UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE CIÊNCIAS JURÍDICAS
FACULDADE DE DIREITO DO RECIFE
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

ARIADNÉE ABREU DE FRANÇA

LEGÍTIMA DEFESA DIGITAL:
uma estratégia de governança corporativa e *criminal compliance* para a preservação das empresas

Dissertação de Mestrado

Recife
2019

ARIADNÉE ABREU DE FRANÇA

LEGÍTIMA DEFESA DIGITAL:
uma estratégia de governança corporativa e de *criminal compliance* para a preservação das empresas

Dissertação apresentada ao Programa de Pós-Graduação em Direito do Centro de Ciências Jurídicas/Faculdade de Direito do Recife da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Mestre em Direito.

Área de concentração: Transformações do Direito Privado

Linha de pesquisa: Relações Contratuais Internacionais

Orientador: Prof. Dr. Paul Hugo Weberbauer

Recife
2019

Catalogação na fonte
Bibliotecária Ana Cristina Vieira CRB/4-1736

F814l França, Ariadnée Abreu de.
Legítima Defesa Digital: uma estratégia de governança corporativa e de criminal compliance para a preservação das empresas / Ariadnée Abreu de França. – Recife: O Autor, 2019.
82 f.

Orientador: Paul Hugo Weberbauer.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. Centro de Ciências Jurídicas. Programa de Pós-Graduação em Direito, 2019.
Inclui referências.

1. Legítima Defesa (Direito). 2. Segurança da Informação. 3. Direito Digital. I. Weberbauer, Paul Hugo (Orientador). II. Título.

343 CDD (22. ed.) UFPE (BSCCJ2019-20)

ARIADNÉE ABREU DE FRANÇA

LEGÍTIMA DEFESA DIGITAL:
uma estratégia de governança corporativa e de *criminal compliance* para a preservação das empresas

Dissertação apresentada ao Programa de Pós-Graduação em Direito do Centro de Ciências Jurídicas/Faculdade de Direito do Recife da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Mestre em Direito.

Área de concentração: Transformações do Direito Privado

Linha de pesquisa: Relações Contratuais Internacionais

Aprovada em: 11/02/2019

Prof º Dr. Paul Hugo Weberbauer (Orientador)

Universidade Federal de Pernambuco

Prof º Dr. Aurélio Agostinho da Bôaviagem (Examinador Interno)

Universidade Federal de Pernambuco

Prof ª Dra. Eugênia Cristina Nilsen Ribeiro Barza (Examinadora Interna)

Universidade Federal de Pernambuco

Prof ª Dra. Wanilza Marques de Almeida Cerqueira (Examinadora Externa)

Faculdade Nova Roma

AGRADECIMENTOS

Ao meu irmão mais novo, Stephann, por ter me dito, um certo dia, para não desistir.

A minha família paraibana, Gustavo, Lúcia, Vinicius, Stephann, Zork e Kiko por todo amor e por sempre incentivarem os meus projetos.

A minha família pernambucana, Diana, Martinha, Gutho, Nathália e Mel, por fazerem os meus dias em Recife-PE mais alegres e tranquilos.

Ao meu orientador, Professor Dr. Paul Hugo Weberbauer pela paciência, dedicação, confiança e amizade.

Aos meus professores, pelo carinho e por todos os ensinamentos valiosos que tive durante cada aula e cada conversa. Em especial, aos meus professores de linha de pesquisa, a Professora Dra. Eugênia Barza por fazer da sala de aula um “doce” ambiente de aprendizagem e ao Professor Dr. Aurélio Boaviagem por sempre nos estimular à curiosidade e à descoberta.

Aos meus colegas do PPGD/UFPE, por toda a amizade e generosidade.

A todos os amigos que carinhosamente contribuíram de alguma forma para a realização deste trabalho, meu muito obrigada!

"*O Universo não é uma ideia minha.*
A minha ideia do Universo é que é uma ideia minha.
A noite não anoitece pelos meus olhos,
A minha ideia da noite é que anoitece por meus olhos.
Fora de eu pensar e de haver quaisquer pensamentos
A noite anoitece concretamente
E o fulgor das estrelas existe como se tivesse peso."

Fernando Pessoa

RESUMO

O Direito Digital ajusta o mundo jurídico à realidade virtual, propiciando a adequação das normas aos fatores concretos de risco que traduzem as necessidades sociais vivenciadas na Era da Informação. Para combater a problemática gerada pela criminalidade digital, a impunidade e o prejuízo econômico, financeiro e social causado por estes delitos, precisamos adequar instituições e institutos jurídicos ao atendimento destas demandas. Na perspectiva de enfrentamento dos crimes digitais, a necessidade de proteção da informação e de outros ativos intangíveis ganham destaque e inspiram o tema proposto neste trabalho. Nesse sentido, apresentamos uma análise reflexiva sobre a aplicabilidade jurídica do instituto da legitima defesa digital com o propósito de incentivar a criação de políticas de segurança da informação e a regulação informática, tendo como objetivo garantir a atuação de grupos de resposta a incidentes em instituições públicas e privadas, como por exemplo, bancos, empresas e a própria Administração Pública consubstanciada nos seus órgãos. Para tanto, utilizamos o método dedutivo com escopo jurídico explícito na legislação pátria e nas diretrizes internacionais, a fim de, amparados por amplo acervo bibliográfico, delinear os limites de atuação com base nesta justificante, visto que se trata da mesma legítima defesa *stricto sensu*, o qual se difere desta última apenas em relação ao meio que será utilizada, qual seja o meio virtual, digital, ou não presencial.

Palavras-chave: Direito Digital. Legítima Defesa Digital. Segurança da Informação. Sociedade Digital.

ABSTRACT

The Digital Law adjusts the legal world to the virtual reality, propitiating the adaptation of the norms to the concrete factors of risk, that reflect the social necessities experienced in the Age of Information. To combat the problem generated by digital crime, impunity and economic, financial and social damage caused by these crimes, we need to adapt legal institutions and institutions to meet these demands. In the perspective of coping with digital crimes, the need to protect information and other intangible assets is highlighted and inspires the theme proposed in this paper. In this work, we present a reflexive analysis on the legal applicability of the institute of legitimate digital self-defense with the purpose of encouraging the creation of information security policies and computer regulation, aiming to guarantee the performance of response groups to incidents in public institutions and private companies, such as banks, companies and the Public Administration itself, embodied in its organs. To do so, we use the deductive method with explicit legal scope in the national legislation and in the international guidelines, in order to, based on a large bibliographical collection, outline the limits of action based on this document, since it is the same legitimate defense stricto sensu, which differs from the latter only in relation to the medium that will be used, which is the virtual, digital, or non-presence medium.

Keywords: Digital Law. Legitimate Digital Self-Defense. Information security. Digital Society.

