídia decorrente de um caso de acesso indevido aos arquivos do computador pessoal de uma atriz de telenovelas com posterior divulgação de fotos íntimas na internet.[33] O escândalo ensejou um esforço legislativo ímpar que buscou aplacar o descontentamento da opinião pública e a cobrança da mídia. Apenas onze dias após os fatos serem noticiados, foi aprovada a Lei 12.737/2012.[34]

A doutrina afirmou que a aprovação da lei "se deu de forma açodada e em completo descompasso com as iniciativas de outros países, especialmente, com as diretrizes da Convenção de Budapeste."[35]

Em outro estudo, a lei foi classificada como: [36]

> altamente atécnica, possuindo elementos do tipo e até mesmo núcleos do tipo extremamente mal escritos. O legislador mal assessorado termina por aprovar e promulgar leis com expressões totalmente equivocadas ou com excesso de elementos, de modo que sua aplicação se torna impossível. Veja-se o art. 154-A e suas 7 (sete) expressões que compõem a primeira parte, tornando-o, na prática, algo quase inaplicável.

Recentemente, a Lei 14.155/2021 alterou a redação do art. 154-A e aumentou significativamente as penas do crime que passaram de 03 (três) meses a 01 (um) ano de detenção para 01 (um) a 04 (quatro) anos de reclusão, podendo chegar a 05 (cinco) anos, "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 mesma lei, finalmente, ao acrescentar o § 2º-A ao artigo 171 do Código Penal, criou o crime de fraude eletrônica na legislação brasileira que ocorrerá quando a conduta for praticada "com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo". Ainda criou uma causa de aumento quando o servidor utilizado no crime estiver localizado fora do território nacional (§ 2º-B).

---

[33] "**Lei Caroline Dieckmann" sobre crimes na internet entra em vigor**. Tilt/UOL, 02 de abril de 2013. Disponível em < https://www.uol.com.br/tilt/noticias/redacao/2013/04/02/lei-carolina-dieckmann-sobre-crimesna-internet-entra-em-vigor.htm > acesso em 06 de março de 2022.

[34] Emerson Wendt descreve com perfeição como se deu a cobertura midiática e sua provável influência na tramitação e aprovação legislativa em ***ESPALDA JUSTICIERA: DELITOS INFORMÁTICOS*** (Revista Mercopol. Ano XI, nº 11, 2018, p. 36-8).

[35] BARRETO, Alessandro Gonçalves e outros. **Cibercrimes e seus reflexos no Direito Brasileiro**. Salvador: Editora JusPodivm, 2020, p. 130.

[36] SYDOW. Spencer Toth. **Curso de Direito Penal Informático**. Obra citada, p. 81.

Em 23 de abril de 2014, entrou em vigor a Lei 12.965, o Marco Civil da Internet. Apesar de não possuir normas de direito penal material, permitiu o acesso aos registros e demais informações (registros de conexão, de acesso, dados pessoais e do conteúdo de comunicações) somente por autorização judicial (art. 10, § 2º). Enfim, entre outras coisas, o Marco Civil da Internet trouxe segurança jurídica ao tema da privacidade de dados pessoais, ao tempo em que passou a permitir o acesso, mediante ordem judicial, sobre os dados e informações relevantes para as investigações criminais.

A Lei 13.260/2016 equiparou a ato de terrorismo a conduta de sabotar o funcionamento de meio de comunicação ou de transporte, porto, aeroporto, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas, instalações de geração ou transmissão de energia, instalações militares, de exploração ou refino de petróleo ou gás, bancárias "servindo-se de mecanismos cibernéticos" (art. 2º, § 1º, IV).

Posteriormente, ocorreram novas mudanças no Código Penal, especificamente, relacionadas aos crimes de informática (impróprios) foram realizadas pelas Leis 13.718/2018 e 13.772/2018, as quais, respectivamente, incluíram o artigo 218-C que criminalizava "divulgação de cena de estupro ou de cena de sexo ou pornografia não consentida" e o artigo 216-B que criminaliza o "registro não autorizado de intimidade sexual".

