18

Análise da proteção jurídica no ambiente virtual na legislação brasileira

Patrícia Macedo de Carvalho

Graduanda de Direito do Centro Universitário São Lucas.

Stefalyne Nascimento

Graduanda de Direito do Centro Universitário São Lucas

Marcelo Lima de Oliveira

Professor Mestre orientador Professor do Centro Universitário São Lucas

DOI: 10.47573/aya.5379.2.82.18

RESUMO

O presente estudo tem como objetivo analisar a questão dos crimes cibernéticos na realidade jurídica brasileira bem como a sua correlação com a proteção de direitos e garantias constitucionalmente tutelados, notadamente, o direito à privacidade e intimidade. Assim, buscou-se fazer um resgate histórico da evolução da internet para que se pudesse compreender a sua complexidade e a justificativa para a sua relevância na sociedade contemporânea. Demonstrou-se com o presente estudo que a proteção de dados foi o principal vetor para a criação da internet, contudo, demonstra-se que, dada as proporções que o sistema de informação assumiu na realidade, tem sido cada vez mais difícil manter o ambiente virtual seguro, haja vista o fluxo incessante de informações inseridas nos servidores operacionais da internet. Desta maneira, o Estado brasileiro não tem mostrado resultados positivos para a proteção de bens jurídicos tão caros e sensíveis para a sociedade. Para a realização do trabalho foi utilizada uma pesquisa básica, estratégica, descritiva e exploratória, com abordagem qualitativa e método hipotético-dedutivo. Utilizou-se o procedimento de pesquisa bibliográfica, documental e análise de situação.

Palavras-chave: crimes. cibernéticos. direitos. privacidade. intimidade.

INTRODUÇÃO

Na atualidade, verifica-se que cada vez os usuários de serviços de internet estão imersos em sites, aplicativos e programas os quais são utilizados dados pessoais para a personalização destes serviços. Contudo, em decorrência da popularização da internet ser fenômeno recente na sociedade brasileira, denota-se que, não raro, ocorrem problemas de toda ordem na utilização destes serviços e, para fins desta obra, especificamente questões relacionadas à privacidade no mundo digital.

A internet não é mais um ambiente sem lei. Em que pese ser um ambiente livre, percebe-se que cada vez mais se busca a regulamentação do uso e acesso, uma vez que se pretende tornar o ambiente em um local seguro, evitando invasões a arquivos pessoais armazenados em bancos de dados digitais e até mesmo acesso a dispositivos, como celulares e computadores.

Contudo, demonstra-se rotineiramente que o ambiente virtual possui uma série de armadilhas que podem comprometer o bem-estar dos usuários, como a captura de dados pessoais e a consequente utilização indevida destas informações, notadamente a divulgação de imagens íntimas e acesso a dados bancários (LÓSSIO, 2022).

Para a realização deste trabalho será utilizada uma pesquisa básica, estratégica, para que possa promover a modificação social baseada em estudos técnicos, descritiva, com foco em aprofundar as questões levantadas no estudo, exploratória, para que se possa conhecer melhor o tema na sociedade, com abordagem qualitativa. Utilizou-se o procedimento de pesquisa bibliográfica e documental.

Assim, a hipótese da presente obra é de que as leis nacionais a respeito dos crimes cibernéticos estão evoluindo paulatinamente, contudo, ainda se mostram insuficientes para o enfretamento efetivo deste problema que é um problema cada vez mais comum na realidade brasileira e mundial.

O objetivo geral desta pesquisa é identificar se a legislação brasileira protege efetivamente os direitos e garantias fundamentais em casos de crimes cometidos por meios cibernéticos. Os objetivos específicos consistem em compreender a história e evolução dos sistemas de informática no Brasil, para que se trace um paralelo com a evolução legislativa das questões relativas ao tema, bem como analisar de que forma os crimes cibernéticos se operam, como são investigados e qual a consequência jurídica para aquele que comete o ato ilícito penal em matéria cibernética.

DESENVOLVIMENTO.