SUMÁRIO

1 INTRODUÇÃO 09

2 DIREITO DIGITAL INTERNACIONAL: A ADEQUAÇÃO DO DIREITO À TECNOLOGIA DA ERA DAS REDES 12

2.1 Um fenômeno da Globalização consagrado pela Internet 12

2.2 Natureza jurídica, fontes e princípios que regem o Direito Digital Internacional 17

2.3 O Direito Digital e sua relação com o Direito Internacional (Público e Privado) e o Direito Transnacional. 21

2.4 *Lex Digitalis*: A evolução do conceito de *Lex Mercatoria* na Era Digital 25

3 PROTEÇÃO DOS BENS JURÍDICOS NO CONTEXTO DA SOCIEDADE DIGITAL 30

3.1 Bens Tangíveis *versus* Bens Intangíveis: um novo paradigma na proteção de bens jurídicos 30

3.2 Segurança Digital entre Estados (*Government Cybersecurity*): proteção dos ativos intangíveis governamentais. 35

3.3 Segurança da Informação em âmbito Privado 39

3.4 Teoria da Antijuridicidade: entre a retórica e a racionalidade na proteção penal dos bens jurídicos intangíveis. 42

4 LEGITIMA DEFESA DIGITAL: NOVAS ABORDAGENS, NOVAS PERSPECTIVAS 48

4.1 Novo Direito Penal aplicado a Sociedade Digital e privatização da investigação criminal (*criminal compliance*) 48

4.2 Legítima defesa digital: Conceito e elementos 53

4.2.1 Agressão injusta: crimes digitais (Incidentes de Segurança) 56

4.2.2 Respostas aos Incidentes de segurança: meios necessários para evitar incidentes 60

4.2.3 Atualidade e iminência da agressão: a relativização do conceito de tempo e espaço na Era Digital 62

4.2.4 Defesa do direito próprio ou de terceiro: a importância social da resposta em uma sociedade de risco 64

4.3 Excesso de legítima defesa digital 68

5 CONCLUSÃO 73

REFERÊNCIAS 77

1 INTRODUÇÃO

O advento da sociedade digital provocou grandes reflexões sobre a dogmática jurídica contemporânea, na medida em que o cidadão passa a viver sobre a influência de dois universos paralelos: o mundo real e o mundo virtual.

O fenômeno globalizatório e a tecnologia digital estabeleceram noções inovadoras sobre os conceitos de tempo, espaço e contato, transcendendo definições que se encontravam estáticas a um campo ilimitado de possibilidades reais de abordagem.

A unificação de mercados em escala planetária, a substituição das empresas nacionais por empresas transnacionais, a internacionalização de processos produtivos, o fim do isolamento geográfico, a valorização dos ativos intangíveis e a interdependência econômica são alguns dos reflexos produzidos por estas mudanças econômico-sociais ocorridas nas últimas décadas.

Os investimentos em pesquisa e desenvolvimento (P&D) e a tecnologia amparada por novas mídias (*internet, smartphones, tablets, notebooks*) foram elementos essenciais para promover o processo de integração global. Porém, apesar de ter trazido benefícios consideráveis, o desenvolvimento tecnológico também ampliou as alternativas de ação delituosa, maximizando os potenciais prejuízos decorrentes destas ações.

Adaptar a dogmática jurídica a esta nova realidade é um desafio necessário. As ações praticadas no âmbito virtual que refletem consequências nocivas no mundo presencial não podem restar impunes. Logo, observamos que a incidência cada vez mais frequente de crimes digitais (*cibercrimes*), bem como, a crescente preocupação no âmbito jurídico, econômico e social em combater de forma segura, eficiente e legal tais delitos, provocam uma análise reflexiva sobre como devemos proteger os bens jurídicos intangíveis da criminalidade digital. Neste contexto, veremos que na perspectiva de enfrentamento dos crimes digitais se faz necessário estabelecer novos parâmetros jurídicos frente à questão. Em uma sociedade hiperconectada, na qual, ideais, culturas e interesses são compartilhados; até mesmo, o pensamento jurídico é influenciado por esta interação.

Os incidentes que envolvem meios digitais, geralmente, produzem efeitos extraterritoriais e são abrangidos por mais de um ordenamento jurídico, gerando conflitos de jurisdição e, muitas vezes, esvaziamentos legislativos. Apesar da seara digital ser compreendida, atualmente, como a nova *law trend*, a produção legislativa e bibliográfica

sobre determinados temas ainda é incipiente, visto que os fenômenos digitais são parcialmente conhecidos. No entanto, estes fenômenos digitais estão em vertiginosa e constante transformação.

Por outro lado, a mecânica jurídica tradicional tem dificuldades em acompanhar a agilidade de uma sociedade global/digital, pois, fundamenta-se em elementos estáticos, como soberania e território. Contudo, adaptar o pensamento jurídico aos novos padrões e anseios sociais pode ser tarefa árdua, todavia, não é impossível.

Considerando que o direito de defesa do cidadão não pode se tornar obsoleto em meio a tantas mudanças comportamentais, este trabalho permite fomentar no âmbito jurídico a troca da burocratização, da morosidade legislativa e da falta de celeridade dos tribunais, por soluções legalmente palpáveis no que concerne a adaptação prática de institutos já consagrados pelo Direito.

Em meio a problemática gerada pelos *cibercrimes*, tentamos demonstrar que o instituto da legítima defesa digital apresenta viabilidade e respaldo legal para assegurar a atuação de grupos de respostas a incidentes, combater a impunidade gerada pelos crimes informáticos, propiciar a colheita de provas e, resguardar a inviolabilidade das informações e de outros ativos intangíveis.

Assim, esta obra traz como enfoque a necessidade de estimular as discussões sobre a abrangência do direito de defesa nos meios digitais, por meio do uso da legítima defesa digital amparada em critérios de razoabilidade, proporcionalidade, tempestividade e efetividade da resposta.

Se incialmente as doutrinas acerca da legitima defesa estavam intrinsicamente ligadas ao crime de homicídio, atualmente observamos que este instituto vem libertando-se dos antigos estereótipos através do Direito moderno, passando a ser tratado como meio de defesa aplicado a outros bens jurídicos e outros crimes.

De sorte que, o reconhecimento da possibilidade do exercício da legítima defesa digital segue como uma tendência de colaboração, cada vez mais estreita, entre os setores público e privado, para unir esforços em promover o bem estar social e aproximar o cidadão dos entes institucionalizados, posto que, não se pode delegar toda proteção aos entes estatais, até mesmo porque estes nem sempre se encontram devidamente preparados para fornecer este tipo de ação protetiva de maneira ágil e efetiva.

Em virtude disso, ao longo de toda a pesquisa tentamos demonstrar que a complexidade dos crimes digitais faz surgir uma nova ótica sobre os modelos de investigação delitiva e de proteção dos bens jurídicos, ainda que, estes bens sejam intangíveis.

Para atingirmos os objetivos almejados nesta dissertação, tanto por uma questão didática, quanto pela delimitação teórica que se faz necessária a qualquer trabalho acadêmico, aprofundaremos nosso debate sobre a legitima defesa digital exposta na obra doutrinária da advogada Patrícia Peck Pinheiro, limitando o nosso campo de estudo as ações de legítima defesa praticadas por grupos de gerenciamento de risco e *Criminal Compliance* desenvolvidas por empresas transnacionais, bancos e demais instituições financeiras.