Como é possível perceber, No Brasil, não existem muitas leis penais sobre crimes informáticos e cibercriminalidade e nem há uma sistematização da matéria. Quanto às leis processuais penais que abordem o tema de provas ou evidências eletrônicas (captação, validade, preservação etc.), são praticamente inexistentes, competindo às instâncias judiciais realizarem generosas interpretações sobre o tema para garantir alguma funcionalidade e segurança ao sistema jurídico.

Como exemplo, podemos mencionar a interpretação, aceita pela doutrina e jurisprudência sobre a validade da prova eletrônica - inclusive em processo penal - sob o argumento da inexistência de vedação expressa na legislação.[37] Não obstante, revela-se paradoxal a utilização como prova de um "documento em forma eletrônica", cuja criação ampara-se na Medida Provisória n. 2.200/2001, quando a Constituição brasileira veda a edição Medida Provisória relativa a processo penal (art. 62, § 1º, I, "b").[38] Por que motivo, afinal, ainda não alteramos o

[37] Peck, Patrícia. **Direito Digital**. Obra citada, p. 261-3.

[38] Apesar da referida Medida Provisória ter sido editada alguns meses antes da EC 32/2001 que textualmente vedou o tratamento de matéria de processo penal por este tipo de espécie legislativa, era consenso esta impossibilidade, mesmo antes da EC 32, com base no art. 68, § 1º, II, do texto constitucional que veda a delegação de matéria sobre

anacrônico art. 232 do Código de Processo Penal de modo a ampliar o conceito de documento, incluindo os chamados documentos eletrônicos? [39]

3.2. A expectativa com a recente adesão do Brasil à Convenção de Budapeste

Passados mais de vinte anos da celebração da Convenção de Budapeste sobre o cibercrime, o Brasil aderiu formalmente ao acordo internacional, com a aprovação do Decreto Legislativo 37/2021, em 16 dezembro de 2021. A adesão impõe a adoção de uma série de iniciativas do Poder Público, muitas delas no âmbito legislativo, pois a Convenção de Budapeste estabelece orientações no sentido de harmonizar a legislação interna a dos demais países aderentes.

Neste sentido, observando o texto da Convenção,[40] observa-se que traz definições específicas para "sistema de computador", "dado de computador" e "provedor" de serviço e estipula providências a serem realizadas no plano legislativo de direito penal, inclusive com determinação de responsabilidade penal da pessoa jurídica (art. 12).

A maioria das medidas legislativas requeridas já se encontra, bem ou mal, inserida em nossa legislação penal, mas sem a abrangência e sistematização definida na Convenção, pois, como se sabe, a legislação penal brasileira sobre crimes informáticos foi resultado de alterações pontuais, realizadas em momentos distintos.

O desafio maior, pensamos, será a adaptação da legislação processual penal, especialmente em relação às medidas legais para rastreamento, interceptação e obtenção de dados, tema chave da Convenção.[45] Como ressalvado acima, existem pouquíssimas leis que tratam do tema no Brasil e se trata de tema especialmente delicado, pois os instrumentos a serem adotados interferem em questões sensíveis, como possibilidade de acesso a dados pessoais, interceptação de comunicação, acesso ao tráfego de dados com acesso a informações sobre sites, aplicativos e provedores acessados, pessoas contactadas etc. Por outro lado, tais dados e informações

---

"direitos individuais". Neste sentido: LOPES, Maurício Antônio Ribeiro. **Princípio da legalidade penal: projeções contemporâneas**. Revista dos Tribunais: São Paulo, 1994, p. 129-130.

[39] Recentemente, a Min. Rosa Weber, do Supremo Tribunal Federal, em decisão liminar, suspendeu a vigência da MP 1.068/2021, que pretendia alterar o Marco Civil da Internet com reflexos no Direito Processual, *verbis*: "O art. 62, § 1º, b, da CF, a seu turno, passou a explicitar, afastando quaisquer dúvidas, a incompatibilidade da utilização de medidas provisórias para veiculação de matéria penal e processual penal. **O mesmo dispositivo constitucional, em verdadeira inovação, também vedou a edição de MP sobre tema processual civil**." A ação foi julgada prejudicada, pois a MP foi rejeitada pelo Congresso Nacional (ADI 6991 MC, DJe 17.9.2021 – destaques originais).