Breve histórico da internet: de aparato militar à ferramenta civil

A internet foi criada em 1969, nos Estados Unidos da América, com o objetivo de permitir o armazenamento de informações e permitir a comunicação entre laboratórios de pesquisa do Departamento de Defesa Americano, ainda que houve algum ataque bélico às unidades americanas durante a Guerra Fria, iniciada em 1957. Nesta época, a ferramenta era denominada como ARPANET, conforme dicção de Briggs e Burke (BRIGGS & BURKE, 2004)

A ARPANET (Advanced Research Projects Agency Network; em português: Rede da Agência para Projetos de Pesquisa Avançada) funcionava por meio daquilo que se chamava de chaveamento de pacotes, que se trata da transmissão de informações entre dispositivos por meios de dados fracionados em pequenas partes, contendo a informação fragmentada até o momento da recepção pelo destinatária que reconstruiria o que foi transmitido pelo remetente, conforme estudo de (HAFNER & LYON, 2019).

Em 29 de outubro de 1969 houve o envio do primeiro e-mail, e na década de 1970 passou-se a ter pesquisas em diversas universidades, o que tornou o sistema da ARPANET difícil de ser gerenciado, razão pela qual o projeto ARPANET se dividiu em dois: ARPANET, para operações civis, e MILNET, para operações militares conforme diz Dermot Turing (TURING, 2019).

Os anos seguintes foram marcados pela soma de esforços de alunos e professores em armazenar informações no sistema e permitir o trânsito de informações, o que culminou em um sistema técnico denominado Protocolo Internet (Internet Protocol - IP),o qual as redes conectadas pelo endereço IP, que se trata de um sistema numérico presente em cada dispositivo de informações em uma rede para a comunicação, de modo que se identifica o hospedeiro da informação, além de informar a localização da rede, conforme Tim Wu (WU, 2012).

Em 1992 foi criado a World Wide Web (www), a qual se trata de uma rede mundial de documentos em formato inteligível à maquina e que são executados pelo sistema da Internet, e logo em seguida se criou o protocolo HTTPS (Hypertext Transfer Protocol Secure) que foi o primeiro sistema criado para a internet com o objetivo de se permitir transações financeiras e comerciais, de modo que se gerou a aproximação da sociedade civil para a internet na década de 1990. Em 2003, meio bilhão de pessoas estavam conectadas na internet, conforme aponta Johnny Ryan (RYAN, 2013).

No Brasil, por seu turno, os primeiros projetos relativos à internet surgiram a partir de 1988, a qual havia a conexão entre instituições estadunidenses e brasileiras. Somente em 1992

houve a abertura ao público, contudo, a infraestrutura primitiva e a ausência de investimentos somente permitiram a inserção do comércio na internet brasileira em 1995, conforme aponta Eduardo Vieira (VIEIRA, 2018).

Dados de 2021, obtidos por meio de pesquisa promovida pelo Comitê Gestor da Internet do Brasil (Comitê Gestor da Internet no Brasil, 2021), apontam que em 2020 o Brasil passou a ter 152 milhões de usuários de internet, e demonstrou que 81% da população com mais de 10 anos de idade têm acesso a internet nos domicílios, ainda que 90% dos lares das classes mais vulneráveis da sociedade se conectam à internet por meio do celular, uma vez que não dispõem de computador.

Foi apresentada no Senado Federal Proposta de Emenda à Constituição (PEC 41/2021) que insere a inclusão digital como direitos fundamentais na Constituição, pela Senadora Simone Tebet. A proposta até a data de publicação desta obra ainda não possui relator, e se encontra sob análise na referida casa legislativa.