Nessa senda, utilizamos o método dedutivo para realizar uma análise sincrética do direito, por meio de amplo acervo bibliográfico, artigos científicos e legislação, a fim de demonstrar com foco na perspectiva nacional e internacional do Direito Digital, como as inovações jurídico-tecnológicas podem contribuir para prevenir e evitar fraudes contratuais, sequestro de dados (*Ransomware*), espionagem industrial, dentre outros crimes digitais que violam bens intangíveis.

Diante deste panorama, o trabalho dissertativo foi dividido em três partes centrais. Na primeira parte abordou-se a influência da globalização e dos avanços da tecnologia no âmbito jurídico, demonstrando que as inovações tecnológicas contribuíram para a modernização e flexibilização do direito através das novas perspectivas trazidas pelo Direito Digital, cujo caráter é, nitidamente, cosmopolita (internacional/transnacional). Na segunda parte, o foco de análise centrou-se na demonstração de que as implicações econômicas trazidas pela valorização dos ativos intangíveis influenciaram a dinâmica jurídica por meio do fortalecimento de novas estruturas de poder e preocupação com a proteção da segurança da informação, ensejando o debate sobre soluções palpáveis para garantir a defesa digital. Por derradeiro, analisamos o instituto da legítima defesa digital como alternativa viável nas estratégias de governança corporativa e *criminal compliance*, para garantir a segurança digital em conformidade com as diretrizes legais e regulamentares, ainda que esta iniciativa resulte na alteração (“privatização”) da titularidade do domínio sobre tais relações.

Assim, ao passo que a semente da discussão sobre a aplicabilidade da legitima defesa digital está lançada e diante da magnitude dos crimes digitais, tendo em vista que, estes podem ocasionar, inclusive, o desaparecimento de uma empresa, esperamos que esta obra contribua para instigar e ampliar os debates, tendo a manutenção dos contratos comerciais e das empresas como elementos inspiradores deste trabalho.

2 DIREITO DIGITAL INTERNACIONAL: A ADEQUAÇÃO DO DIREITO À TECNOLOGIA DA ERA DAS REDES

2.1 Um fenômeno da Globalização consagrado pela Internet

O desenvolvimento e a propagação do uso das tecnologias digitais e da internet ampliou os modelos de interação entre as pessoas possibilitando que estas realizem transações comerciais e não comerciais em um ambiente hiperconectado, no qual, praticamente, toda transmissão das informações ocorre de forma instantânea.

A internet proporcionou uma maior aproximação dos indivíduos e, por sua vez, eliminou barreiras que outrora eram consideradas intransponíveis, à exemplo das fronteiras temporais, territoriais, ideológicas, políticas, econômicas e culturais que permeiam a sociedade, alimentando o caráter globalizante da rede mundial de computadores. Ocorre que ao eliminar tais barreiras, observamos que os interesses (individuais, sociais, estatais, econômicos e etc.) envolvidos passam a maximizar-se diante da rápida transmissão de ideias e valores propagados pela rede. Do mesmo modo, esta diversidade de interesses adquire unidade à medida que são amparados por esta aldeia global virtualizada.

Segundo Ramos (2016), a globalização contemporânea revela a fluidez das fronteiras estatais e a hipermobilidade da sociedade digital que são evidenciadas na internet e cuja regulação representa um desafio inequívoco para os Estados isoladamente considerados e/ou até mesmo para o próprio Direito Internacional, dada a diversidade de interesses entre os Estados que utilizam e gerenciam a rede mundial de computadores.

Deste modo, o processo globalizante vem sendo impactado pela internet ao criar uma atmosfera de erosão da soberania estatal e contestar a relevância do território como elemento geográfico de demarcação intransponível do direito determinado por cada Estado-nação. Esta ingerência dos efeitos globalizantes no campo jurídico informa a necessidade de definir e consolidar um conceito jurídico único, irradiando, cada vez mais, os anseios por liberdade, igualdade e harmonização de interesses, sendo este último um dos pilares a ser perseguido para alcançar o bem-estar social.

No entanto, observamos que esta realidade só é possível por meio da resolução dos conflitos que eventualmente surgirem neste contexto de novidades tecnológicas. Cada Estado possui capacidade de celebrar, de forma livre, acordos e tratados internacionais, cujas regras definem ou ampliam a convivência entre as diferentes nações, sem que isso implique ferir suas soberanias jurídicas e políticas internas, abrindo espaço para que se possa repensar os modelos

e estruturas jurídicas vigentes em seus territórios, inibindo o isolamento jurídico dos mesmos e, provocando maior interdependência e colaboração entre as nações.

Nesse sentido, Pinheiro (2016) afirma que a globalização da economia e da sociedade exige a globalização do pensamento jurídico, de modo a encontrar mecanismos de aplicação de normas que possam extrapolar os princípios da territorialidade, principalmente no tocante ao Direito Penal e ao Direito Comercial, refletindo uma tendência à globalização do próprio direito. Entretanto, este ideal de globalização jurídica não surgiu com o advento do Direito Digital, mas, encontra suas linhas basilares no Direito Internacional, por meio de Convenções[1] e Tratados Internacionais, tentando estabelecer critérios mais uniformes de análise jurídica entre os vários Estados nacionais.

Seguindo estas novas bases, não é viável agarrar-se à noção estática de Estado e de trias políticas (Poder Executivo, Poder Legislativo e Poder Judiciário) que se desenvolveu conforme a construção ideológica do Séc. XIX. Não podemos nos olvidar de que o Estado é uma criação abstrata da sociedade civil, sendo um produto histórico do jogo de forças sociais, que se antes eram geograficamente (território) e, juridicamente (Constituição), delimitadas no interior da sociedade nacional, agora tendem a ser universalmente consideradas a partir do reconhecimento de uma sociedade mundial e de outras esferas de poder além das institucionalizadas pelo Estado.

De acordo com Barbosa (2017), a formação jurídica, em larga medida, ainda se mantém presa a visão do Direito calcada na ideologia do século XIX, que reivindica o monopólio estatal em todos os sentidos, seja na sua produção, seja na sua aplicação, sob o postulado de que se trataria de condição para o bem comum. Com isso, prioriza-se as análises descritivas do Direito, reservando pouco ou quase mesmo nenhum espaço para as discussões teóricas e para os fatos tais como se apresentam no mundo real, os quais se opõe profundamente ao discurso hegemônico institucionalizado e positivista do Direito Estatal.