[40] Disponível em < https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1963474 > Acesso em 10 de fevereiro de 2022.

privadas podem se mostrar essenciais para investigação criminal, especialmente, nos casos de crimes de informática e cibercriminalidade.

Neste sentido, o texto da Convenção expressamente prevê a adoção de medidas como busca e apreensão de dados informáticos, com possibilidade inclusive tornar inacessíveis ou eliminar os dados acessados (art. 19º, 3, d); registro em tempo real de dados informáticos (art. 20º), interceptação de dados em tempo real, ou seja, medidas que afetam a individualidade pessoal de forma relevante.

A Convenção ainda prevê orientações sobre questão de competência e, por fim, estabelece as medidas a serem implementadas de modo a permitir a cooperação internacional, incluindo a realização de assistência mútua, inclusive, em caráter de urgência ("Rede 24/7")**.**

Não há um prazo assinalado para implementação das alterações. Assim, espera-se seja realizada adequada reflexão a permitir a elaboração de leis adequadas com assessoria de pessoas especializadas, pois são temas altamente técnicos e complexo que irão impactar significativamente a esfera da individualidade das pessoas.

O estabelecimento de um diálogo constante entre os operadores do direito, órgãos técnicos de setores públicos e privados e membros da academia seguramente auxiliará na criação de uma legislação penal e processual que atenda aos ditames da Convenção de Budapeste e insira o Brasil definitivamente no plano internacional de combate à cibercriminalidade, porém sem descuidar dos direitos e garantias fundamentais previstas na Constituição da República.

4. Conclusão

[45] PAOLETTI, Alessandro. ***La ricerca dela prova penale nell'era dele nuove tecnologie informative: Individuare ed acquisire la prova "statica" archiviata all'interno di un dispositivo elettronico***. Editore Key, Milano, 2020, p.
35.

A recente adesão do Brasil à Convenção de Budapeste não foi providência natural ou desinteressada. Decorreu de um conjunto de fatores que revelava o atraso do Brasil na implementação de medidas efetivas de prevenção e repressão à cibercriminalidade.

Conforme relatório da Internet *Organised Crime Threat Assessment - IOCTA*, de 2018, da Agência da União Europeia para a Cooperação Policial – Europol, "a falta de legislação adequada sobre crimes cibernéticos fez com que o Brasil fosse o alvo número um e a principal fonte de ataques *online* na América Latina; 54% dos ataques cibernéticos reportados no Brasil supostamente são originários de dentro do país". O documento ainda esclarece que, à semelhança dos Estados Unidos da América, o Brasil é um dos grandes hospedeiros de sites de *phishing* e uma das dez maiores fontes mundiais de ataques cibernéticos.[41]

A desatenção ao tema da cibercriminalidade e dos crimes informáticos, durante alguns anos, colocou o Brasil como um destaque negativo no cenário mundial,[42] fonte de perigo para as demais nações, para os seus próprios cidadãos e empresas que dependem diariamente da informática e dos sistemas de informação para consecução de suas atividades, obrigando as instituições públicas e privadas a realizarem um esforço conjunto para transformar esta realidade.

Nos últimos anos, o Brasil realizou uma série de mudanças legislativas que propiciaram maior segurança jurídica em relação a privacidade de dados e fluxo de dados na internet, como exemplos o Marco Civil da Internet e a Lei Geral de Proteção de Dados que tiveram grande impacto social. Associado a isso, foram realizadas alterações no plano de governança com a criação da Política Nacional de Segurança da Informação, pelo Decreto 9.637, de 26 de dezembro de 2018.

Como consequência, foi apresentada e tornada pública a Estratégia Nacional de Segurança Cibernética (E-Ciber), elaborada por mais de quarenta órgãos e entidades do governo, com a participação da iniciativa privada e do setor acadêmico.[43] A Estratégia foi aprovada pelo Decreto nº 10.222, de 05 de fevereiro de 2020 que impõe implementação das ações estratégicas previstas na E-Cyber, preenchendo importante lacuna no arcabouço normativo sobre segurança cibernética.

---

[41] *INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2018*. EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION, EUROPOL. Disponível em < https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessmentiocta-2018 Acesso em 03 de março de 2022.