Do direito à intimidade e privacidade

Os Direitos à intimidade e privacidade são protegidos constitucionalmente, conforme previsão constante no Art. 5º, X, da Constituição Federal (BRASIL, 1988), razão pela qual se trata de um direito fundamental. Importa trazer a obra de Gilmar Mendes e Paulo Branco (MENDES & BRANCO, 2022) a qual diz o seguinte:

> O catálogo dos direitos fundamentais vem -se avolumando, conforme as exigências específicas de cada momento histórico. A classe dos direitos que são considerados fundamentais não tende à homogeneidade, o que dificulta uma conceituação material ampla e vantajosa que alcance todos eles. Tampouco a própria estrutura normativa dos diversos direitos fundamentais não é coincidente em todos os casos.
>
> (...)
>
> Os direitos e garantias fundamentais, em sentido material, são, pois, pretensões que, em cada momento histórico, se descobrem a partir da perspectiva do valor da dignidade humana.
>
> (MENDES & BRANCO, 2022, p. 280 e 282)

Nesta esteira, convém expressar o que consiste em Direito à Privacidade e Intimidade. Para Nathalia Masson (MASSON, 2016, p. 218) traz importe posicionamento a respeito da privacidade:

> A privacidade representa a plena autonomia do indivíduo em reger sua vida do modo que entender mais correto, mantendo em seu exclusivo controle as informações atinentes à sua vida doméstica (familiar e afetiva), aos seus hábitos, escolhas, segredos, etc., sem se submeter ao crivo (e à curiosidade) da opinião alheia. (MASSON, 2016, p. 218)

A intimidade, por sua vez, considera naquilo que é referente ao modo de ser da pessoa, de modo que os demais da sociedade são excluídos ao acesso do objeto íntimo, conforme aponta Guilherme Peña de Moraes ((DE MORAES, 2018).

Importa destacar contudo, que não se trata de direito absoluto. Razão pela qual trazemos à discussão a valiosa lição de Robert Alexy (ALEXY, 2015), a qual traz a teoria das esferas para o debate. De acordo com o mencionado autor, existem três esferas de proteção aos direitos fundamentais.

A esfera mais interna tutela a liberdade humana, e se trata de um núcleo protegido em sua totalidade, uma vez que dispõe de matérias que não devem chegar ao conhecimento alheio, em razão de sua delicadeza. O outro círculo é a esfera privada ampla, que admite a interação com outros indivíduos, ainda que se trate de assunto reservado; por fim, existe a esfera social, que alcança tudo aquilo que não for protegido pelas esferas anteriores.

Importante destacar esta afirmação uma vez que não há direito absoluto, contudo, é necessário destacar que o não absolutismo não configura ausência de tutela, mas, apenas que o exercício deste direito sofre limitações a depender do caso em que se esteja discutindo. Assim, importa mencionar que pessoas famosas e públicas possuem direito à intimidade e privacidade como todos os seus pares sociais, contudo, há limitação em razão do ofício em que exercem e pelo interesse público. Trazemos a dicção de Gilmar Mendes a respeito:

> A reclusão periódica à vida privada é uma necessidade de todo homem, para a sua própria saúde mental. Além disso, sem privacidade, não há condições propícias para o desenvolvimento livre da personalidade. Estar submetido ao constante crivo da observação alheia dificulta o enfrentamento de novos desafios. A exposição diuturna dos nossos erros, dificuldades e fracassos à crítica e à curiosidade permanentes de terceiros, e ao ridículo público mesmo inibiria toda tentativa de autossuperação. Sem a tranquilidade emocional que se pode auferir da privacidade, não há muito menos como o indivíduo se autoavaliar, medir perspectivas e traçar metas. (MENDES & BRANCO, 2022, p. 548)

No que se refere à privacidade e à intimidade, percebe-se que existe intensa (e justa) proteção constitucional e infraconstitucional. Conforme se observa no Capítulo I-A do Código Penal, o qual prever tipo penal de Registro não autorizado da intimidade sexual, no Art. 216-B, (BRASIL, 1940), por exemplo.

No tocante à privacidade na internet, denota-se que houve movimentação para a proteção aos dados pessoais na Europa com o Diretiva 95/46/CE, que dispõe sobre a proteção de dados pessoais e a circulação desses dados, a qual foi recentemente substituída pela General Data Protection Regulation (GDPR), que tem como objetivo estabelecer novos padrões e diretrizes para o uso e armazenamento de dados pessoais, uma vez que, não raro, ocorrem violações a direitos por uso indevido destas informações em várias áreas da sociedade, notadamente direitos do consumidor.