---

[1]Podemos citar: a) a "Lei Modelo da United Nations Commision on International Trade Law (Uncitral) para o comércio eletrônico como guia de aplicação", produzido pela primeira vez em 1996, atualizada em 1998. Esse documento é referência mundial e todos os países devem fundamentar-se nele ao regulamentar o comércio eletrônico em seu território. Todavia, esta lei não define o que é comércio eletrônico, mas, introduz parâmetros importantes para as relações comerciais e não comercias, sobretudo, no que se refere a troca eletrônica de dados e a definição dos seus elementos, ou seja, a mensagem eletrônica, o intercâmbio eletrônico de dados – EDI, o remetente, o destinatário, o intermediário e o sistema de informação, sendo aplicável a todos os tipos de informação em forma de mensagem de dados, utilizados no contexto de atividades comerciais. Disponível na íntegra em <www.uncitral.org>; b) a "Cartilha sobre Comercio Eletrônico e Propriedade Intelectual", publicada pela WIPO/OMPI (http://www.wipo.int), que aborda questões como jurisdição e legislação aplicável, entre outras, relativas ao comércio eletrônico.

Assim, observamos que a sociedade digital caminha no sentido de criar um ordenamento jurídico global, visto que, até mesmo o próprio Estado, como unidade política fundamental, passa a ter sua imprescindibilidade questionada, transmutando-se conceitualmente para contestar a sua abrangência como Estado-nação e fomentar o surgimento de um Estado supranacional, à medida que, tais ideais ganham forma e força na sociedade convergente para instigar a concepção de um Constitucionalismo Global.

Para Ianni (1999), a noção de Estado supranacional e, consequentemente, de Constitucionalismo Global pode ser apenas uma metáfora, pois, a ciência jurídica ainda não assimilou a metamorfose da sociedade nacional em sociedade global. No entanto, o Estado-nação passa a ser redefinido, pois, perde algumas de suas prerrogativas econômicas, políticas, culturais e sociais, debilitando-se. Aos poucos, algumas dessas prerrogativas aparecem nas decisões e atividades de empresas transnacionais e organizações multilaterais. Estas empresas mundiais levantam uma quantidade de novas questões para governos que procuram modelar os destinos econômicos de suas nações e de outros países que sofrem a sua influência.

Essa nova abordagem do direito corrobora com o entendimento de que a sociedade moderna, globalizada e digital encontra-se em constante transformação e, portanto, situa-se para além do positivismo, da dogmática jurídica e dos desenvolvimentos meramente materialistas e econômicos. As novas dinâmicas desta sociedade complexa revelam que a relação entre teoria e prática pode ser produtiva para solucionar os conflitos que emergem vertiginosamente da Revolução Digital e que demandam maior flexibilidade da ciência jurídica.

Observamos que “as expressões sociedade industrial, pré-industrial e pós- industrial são conseqüências conceituais ao longo do eixo da produção e dos tipos de conhecimento utilizados” (BELL, 1973, p. 25). A sociedade pós-industrial, informacional e digital desenvolve-se em um ambiente em que, os pilares da transparência, colaboração, cooperação, compartilhamento de informação (conhecimento), mobilização e modelo de riqueza baseado em ativos intangíveis, funcionam como alicerces para os modelos de governo e de governança contemporâneos.

O sociólogo japonês, Yoneji Masuda (1982) foi um dos teóricos precursores da utilização do termo Sociedade da Informação, ao prever, na década de 80, as transformações que seriam causadas pelas Tecnologias de Comunicação e Informação –TIC, explanou em suas obras, que esta sociedade é baseada na alta criatividade intelecto-informacional resultante da revolução da informática, por meio do desenvolvimento do computador, expandindo o poder produtivo e valorativo da informação digital, possibilitando a produção automatizada em massa de informação, através da tecnologia e do conhecimento cognitivo.

Para Masuda (1982), a base dessa sociedade seria a produção de valores informacionais intangíveis em substituição aos valores tangíveis, prevalecendo a indústria do conhecimento, a partir da expansão de uma economia sinérgica e da utilização compartilhada dos bens, com a criação de uma comunidade interativa e voluntária, voltada para o benefício social.

O sociólogo espanhol, Manuel Castells (apud Brandão 2018), afirma que a sociedade da informação em redes ou sociedade digital, representa um período histórico-cultural caraterizado por uma revolução tecnológica movida pelas tecnologias digitais de informação e de comunicação, na qual o funcionamento advém de uma estrutura social em rede, que envolve todos os âmbitos da atividade humana, numa interdependência multidimensional, que depende dos valores e dos interesses subjacentes em cada país e organização, classificando este período referente a última metade do séc. XIX como a Era da informação, em virtude do desenvolvimento da internet e das tecnologias eletrônicas/digitais.

De acordo com Takahashi (2000), a sociedade digital está sendo construída em meio a diferentes condições e projetos de desenvolvimento social observados localmente, em cada país, e globalmente, por meio de politicas integradas, segundo estratégias moldadas de acordo com cada contexto econômico-cultural. Deste modo, regiões, segmentos sociais, setores econômicos, organizações e indivíduos são afetados diferentemente pelo novo paradigma, observando as peculiaridades, expectativas, carências e a aptidão para iniciativa criativa de cada setor, em função das condições de acesso à informação, da base de conhecimentos e, sobretudo, da capacidade de aprender e inovar.

Para compreender essas passagens de uma cultura à outra, Santenella (2003) utiliza uma divisão das eras culturais em seis tipos de (in)formações: a cultura oral, a cultura escrita, a cultura impressa, a cultura de massas, a cultura das mídias e a cultura digital. Acompanhando este cenário evolutivo, percebemos que a cultura digital vêm incorporando, gradativamente, as novas tecnologias e transformando as estruturas e as práticas de produção, comercialização, consumo, cooperação e de competição entre os agentes, alterando, enfim, a própria cadeia de geração de valor.

“Surgiram, então, com a infraestrutura do ciberespaço, novo espaço de comunicação, de sociabilidade, de organização e de transação, mas também novo mercado da informação e do conhecimento” (LEVY, 1999, p. 32). Nesse diapasão, a internet torna-se protagonista de um cenário econômico-social globalizatório, no qual, o poder tecnológico emergente passa a ser uma instância de expressão da sociedade global em formação, e portanto, um meio passível de intervenção estatal.

Contudo, sua governabilidade é contestável devido a rede mundial de computadores ser considerada um espaço transnacional. Por não pertencer a nenhum Estado-nação e ao mesmo tempo pertencer a todos, a internet não deve ser dirigida política-juridicamente por nenhum governo específico, assim como não deve existir um controle sobre o tráfego global diante das suas características comunitárias e de neutralidade.

No entanto, a ideia de ingovernabilidade, que aqui não se confunde com a ideia anárquica de total liberdade, passa a ser substituída pelo conceito de governança multilateral, democrática e transparente, demonstrando a complexidade do regramento dos fatos transfronteiriços que emergem da internet e que conta com regras domésticas, internacionais estrito senso e, ainda, transnacionais.