[42] Em 2018, o Brasil ocupava o 70º lugar no Global Cybersecurity Index, da UIT. Disponível em < https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf > (pp. 63-64). Acesso em 07 de março de 2022.

[43] Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm > (Anexo). Acesso em 04 de março de 2022.

As medidas implementadas, no plano legislativo e institucional, produziram impactos imediatos na percepção da segurança relacionada aos sistemas de informação e telemática. Não por acaso, o Brasil pulou do número 70º no Raking Cybersecurity da UIT de 2018[44] para 17º em 2020, superando, inclusive, a Itália.[45]

Essencial, no entanto, prosseguir com as adaptações legislativas e institucionais. Neste sentido, importante nos próximos anos, realizar alterações legislativas que permitam o ajustamento da nossa legislação sobre cibercriminalidade e, para tanto, podem ser aproveitados algumas orientações previstas da legislação italiana.

Em especial, considerando nossa controvertida experiência com o tema da responsabilidade penal da pessoa jurídica,[46] a adoção da responsabilidade administrativa do ente jurídico por crime de informática vinculada a atuação de seu preposto quando houver algum proveito para ela, nos termos do decreto legislativo nº 231, de 08 de junho de 2001.[47]

Além das alterações legislativas referentes a medidas de busca e recolhimento de evidências eletrônicas, seria oportuno, pensamos, estabelecer a possibilidade de confisco concreto dos instrumentos de informática utilizados no cometimento de crimes informáticos próprios ou impróprios, nos termos admitidos pelo art. 240-*bis* do Código Penal italiano.[53] A determinação específica complementaria o disposto no art. 91, II, do Código Penal brasileiro e ocasionaria um desestímulo à pratica delitiva ou ao menos dificultaria, de alguma forma, a reiteração delitiva.

Enfim, o Brasil pode se aproveitar da experiência da Itália, signatária da Convenção de Budapeste há mais tempo, para potencializar os efeitos das mudanças legislativas que serão feitas em breve.

4.1. Considerações finais

---

[44] Global Cybersecurity Index, 2018, UIT. Disponível em < https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf > (pp. 63-64). Acesso em 07 de março de 2022.

[45] Global Cybersecurity Index, 2020, UIT. Disponível em < https://www.itu.int/dms_pub/itu-d/opb/str/D-STRGCI.01-2021-PDF-E.pdf > (p. 25). Acesso em 07 de março de 2022.

[46] PRADO, Luiz Regis. **Direito Penal do Ambiente**, 2005. São Paulo: Revista dos Tribunais, p. 144.

[47] Disponível em < https://web.camera.it/parlam/leggi/deleghe/01231dl.htm > acesso em 05 de março de 2022.

[53] Disponível em < https://www.gazzettaufficiale.it/dettaglio/codici/codicePenale/623_1_3 > acesso em 05 de março de 2022.

Os governos e empresas ao redor do mundo estão cada vez mais alarmados com a escalada de ataques cibernéticos que danificam ou mesmo bloqueiam serviços essenciais para as atividades da sociedade e começam a ser realizados em número e intensidade que podem levar ao colapso da sociedade se não forem combatidos.[48]

Em resposta, diante da ubiquidade da cibercriminalidade e dos crimes de informática, mostra-se adequada a utilização de estratégias comuns de combate à cibercriminalidade pelos países, incluindo a harmonização no plano legislativo e aumento da cooperação internacional, conforme proposto pela Convenção de Budapeste, de modo a permitir a identificação dos autores e assim impedir, tanto quanto possível, o cometimento desta espécie de crimes ou mesmo diminuir suas consequências.

O conhecimento e o compartilhamento de experiências bem-sucedidas tanto no campo normativo quanto no campo técnico, igualmente, podem auxiliar neste combate.

5. Referências bibliográficas

ACCIOLY, Elizabeth. **Mercosul e União Europeia Estrutura Jurídico-Institucional**. 4ª Ed. Curitiba: Juruá, 2010.

ARAS, Vladmir. **Crimes de informática: Uma nova criminalidade**. 2001. Disponível em < https://jus.com.br/artigos/2250/crimes-de-informatica >

BARRETO, Alessandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e seus reflexos no Direito Brasileiro**. Salvador: Editora JusPodivm, 2020.