A proteção de dados na legislação brasileira

Como dito ao norte, há proteção constitucional à intimidade, privacidade e vida privada no ordenamento pátrio. Imperativo destacar que no ano de 2019 houve a aprovação de Proposta de Emenda Constitucional (PEC 17/2019), a qual incluía a proteção de dados pessoais no rol de garantias individuais.

Em 2018 foi publicada a Lei Geral de Proteção de Dados (LGDP), Lei 13.709/2018 (BRASIL, 2018), a qual dispõe a respeito da forma de uso e armazenamento de dados pessoais, notadamente os inseridos em mídias digitais, a qual se protege pessoa natural ou pessoa jurídica, de Direito Público e Privado, para que se promovesse a proteção de direitos fundamentais de liberdade e privacidade, de modo que se atribuiu uma série de responsabilidades, e suas respectivas sanções, aos gestores e usuários de dados pessoais, conforme aponta (JORGE, 2021).

Assim, demonstra-se que tem a proteção de dados na legislação nacional tem se mostrado uma preocupação para o Estado, uma vez que, com a mudança de realidade, as pessoas

tem passado cada vez mais tempo no mundo virtual, o que indica que novas condutas possam ser eventualmente lesivas e prejudiciais a determinados bem jurídicos, exigindo que seja dada a devida proteção.

A exemplo de violações a direitos no mundo virtual podemos citar o bullyng, porn revenge, racismo, pedofilia, furtos, entre outros. Com isto, nota-se que os meios tradicionais de repressão à criminalidade não têm se mostrado efetivos, razão pela qual se pugna pela atualização da legislação e das formas de torná-la efetiva.

Detecta-se que, em razão do grande volume de usuários, e a expansão massiva de informações veiculadas nas redes, o controle exercido pelas autoridades públicas é insuficiente, para não dizer irrisório. Ocorrem no ambiente virtual algumas práticas altamente danosas aos direitos individuais e coletivos, como por exemplo a invasão a sistema de dados, conhecido como *hacking, superzaping*, entre outras formas de prejuízo a nível pessoal ou institucional.

Ademais, é oportuno destacar que na rede mundial de computadores, existe uma rede paralela de circulação de dados, as quais comumente são realizados crimes cibernéticos, a saber: Deep Web e Dark Web.

Diante deste cenário, é pertinente trazermos à discussão o conceito de cibercrime. De início, cumpre mencionar que por se tratar de instituto jurídico recente, não existe definição precisa e pacífica a respeito do que vem a ser um crime cibernético. Para Garcia Martins (MARTINS, 2006), trata-se de ato em que o computador serve de meio para atingir um resultado crime, ou, ainda, onde o computador é alvo simbólico, ou ato em que o computador é objeto do crime.

Para Diana Simas (DE SIMAS, 2014), diz-se dos crimes cibernéticos:

> Podemos afirmar que associado a este fenômeno da criminalidade informática estão, sem dúvida, condutas violadoras de direitos fundamentais, seja através da utilização da informática para a prática de um crime, ou como um elemento do tipo legal de crime. Face a esta perspectiva, a criminalidade informática em sentido amplo, engloba toda a atividade criminosa que pode ser cometida através de meios informáticos. Em sentido estrito, são englobados os crimes quem que o meio informático surge como parte integradora do tipo legal, ainda que o bem jurídico protegido não seja digital. (DE SIMAS, 2014, p. 14)

Ademais, necessário trazer o conceito de Fabrício Rosa (ROSA, 2002):

> A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O 'Crime de Informática' é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o 'Crime de Informática' pressupõe does elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, [entre outros].