Conforme assevera Teubner (2016), é inaceitável a proliferação da falácia de que a Internet é um ambiente totalmente livre e "ingovernável", pois, a constatação de um vazio constitucional do espaço transnacional se trata de uma inconsistência que pode ser corroborada empiricamente, uma vez que, pesquisas científicas fundamentadas em análises das ciência sociais apontam para um "novo constitucionalismo", assim como, as pesquisas desenvolvidas há tempos por economistas e estudiosos do direito econômico sobre as instituições emergentes direcionam para uma constituição econômica mundial. Do mesmo modo, os estudos de direito internacional assinalam à crescente relevância das normas constitucionais no âmbito transnacional indicando, exatamente, a direção oposta àquela da tese do vazio constitucional.

Logo, constatamos que a globalização jurídico-tecnológica foi um dos fatores de maior expressividade para criar uma conjuntura social representada por atores multissetoriais (Governos, empresas transnacionais, sociedade civil, ONGs. Universidades e etc.) que seguem uma sistemática baseada na tolerância e cooperação, evidenciando a tentativa de conciliar interesses em favor da resolução dos conflitos oriundos do ciberespaço através de regulações específicas para este setor e do surgimento de um ramo próprio para atuar sobre esta problemática, qual seja o Direito Digital Internacional.

Por ser um ramo dedicado ao estudo dos fenômenos oriundos da influência da tecnologia nas relações jurídicas, o Direito Digital traz para os operadores do direito sérios desafios para adaptação e aplicabilidade da ciência jurídica aos conflitos que surgem na sociedade digital, o que exige do jurista contemporâneo a busca pelo entendimento dialógico das diversas fontes a fim de compreender as hipóteses de harmonia e dissenso existente entre elas a partir da análise do caso concreto.

É praticamente impossível enquadrar todas as peculiaridades exigidas pelo Direito Digital em um ordenamento jurídico nacional especifico e, relativamente, estável, diante do

dinamismo e da celeridade exigidos pelo mundo hiperconectado. Nesse diapasão, a elaboração de instrumentos regulatórios em âmbito estatal e privado para tratar de assuntos relativos a internet resultou na cooperação, cada vez mais constate, entre o Direito Internacional Privado e o Direito Transnacional tendo em vista que ambos regulam fatos sociais que escapam às fronteiras dos Estados e, por conseguinte, extravasam as concepções existentes no direito doméstico.

Deste modo, internacionalizar/transnacionalizar o Direito Digital apresenta-se como uma das alternativas viáveis para impedir o vazio legislativo/regulatório que pode decorrer das novas problemáticas da Era da Informação. As questões digitais exigem respostas tempestivas e palpáveis. Por isso os debates neste setor devem ocorrer no sentido de promover a verificação da possibilidade de regular fatos sociais que extravasem às fronteiras dos Estados propiciando soluções efetivas para incidentes que envolvam meios digitais e a internet de forma segura e em tempo hábil.

2.2 Natureza jurídica, fontes e princípios que regem o Direito Digital Internacional

Muito se discute sobre a natureza jurídica do Direito Digital. Alguns autores entendem que se trata de um ramo específico do Direito, e outros advogam no sentido de que é apenas uma atualização circunstancial do mesmo. No entanto, o seu caráter multidisciplinar informa a importância e influência desta disciplina no cotidiano da sociedade. Nos últimos anos, a disciplina ganhou notoriedade e seu campo de atuação foi sendo ampliado para alcançar todas as áreas do Direito, seja de forma horizontal ou transversal, passando a incorporar também vários aspectos e princípios de Direito Internacional, devido a descontinuidade espacial que os incidentes digitais provocam nos ordenamentos jurídicos e o caráter transnacional e comunitário da internet.

Logo, a complexidade dos problemas versados pelo Direito Digital Internacional conduz a uma variedade de fontes produtoras de normas que se situam no plano interno de cada país, assim como, também se apoiam em regras oriundas de sistemas jurídicos desenvolvidos nos planos regional e internacional. Essas regras consubstanciam a mutação/aglutinação dos costumes de uma sociedade digital globalmente considerada, e são instrumento de afirmação dos valores dos “novos” Estados que modelam o direito, adaptando-o aos fatores econômico-sociais para promover o seu desenvolvimento por meio da tecnologia.

Esta sociedade a qual nos referimos, vem sendo denominada de sociedade pós-industrial, digital, da informação ou do conhecimento por fundamentar-se no sentido valorativo que é atribuído à informação, principalmente, quando ela está expressa em dados digitalizados.

Segundo Fiorillo (2015), a definição de sociedade da informação é bastante complexa e repleta de contradições, mas sobretudo é marcada por duas características essenciais: flexibilidade e capacidade criativa. Flexibilidade porque absorve trocas intensas de informação e, com isso, mantém sua fluidez no tempo e no espaço. Capacidade criativa porque propicia uma maior abertura quanto a titularidade do conhecimento gerado e posto em divulgação.

Desta forma, alimentando-se do alto fluxo de informações e promovendo infindáveis questionamentos sobre a realidade posta(imposta), a sociedade digital ressuscita dilemas jurídicos e econômicos para recolocar o sujeito e a ética como elementos indissociáveis para a instrumentalização do meio ambiente digital.

Por demandar uma forte reflexão sobre a cultura, a justiça e o profundo sentido das regras, o Direito Digital Internacional assume como premissa a cooperação e a responsabilidade partilhada, a partir do momento em que se constata a necessidade de negociações mais flexíveis entre os atores globais e de processos normativos menos engessados.

Segundo Pinheiro (2016), os valores a serem protegidos são determinados dentro de um espaço social maior que os limites territoriais do Estado, o que exige mais flexibilidade das normas e uma maior aceitabilidade dos instrumentos de autorregulação. Por isso, os Diplomas Normativos Supranacionais e as Diretrizes gerais têm ganhado notoriedade como instrumentos que permitem legislar sem prejudicar a evolução da própria internet, dos negócios, do mercado e da sociedade.

Assim, o Direito Digital Internacional prioriza as fontes com maior flexibilidade e abrangência comunitária, como as normas de natureza autorregulamentar, os princípios, os costumes (*Lex Digitalis*), a jurisprudência, a doutrina e as regra estabelecidas na *soft law*[2], que passa a ter caráter cogente, isso sem descurar da observância da legislação nacional e dos tratados internacionais.

Nessa conjuntura, podemos constatar que a sociedade digital caminha no sentido de criar um sistema jurídico global. No entanto, uma Constituição Global apresentada como Lei

[2]A velocidade das transformações mundiais não comporta mais as velhas formas de negociação, como a dos tratados multilaterais, com formalidades em excesso e engessamentos que demandam um tempo que já não se tem. A *soft law* surge, então, para atender essa necessidade e não há mais como negar seu caráter cogente. Uma visão contemporânea da *soft law* – Matsalém Gonçalves Pimenta. Publicado em 02.2018. Disponível em: https://jus.com.br/artigos/64141/uma-visao-contemporanea-da-soft-law.

Fundamental de uma sociedade nitidamente globalizada, tecnológica e comunitária, e não apenas como um estatuto organizatório do Estado, ainda é um projeto distante.