BUCCINI, Alfonso. ***La Legge 48/2008 a dieci anni dalla pubblicazione***. 2018. Centro Studi Informatica Giuridica – Observatorio di Bologna (CSIG Bologna). Disponível em < https://www.csigbologna.it/referenze/giurisprudenza/la-legge-48-2008-a-dieci-anni-dallapubblicazione/ >.

[48] RIFKIN, JEREMY. **Sociedade com Custo Marginal Zero**. 2016. São Paulo: M.Books do Brasil Editora, p. 336.

CONTRAFATTO, Vania. ***I reati informatici***. Collana Direta da Gianni Reynaud. Diritto Penale Dell'Impresa. Milão: Key Editore, 2017.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Editora Saraiva, 2011, pp. 47-62).

DELUCA, S; DEL CARRIL, E. (2017). **Cooperación Internacional en Materia Penal el MERCOSUR: El Cibercrimen**. Revista da Secretaria do Tribunal Permanente de Revisão: Ano 5, Nº 10; outubro, 2017, pp. 13 – 28. Revista da Secretaria do Tribunal Permanente de Revisão: Assunção, República do Paraguai. Disponível em: <http://revistastpr.com/index.php/rstpr/article/view/266/359 >

FABEIRO. Valentina; VELOSO, Paulo Potiara de Alcântara; KALB, Christiane. **Segurança Regional no Mercosul**. Montevideo Revista de La Facultad de Derecho (online), nº 50, janjul. 2021.

FOLTRAN, Francesco. ***Reati informatici del dependente: quando è responsabile anche il datore di lavoro?*** Disponível em < https://www.smartius.it/data-it-law/guida-reati-informaticiazienda/reati-informatici-dipendente-responsabile-datore-lavoro/ >

LA GRECA, Federico Tavassi. ***Hacking e criminalità informática.*** *La Rivista* ADIR, 2003. Disponível em < http://www.adir.unifi.it/rivista/2003/tavassi/cap3.htm >.

LOPES, Maurício Antônio Ribeiro. **Princípio da legalidade penal: projeções contemporâneas**. São Paulo: Editora Revista dos Tribunais, 1994.

PAOLETTI, Alessandro. ***La ricerca dela prova penale nell'era dele nuove tecnologie informative: Individuare ed acquisire la prova "statica" archiviata all'interno di un dispositivo elettronico.*** Milão: Editore Key, 2020.

PECK, Patrícia. **Direito Digital**. 7ª Ed. São Paulo: Editora Saraiva, 2021.

PRADO, Luiz Regis. **Direito Penal do Ambiente**. São Paulo: Editora Revista dos Tribunais, 2005.

RIFKIN, JEREMY. **Sociedade com Custo Marginal Zero**. São Paulo: M.Books do Brasil Editora, 2016.

SBORDONI, Stefano. ***Web, Libertà e Diritto, aspetti di dirito positivo nella comunità virtuale***. 2014. Roma: IPZS - Istituto Poligráfico e Zecca dello Stato, Libreria dello Stato, 2014.

SYDOW. Spencer Toth. **Curso de Direito Penal Informático – Parte Geral e Especial**. 2ª Ed. Salvador: Editora JusPodivm, 2021.

_____ **Princípio da Dupla Presunção de Inocência no Direito Penal Informático**. São Paulo: Editora Revista dos Tribunais, Vol. 975, janeiro de 2017.

TADDEI, Sara. ***Le norme vigente sui reati telematici***. Filo Diritto, 04 de agosto de 2015. Disponível em < https://www.filodiritto.com/le-norme-vigenti-sui-reati-telematici >

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos: ameaças e procedimentos de investigação**. 1ª Ed. São Paulo: Editora Brasport, 2012.

_____ ***ESPALDA JUSTICIERA: DELITOS INFORMÁTICOS*** *in* Revista Mercopol. Ano XI, nº 11, 2018, p. 31-42. Disponível em < https://www.gov.br/mj/pt-br/acessoa-informacao/atuacao-internacional/foros-e-redes/revista-mercopol-ndeg-11-2018-paraguaycompressed.pdf >