Lei 12.737 de 2012 – A Lei Carolina Dieckman

Em maio de 2011, a atriz Carolina Dieckmann sofreu atentado cibernético o qual resultou na captura de arquivos de mídia em formato de fotos e mensagens de texto, o qual se encontravam em situação de nudez e exposição de intimidades e o invasor exigiu o pagamento na quantia de R$ 10.000 reais para que não houvesse a publicação das mídias. Como não houve o pagamento, fez-se a divulgação clandestina de 36 fotos da atriz que rapidamente foram espalhadas por toda a internet, sendo hospedadas nos mais diversos bancos de dados de sites de conteúdo adulto e erótico.

No caso em questão, verificou-se intensa pressão de vários setores da sociedade civil para que houvesse resposta legislativa para o caso concreto. Cumpre destacar que mesmo antes da lei, a invasão de ambiente virtual e subtrair dados já era conduta tipificada na lei pena, contudo, não havia norma que tratava especificamente sobre a matéria, razão pela qual se operou a promulgação da referida lei (BRASIL, 2012).

Imperativo destacar que a previsão da lei não se limita somente ao sequestro de mídias e divulgação clandestina, conforme a exposição midiática à época fez parecer. A lei em comento tipifica três condutas. Tais sejam: 1) Art. 154-A - Invasão de dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa; 2) Art. 266 - Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública - Pena - detenção, de um a três anos, e multa; e 3) Art. 298 - Falsificação de documento particular/cartão - Pena - reclusão, de um a cinco anos e multa.

Importa destacar que a apreciação da violação ao bem jurídico quando resulta deste tipo penal somente se opera mediante representação do ofendido, ressalvados os casos em que o ofendido é a Administração Pública direta ou indireta, qualquer dos Poderes da União, Estados, Municípios e Distrito Federal, conforme aponta (SYDOW, 2022).

Lei nº13.718/2018

Conhecida como a lei da importunação sexual criminaliza atos libidinosos sem o consentimento da vítima além da divulgação de cena de estupro, de sexo ou de pornografia sem o consentimento de quem está participando da gravação, bem como daquele que se destina o envio.

A lei em comento surge diante de um cenário em que houve uma série de ocorrências sociais em que havia a gravação de cenas de sexo, com ou sem o consentimento dos envolvidos, e o envio desta mídia para terceiros de maneira não autorizada pelos filmados. A conduta em questão atenta contra a dignidade, uma vez que expõe de maneira desmedida a vida sexual dos envolvidos na prática do ato libidinoso.

Verificou-se, ao longo da década de 2010, a prática daquilo que se convencionou denominar de *revenge* porn em que o sujeito ativo do crime divulga material erótico do companheiro atual ou pretérito como forma de retaliação após o término de um relacionamento ou ocorrência de algum dissabor na relação. A prática se enquadra neste tipo penal.

Da apuração de crimes cibernéticos

A apuração de crimes mais frequentes na sociedade, como roubo, tráfico de entorpecentes, homicídios, já são suficientemente difíceis de se operar, ainda que se trate de violação corriqueira e há muito tempo assola a realidade de nosso país. Contudo, em decorrência da cada vez mais frequente informatização da sociedade, constata-se que um crescente aumento na ocorrência de crimes no ambiente virtual. Diante de um cenário pouco explorado, demonstra-se uma verdadeira dificuldade do Poder Público em investigar a ocorrência desta modalidade de crime.

De início, percebe-se que há uma verdadeira ausência de metodologia para a investigação destes delitos, uma porque há cada vez mais sistemas operacionais que permitem uma atuação furtiva do infrator, duas porque não há um compartilhamento de informações e dados entre os órgãos e organizações governamentais e não governamentais, além do elevado grau técnico que a ocorrência deste tipo de crime se opera, vê-se que nem sempre existe pessoal capacitado para lidar com eventos desta magnitude. Não o suficiente, demonstra-se o caso da extraterritorialidade do crime, conforme aponta França, Araújo e Taveira (FRANÇA, ARAÚJO, & TAVEIRA, 2018). Muitas das vezes um crime cujo resultado se deu em determinado país, foi realizado por sujeito ativo em um segundo país, utilizando de um servidor de um terceiro país.