Devido a necessidade de respostas ágeis e eficientes para solucionar os incidentes que envolvam esta matéria, o Direito Digital Internacional assume uma postura principiológica, tendo em vista que a obsolência e o vazio legislativo ou regulamentar ocasionados por uma estrutura tradicionalmente positivista são problemas constantes neste campo de atuação.

Portanto, uma carta de princípios gerais aplicáveis a qualquer um, em qualquer lugar, apresenta-se atualmente como o instrumento mais viável para aumentar o grau de segurança jurídica e efetividade das decisões judiciais que envolvam temas digitais, além de possibilitar uma maior interação entre os atores globais que gerenciam a internet e outras questões sobre governança digital.

Segundo Pinheiro (2016), no Direito Digital prevalecem os princípios em relação as regras, pois o ritmo de evolução tecnológica será sempre mais veloz do que o da atividade legislativa. Logo, observa-se que a disciplina jurídica tende à autorregulamentação, ou seja, os próprios interessados na resolução da questão assumem o compromisso de criar um conjunto de regras com soluções práticas que atendem ao dinamismo que as relações de Direito Digital exigem.

Nesse sentido, o acesso facilitado à informação possibilitou que as pessoas passassem a questionar e fiscalizar de forma enérgica, toda e qualquer, instituição e organização pública ou privada que interfira direta ou indiretamente no cotidiano do cidadão.

Vivenciamos um período no qual as grandes corporações, assim como os Governos, passam por uma severa crise de credibilidade. Nesse cenário, os anseios dos cidadãos/consumidores deram margem a debates sobre ética e responsabilidade social, dando especial destaque a sustentabilidade e ao *compliance* no seio das corporações, e bem como, a corrupção e a *accountability* no setor público.

Uma tendência crescente entre atores estatais e não estatais é a de incentivar a cooperação e a colaboração entre os mesmos, possibilitando uma parceria público-privada significativa para que haja uma maior repartição de poderes (responsabilidades), deveres e direitos que extravasem a esfera pública governamental. Essa vertente de incorporação de princípios axiológicos vem se fortalecendo no direito positivo brasileiro. No âmbito do Direito Digital, encontramos na Constituição Federal como na Lei nº 12.965/14 (Marco Civil da Internet – MCI) regras cuja natureza principiológica possibilitam uma maior durabilidade da norma como instrumento de resolução de conflitos.

Segundo Canabarro (2014), devido a sua importância legal, o MCI foi, inclusive, uma das leis inspiradoras da Declaração de Direitos na Internet Italiana publicada em 13 de outubro de 2014. Portanto, há muitas semelhanças entre o conteúdo do texto italiano e os principais marcos normativos que tratam da questão no Brasil (o Decálogo de Princípios do Comitê Gestor da Internet no Brasil – CGI.br[3] e a Lei 12.965/2014).

Nesse diapasão, o modelo brasileiro foi um dos precursores nos debates sobre a governança global da Internet. No entanto, observamos que o caso da Itália é bem peculiar, pois, o Brasil teve participação direta nos debates e diálogos que levaram à formulação e adoção da Declaração na Câmara dos Deputados da Itália. Por intermédio dos Conselheiros do CGI, Demi Getschko e Carlos A. Afonso, o governo brasileiro pôde apresentar ao público italiano um relato detalhado do desenvolvimento institucional da governança da Internet no Brasil, durante o evento organizado pela organização Internet Society – ISOC na Itália sobre a governança da Internet. Do mesmo modo, parlamentares italianos, à exemplo da presidente da Câmara dos Deputados italiana, Laura Boldrini, também visitaram o Brasil para conhecer o processo de criação do MCI através de consultas populares elaboradas com a utilização das TIC.

Logo, tais valores, princípios, e modelos de atuação apontam os objetivos e caminhos almejados por esta geração movida pela tecnologia, demonstrando que princípios como o da

[3] O Comitê Gestor da Internet no Brasil – CGI.br, reunido em sua 3ª reunião ordinária de 2009 na sede do NIC.br na Cidade de São Paulo/SP, decide aprovar a seguinte Resolução: CGI.br/RES/2009/003/P - PRINCÍPIOS PARA A GOVERNANÇA E USO DA INTERNET NO BRASIL. Considerando a necessidade de embasar e orientar suas ações e decisões, segundo princípios fundamentais, o CGI.br resolve aprovar os seguintes Princípios para a Internet no Brasil: 1) Liberdade, privacidade e direitos humanos: O uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática; 2) Governança democrática e colaborativa: A governança da Internet deve ser exercida de forma transparente, multilateral e democrática, com a participação dos vários setores da sociedade, preservando e estimulando o seu caráter de criação coletiva; 3) Universalidade: O acesso à Internet deve ser universal para que ela seja um meio para o desenvolvimento social e humano, contribuindo para a construção de uma sociedade inclusiva e não discriminatória em benefício de todos; 4)Diversidade: A diversidade cultural deve ser respeitada e preservada e sua expressão deve ser estimulada, sem a imposição de crenças, costumes ou valores; 5) Inovação: A governança da Internet deve promover a contínua evolução e ampla difusão de novas tecnologias e modelos de uso e acesso; 6) Neutralidade da rede: Filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos, culturais, ou qualquer outra forma de discriminação ou favorecimento; 7) Inimputabilidade da rede: O combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos; 8) Funcionalidade, segurança e estabilidade: A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas; 9) Padronização e interoperabilidade: A Internet deve basear-se em padrões abertos que permitam a interoperabilidade e a participação de todos em seu desenvolvimento. 10) Ambiente legal e regulatório: O ambiente legal e regulatório deve preservar a dinâmica da Internet como espaço de colaboração. Resolução CGI.br/RES/2009/003/P: https://www.cgi.br/resolucoes/documento/2009/003

extraterritorialidade, cooperação/colaboração, transparência, ubiquidade e prevenção[4] devem nortear as relações humanas na Era Digital e propiciar o ciberativismo, pois, deste modo, o pluralismo jurídico permite a aplicação da lei com fundamento na justiça e nos valores humanos de forma atemporal.

Sendo assim, a sociedade digital nos conduz a reformulação da lei como única fonte do direito, tendo em vista que as soluções derivam da hermenêutica calcada na pluralidade de fontes, sejam estas estatais ou não, compatibilizando ideologias e valores aparentemente contraditórios para garantir a efetividade da norma na Era Digital.

2.3 O Direito Digital e sua relação com o Direito Internacional (Público e Privado) e o Direito Transnacional.

Diante desta realidade social que se revela cada vez mais globalizada e interconectada, o Direito Digital passa a assumir um caráter internacional e/ou transnacional. Por serem áreas afins, o Direito Internacional (Público e Privado) e o Direito Transnacional acabam servindo como parâmetro a ser utilizado nos conflitos que envolvem o ciberespaço. Estes ramos estão intrinsicamente ligados, pois, regulam fatos sociais que geralmente escapam às fronteiras dos Estados, enfrentando problemas político-jurídicos que dependem da flexibilização de marcos temporais e territoriais para obtenção de soluções satisfatórias.