Assim, percebe-se que há um verdadeiro óbice no que tange à identificação do infrator haja vista comumente se utilizar de sistemas cuja a localização do usuário seja camuflada e, até mesmo, alterada. Além de tudo, diariamente são depositadas incontáveis informações no sistema da internet, o que torna, até o momento, impossível a filtragem da legalidade de determinado conteúdo.

Dimas (DE SIMAS, 2014) aponta algumas soluções interessantes para amenizar a ocorrência de crimes cibernéticos. A autora destaca a importância do aumento de investimentos em combate ao cibercrime, isto porque, segundo a mesma o Reino Unido e os Estados Unidos, países com uma forte resposta ao crime informático, aplicam poucos recursos nos seus orçamentos que nas forças policiais atingem 12,3 milhões no Reino Unido e 79 milhões de dólares nos Estados Unidos.

Outra resposta da autora é a incrementação à informação, conscientização e preparo na defesa digital. De maneira que as empresas (a nosso ver, notadamente as que lidam com operações comerciais e gerenciamento de dados) possam se preparar e prever as ações criminosas a partir da consciência do problema e a implementação de medidas de segurança, além do investimento do setor público em investigação, com a especialização de pessoal qualificado para a apuração das práticas delitivas deste tipo.

No Brasil, a investigação destes crimes se opera de maneira rudimentar e manual, por mais das vezes, ainda que se tenha investido em infraestrutura nos últimos anos, a realidade é que o maquinário e os recursos humanos são escassos e pouco qualificados.

Assim, o primeiro procedimento a ser realizado quando diante de um fato possivelmente qualificado como crime cibernético é a identificação do meio empregado. Existem muitas formas de ocorrer um crime informático, podendo ocorrer por e-mail, salas de bate papo, aplicativos de mensageiro, serviços de relacionamento, páginas da web.

Após, é necessário que haja a preservação das provas obtidas como meio de se com-

provar a materialidade do fato criminoso. Assim, o primeiro passo que salvar e garantir os dados obtidos e, posteriormente, notificar o provedor para que sejam mantidos os registros no ambiente em que se deu o ocorrido, requerendo, na medida do possível a colaboração de todos os provedores envolvidos.

Com a identificação do crime e do meio empregado e tomadas as providências para o armazenamento das provas, é necessário atuar para a identificação dos responsáveis pelo serviço, seja nacional ou estrangeiro. Em havendo sido cometido através da extraterritorialidade, poderá ocorrer cooperação internacional, que há previsão em tratados e acordos internacionais a qual o Brasil é signatário.

Em seguida, é necessário que haja a violação de sigilo de dados telemáticos, nos termos da Lei 9.296 de 1996, (BRASIL, 1996). Com esta medida, o que se busca é a identificação do dispositivo o qual foi utilizado para a prática do crime, a partir do protocolo internet (IP) fornecido pelo provedor do serviço. Esta ocorrência se dá, quando em caso de crimes cometidos no Brasil, por meio de requisição de informações à concessionária de serviços telefônicos, pelo juízo.

Com todas estas informações, é necessário que a investigação incida para a comprovação da autoria e da materialidade do fato típico. Assim, poderão ser adotadas medidas para o melhor aproveitamento da investigação, como a busca e a apreensão do dispositivo eletrônico, com a necessária autorização judicial para que se proceda o acesso aos dados inseridos no dispositivo. A oitiva daquele que é contratante do serviço de internet utilizado para a operação criminosa, além de fotografias do local em que se deu a prática do crime. Com o dispositivo em posse dos investigadores, será realizada perícia nos dispositivos e materiais apreendidos.

A Lei de intercepção de dados telemáticos, Lei 9.296/1996, dispõe a respeito da possibilidade de se criar a uma espécie de conta paralela à original de modo que seja possível acessar os e-mails recebidos e enviados pelo investigado, além da gravação de todos os e-mails, bem como o acesso ao conteúdo da caixa postal e intercepção de todos os dados.

Importante mencionar que as principais dificuldades enfrentadas na apuração destas condutas são relacionas à legislação insuficiente sobre o assunto. No Brasil, a atividade legiferante ainda não conhece as particularidades que este tipo de conduta criminosa possui, de maneira que se legisla somente aquilo que é lugar comum, como divulgação de mídias sexuais, por exemplo.

Além disso, demonstra-se que não há um canal específico para a o recebimento de denúncias destes crimes, havendo comumente dupla investigação sobre o mesmo fato, o que gera prejuízo ao erário e a não proteção a outras pessoas também prejudicadas por este tipo de delito. Também, os sites hospedados em países estrangeiros são mais difíceis de se empreender medidas investigativas, ainda que haja ordem judicial para o cumprimento de diligências, o que demonstra que a cooperação internacional é deficitária.

CONSIDERAÇÕES FINAIS

Conforme todo o exposto na presente obra, constata-se que a realidade mundial caminha no sentido de que o mundo digital esteja cada vez mais inserido no dia a dia das pessoas, corporações e governos, de modo que é necessária uma regulamentação eficiente e atualizada

do uso e armazenamento de informações e dados nos sistemas informáticos. No Brasil, a tecnologia chegou com pelo menos 20 anos de atraso, considerando que a internet foi criada na década de 1960 e somente no final dos anos 1980 houve alguma movimentação para que houvesse a inserção desta nova realidade no cotidiano acadêmico e militar e, muito posteriormente, na rotina da sociedade civil.

A internet é vista por muitos como a grande responsável pelas transformações sociais nas últimas décadas, muito porque, em virtude de sua popularização nos últimos anos, viabilizou a mudança de paradigmas em todas as classes sociais, no sentido de que o mercado financeiro atualmente opera na velocidade dos fatos, não havendo um atraso relevante na transação das informações. A internet aproximou pessoas com as redes sociais, facilitou a comunicação por meio de mensageiros instantâneos e facilitou procedimentos mercantis, como mais recente a implementação do sistema de pagamentos e transação financeira pix.

No entanto, como já dito, é importante destacar que a legislação brasileira não é atenta às diversas possibilidades de cometimento de crimes por meios cibernéticos, isto porque parece existir somente uma visão tradicional de cometimento de crimes, não levando em consideração que existem diversos dispositivos conectados à internet que, se utilizados de maneira equivocada ou mal intencionada, poderão gerar prejuízos à vítima.

Existem sistemas de segurança que são majoritariamente operacionalizados por meio remoto, via internet, o que significa que poderia haver o cometimento de um crime de incêndio (Art. 250 do Código Penal) Atentado contra a segurança de transporte marítimo, fluvial ou aéreo (Art. 261 do Código Penal), violação de domicílio (Art. 150 do Código Penal), Furto (Art. 155 do Código Penal), Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (Art. 266 do Código Penal), entre tantos outros.

Assim, este universo digital exige uma regulamentação adequada para que a convivência neste ambiente se opere de maneira lícita e saudável a todos os envolvidos. É necessário que haja produção legislativa clara, objetiva e precisa sobre o tema, de maneira que não é útil, tampouco desejável que se legisle sobre tudo e que esta lei não atenda aos fins que se pretende. É necessário que os órgãos de investigação sejam devidamente equipados com material moderno e equipe técnica devidamente qualificada e atualizada, além de que deve haver investimento no sentido de se prevenir a ocorrência de delitos, não apenas se reprimir o mal causado.

No Brasil as principais leis sobre o assunto são insuficientes para a prevenção destes delitos e a repressão muitas vezes não ocorre, justamente pelos fatos e motivos acima expostos. Se na década de 1990 verificou-se a tipificação de crimes contra a propriedade industrial, na contemporaneidade, os crimes evoluíram à sofisticação de espionagem industrial, de modo que se afeta o funcionamento ordinário e correto de economia regionais e globais, uma vez que incidem sobre a atividade financeira de grandes corporações e governos.