Os problemas que envolvem direitos digitais e regulação da internet não podem ser satisfatoriamente resolvidos apenas com a observância de ordenamentos jurídicos nacionais, pois, este são (de)limitados por critérios de soberania e território que traduzem positivismos estadocentristas que não são compatíveis com a dinâmica do Direito Digital.

O Direito Digital em suas mais variadas formas de manifestação tem por fundamentos teóricos fenômenos como a transnacionalidade do direito, a globalização tecnológica, a economia internacional e a cooperação internacional. Nesse sentido, contextualizar os fenômenos que ensejam direitos digitais para a realidade da vida cotidiana, aponta para o aparecimento de esferas normativas que fogem ao domínio estatal, provocando a redefinição das fronteiras políticas, alterando o equilíbrio do poder e criando uma disputa pela hegemonia mundial.

[4] Interessante notar que estamos analisando o meio ambiente digital objetivando promover o desenvolvimento, a qualidade e o equilíbrio socioambiental no ciberespaço, portanto, acabamos sofrendo a influência dos princípios do Direito Ambiental

Desta forma, o Direito Digital sofre influência do Direito Transnacional, pois, estes dois ramos defendem a criação de normas especializadas por novos membros, retirando, assim, o monopólio do direito dos Estados-nação, sem que haja divisão hierárquica entre este e os demais sujeitos globais na elaboração, interpretação e aplicação de normas globais.

Segundo Rodegheri (2015), os Estados-nação necessitam abrir as suas fronteiras geográficas e ideológicas, não apenas à comercialização de produtos e a dinamização da economia, como também para o intercâmbio de informações, decisões, ideias, soluções de conflitos, precedentes e julgados, para que, compartilhando valores universais adaptados às realidades nacionais, possam coexistir de forma cooperativa.

Nesse contexto, a cooperação é um atributo essencial nas relações de Direito Digital e torna-se perceptível em três vertentes. A primeira, denota a necessidade de regulação da internet através do diálogo entre os Estados-nação. No âmbito do Direito Internacional Público esta interação dialógica é representada, primordialmente, pela Organização das Nações Unidas – ONU. Por outro lado, a cooperação deve existir para influenciar a aplicação de normas nacionais norteadas por princípios estrangeiros ou de caráter universal e a aplicação de normas estrangeiras no âmbito nacional com ênfase nas diretrizes de Direito Internacional Privado. Por derradeiro, observamos a descentralização do sistema normativo do eixo estatal para empresas transnacionais e organizações não governamentais num claro reflexo de transnacionalização do Direito.

Assim, compartilhando a responsabilidade pela gerência (governança) e regulamentação do meio ambiente digital e, sobretudo, da Internet, com outros atores globais, desenvolveremos uma atividade multisetorial que envolva governos, empresas, cidadãos e organizações independentes (ONGs).

Isto posto, Silva (2003) preleciona que não há um único centro que governa ou gerencia a Internet. As redes constituintes pertencem a alguma organização, mas a rede mundial de computadores não pertence a ninguém. Quando se fala em decisões sobre a internet, sendo estas apenas em padrões tecnológicos, elas são de responsabilidade de órgãos como a *Internet Numbers Authority*, a *Internet Engineering Task Force*, a Isoc, a Internet Corporation for Assigned Names and Numbers – ICANN, dentre outras organizações de membros voluntários que constituem a *Internet Society*.

Logo, temos que a lógica jurídica deve ser repensada de acordo com as mudanças sociais, pois, conforme Lorenzetti (2004) aduz, o Direito positivista, burocrático e estadocentrista que conhecemos não está apto a regular este novo mundo e também não tem muitas funções a desempenhar. Por este prisma, o renomado autor faz uma clara analogia entre

a Terra e o Mar, afirmando que o Direito do "mundo real" emana dos Estados nacionais, estando vinculados ao conceito de território dentro do qual exercem seus limites. Esse mesmo Direito, admite um espaço liberado, que é o mar, sobre o qual não existe controle além das áreas próximas da terra firme. Nesse sentido, esta analogia poderia dar lugar a um "Direito da Navegação Virtual", ou seja, ao Direito Digital.

Seguindo o mesmo entendimento, Pacheco (2016), destaca que causa estranheza a vontade dos governos em legislar sobre algo que, por sua essência, não dever ser legislado, uma vez que, a própria Internet é capaz de desenvolver os contratos sociais necessários para lidar com os seus problemas, pois, o princípio que sustenta a rede é a ausência de vinculação a qualquer governo.

A Internet e os princípios que dela são inerentes já sofreram inúmeras mutações desde que esta foi criada como "arma militar" e depois foi propagada nas universidades. Historicamente, observamos que a internet surgiu como instrumento de dominação e demonstração do poderio estatal, mas foi remodelando-se nos centros acadêmicos e adquirindo outro traço ideológico, difundindo-se como meio de expressão da autonomia, colaboração e liberdade de uso, principalmente, por se tratar de um mecanismo rápido, fácil e abrangente de propagação do conhecimento e de informação.

Como um meio de comunicação exclusivamente militar, a internet sofria, portanto, grande influência estatal. Este poderio estatal sobre o meio de comunicação começou a se fragmentar quando a internet atingiu os ambientes acadêmicos, pois, no meio universitário era difundido o ideal de informação/conhecimento livre e para todos. Assim, a informação passou a ser produzida e propagada pelo próprio individuo sem que houvesse a necessidade de um intermediador, e/ou sem a interferência de um ente regulador (censurador).(SILVA, 2003).

Neste diapasão, as relações que emanam dos meios digitais e, principalmente, da internet, tornam imperiosa a necessidade de reconhecer a autonomia e a importância de outros atores internacionais que não apenas os Estados para construir mecanismos que primam pela regulação e, consequentemente, solução de conflitos emergentes no âmbito digital, através de um ramos próprio que sintetize todos esses modelos de "Direito" para formular melhores práticas e contribuir para consolidação de uma *Lex Digitalis*, ou seja, de um Direito Digital.

Predominantemente, mas não exclusivamente, o Direito Digital é definido por atores não-estatais em forma de contrato, termos de uso, códigos de ética, leis-modelo e regulamentos próprios. Desta forma, a combinação da globalização tecnológica com a privatização da legislação quebrou a cadeia de legitimidade do direito baseada no modelo de Constituição de Estado.

Conforme Rodegheri (2015), neste mundo cada vez mais permeado pela rapidez dos processos, globalização da economia, utilização da internet e tecnologias digitais, o indivíduo também tem alterado a condição de mero expectador de programas e ações governamentais, para o patamar de cidadão engajado e preocupado com os problemas que envolvem o ambiente em que habita. Sendo assim, estes indivíduos (cidadãos) representados por governos, empresas e organizações independentes refletem a necessidade de diálogo em múltiplos níveis de poder para que coexistam sistemas de proteção gradativos do meio ambiente digital em escala local, nacional, regional ou supranacional e internacional.

2.4 *Lex Digitalis*: A evolução do conceito de *Lex Mercatoria* na Era Digital.