É inegável os avanços trazidos pela internet e todo o aparato técnico que permite a sua utilização. Contudo, os problemas enfrentados não parecem encontrar soluções na forma em que se tem empreendido esforços. Rotineiramente direitos são violados com a divulgação de imagens pessoais em sites públicos, o vazamento de informações pessoais, como dados cadastrais e senhas de bancos, contas em aplicativos e outras informações relevantes e o ordenamento jurídico não parece trazer solução ao problema, o que demonstra que além de ineficaz

na proteção, o Poder Público não sabe como resolver a questão, ainda que temporariamente, embora o desejável seja uma resposta definitiva.

A Lei 12.737 de 2012 trouxe luz a uma problemática na realidade brasileira. Contudo, importa asseverar que dado o grau de sofisticação que a conduta exige para ser realizada, além do prejuízo, muitas vezes irreparável, à vítima, repara-se que as penas são, no mínimo, insuficientes, haja vista a pena máxima para os crimes previstos nesta lei é de 2 anos e multa, Art. 2º da mencionada lei que acresceu o Art. 154-A ao Código Penal, o que implica em dizer que se trata de crime de menor potencial ofensivo. A mera imposição de penas mais rígidas não tem o condão de diminuir a ocorrência destes crimes, mas ocorre que além da captura destes criminosos ser cada vez mais difícil, o resultado do esforço culmina apenas em uma pena que não é sequer inibidora da reiteração da conduta, o que é um indicativo de que a situação é preocupante.

REFERÊNCIAS

ALEXY, R. (2015). Teoria dos Direitos Fundamentais. São Paulo: Malheiros Editores.

BRASIL. (1940). DECRETO-LEI No 2.848, DE 7 DE DEZEMBRO DE 1940. Rio de Janeiro: Senado Federal.

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

BRASIL. (1996). Lei 9.296 de 24 de julho de 1996. Brasília: Senado Federal.

BRASIL. (2012). Lei 12.737 de 2012. Brasília: Senado Federal.

BRASIL. (2018). Lei Nº 13.709, de 14 de agosto de 2018. Brasília: Senado Federal.

BRIGGS, A., & BURKE, P. (2004). Uma história social da mídia: De Gutenberg à internet. São Paulo: Zahar.

Comitê Gestor da Internet no Brasil. (2021). Pesquisa Sobre o Uso das Tecnologias de informação e comunicação nos domicílios brasileiros. São Paulo: Comitê Gestor da Internet no Brasil.

DE MORAES, G. (2018). Curso de Direito Constitucional . São Paulo: Atlas.

DE SIMAS, D. (2014). O cibercrime. Lisboa: Universidade Lusófona de Humanidades e Tecnologias.

HAFNER, K., & LYON, M. (2019). Onde os Magos Nunca Dormem: a Incrível História da Origem da Internet e dos Gênios por Trás de sua Criação. São Paulo: Red Tapioca.

JORGE, H. (2021). Manual de educação digital, cibercidadania e prevenção de crimes cibernéticos - um guia para jovens, adultos, empresas, instituições e autoridade. Salvador: Juspodvim.

LÓSSIO, C. (2022). O direito e o ciberespaço. Salvador : Juspodivm.

MARTINS, G. (2006). Direito da Informática. Coimbra: Almedina.

MASSON, N. (2016). Manual de Direito Constitucional. Salvador: Juspodivm.

MENDES, G., & BRANCO, P. (2022). Curso de Direito Constitucional . São Paulo: Saraiva.

ROSA, F. (2002). Crimes de Informática. Campinas: Bookseller.

RYAN, J. (2013). A history of the Internet and the Digital Future. Londres: Reaktion Books.

SYDOW, S. (2022). Curso de Direito Penal Informático - Partes Geral de Especial. Salvador: Juspodivm.

TURING, D. (2019). A história da computação: do Ábaco à Inteligência Artificial. São Paulo: M Books.

VIEIRA, E. (2018). Os bastidores da internet: a história de quem criou os primeiros negócios digitais do Brasil. São Paulo: Manole.

WU, T. (2012). Impérios da comunicação: do telefone à internet, da AT&T ao Google. São Paulo: Zahar.