O Direito Digital acolhe a ideia de que ninguém melhor do que o próprio indivíduo para manifestar as suas preferências e interesses neste processo de construção cooperativa, global e colaborativa na Era da Informação.

O pensamento de Habermas (2001) transmite esta ideia com maestria no sentido de que os primeiros destinatários de uma república mundial são justamente os cidadãos, especialmente os organizados em movimentos sociais e ONGs, pois, estes representam um canal independente de transmissão da "voz" do povo. De modo que, o indivíduo passa a ser reconhecido de fato, e não apenas de direito, como o grande cerne de todo o sistema e, portanto, o foco de atuação deve ser baseado nele.

Essa ideia de autonomia da vontade nas relações jurídicas é secular e tem como grande representante o fenômeno da *Lex Mercatoria.* Por isso é tão importante relembrar esse instituto, tendo em vista que foi justamente a utilização da *Lex Mercatoria* nas relações comercias que possibilitou a aceitação das novas modalidade de *Lex*, à exemplo da *Lex Digitalis* e da *Lex Sportiva*.

Costa (2011) afirma que a guerra em defesa da autonomia da *Lex Mercatoria*, é importante não apenas para o desenvolvimento do instituto, mas, também, para o fortalecimento de todas as áreas do Direito que se pretendem globais, cujo debate e emergência no cenário internacional se dá em relativo isolamento em relação a política oficial dos Estados.

A *Lex Mercatoria* se desenvolveu a partir de cenários de interdependência e dinamização das relações comerciais internacionais, prevalecendo, na maioria dos casos, a autonomia da vontade deliberada nos contratos, no qual se podia dispor sobre a liberdade de arranjos das condições e jurisdições que melhor representariam o interesse dos contratantes. Desta forma, por ser considerada uma espécie de direito (ou sistema regulatório) global, em que as redes especializadas são formadas por meio da conexão contratual de cunho comercial com a finalidade de regular, material e formalmente, as atividades econômicas de forma mais abrangente, a *lex mercatória*, portanto, tenciona atingir mais de um território, ainda que determinadas atividades que possam por ela ser reguladas venham a se desenvolver apenas em um Estado-nação específico.

Deste modo, visando uma maior abrangência, as regulamentações da *lex mercatória* podem advir tanto de instrumentos modelo, estatutos, códigos de conduta, regulamentos, quanto de costumes e de precedentes de tribunais arbitrais, ou de quaisquer outras formas prévias de

inserções normativas que possam formar elementos de conexão comercial, com a finalidade de regular, material e formalmente, as atividades econômicas de forma global.

Seguindo este traço evolutivo, o instituto se desenvolveu e possibilitou o aparecimento de suas novas vertentes. No âmbito do Direito Digital ela serve como parâmetro, pois, tanto a *Lex Mercatoria* como a *Lex Digitalis* representam diferentes conjuntos de normas que fogem do controle estatal nas relações internacionais. A Internet é um fenômeno global e transnacional. Ela influencia desde os níveis mais baixos da sociedade e da economia, como também pode influir no destino de superpotências, à exemplo da suposta influência Russa nas eleições presidenciais norte-americanas que elegeram Donald Trump em 2018[5].

Por ter grande poder de influência, a Internet é um meio de comunicação e informação que vem ganhando novos contornos no mundo interconectado da contemporaneidade e, por tal razão, vem provocando disputas entre Governos e organizações independentes quanto ao papel destas instituições na regulação de domínios na Rede Mundial de Computadores.

Segundo Ramos (2016), a característica de acessibilidade global da internet gera debates sobre qual é a jurisdição nacional apta a conhecer de litígios, bem como estimula discussões sobre as diferentes leis nacionais de regência e, ainda, suscita dúvidas sobre se um Estado deve cumprir ordem estrangeira de controle da internet em seu território (por exemplo, suspensão de um site, cujo funcionamento é ilícito no Estado requerente). Nessa hipótese, os agentes privados utilizam sua autonomia para escolher o Estado mais protetivo em termos de legislação, regulação e fiscalização (para armazenar dados, localizar seus provedores, hospedar seus sítios etc.), aproveitando-se da irradiação mundial do espaço virtual.

Logo, o controle dos sistemas de endereços da Internet, a partir da concessão e supervisão destes domínios é uma das funções-chave da Corporação para Atribuição de Nomes e Números na Internet (ICANN) por meio de sua Política de Resolução de Disputas por Nomes

[5] O relatório divulgado pelos serviços de inteligência dos Estados Unidos não traz provas concretas sobre o papel de Putin na campanha contra Hillary Clinton, mas afirma que as ações da Rússia incluíram:Hackear emails de contas do Comitê Nacional Democrata e de membros da alta cúpula do partido;- Usar intermediários como WikiLeaks, DCLeaks.com e Guccifer 2.0 para publicar informações adquiridas no hackeamento;- Usar propaganda financiada pelo Estado e pagar usuários de mídia sociais ou "trolls" para fazer comentários desagradáveis sobre Hillary. Segundo o documento, Putin apoiava Trump porque ele havia prometido trabalhar ao lado da Rússia. Além disso, o presidente russo havia tido "muitas experiências positivas trabalhando com líderes políticos do Ocidente que, por conta de interesses de negócios, ficavam mais propensos a fazer acordos com a Rússia - como o antigo primeiro-ministro italiano Silvio Berluscono e o ex-chanceler alemão Gerhard Schroeder". Mais do que isso, Putin também não teria boas relações com Hillary, porque a considerava responsável por incitar protestos anti-governo em 2011 e 2012 na Rússia. Ver matéria na íntegra: Por que os serviços de inteligência dos EUA acham que a Rússia interferiu na eleição de Trump? BBC News (Brasil): https://www.bbc.com/portuguese/internacional-38525951. Publicado em 07 de janeiro de 2017.

de Domínio (UDRP)[6], sendo uma organização monitorada pelos Estados Unidos. No entanto, a ONU vem questionando esse modelo de gestão, pois acredita que a gerência americana da web pode representar o mais novo modelo de imperialismo mundial.

Em que pesem as disputas de poder entre estes dois sujeitos, é notória a constatação de que a ONU ainda não possui uma atuação suficientemente influente em termos de regulação transnacional dos direitos humanos na Internet, de modo que as ações regulatórias acabam sendo predominantemente coordenadas pela ICANN.

Para Ramos (2016), diante do poder regulamentar da ICANN sobre os domínios na internet, o qual se coloca, inclusive, acima dos Estados, surgiu a discussão sobre a existência de um direito transnacional da internet, ou seja, uma ordem legal autônoma, que normatiza as relações jurídicas entre atores privados e públicos, que transcendem as fronteiras. É a chamada *lex digitalis*.

A *lex digitalis* é um instrumento jurídico em que novas formas de elaboração de regras estão sujeitas a uma ampla discussão social sobre os desafios normativos do direito transnacional, portanto, é moldada por uma variedade de instituições diferentes, na qual, o ator central desse esquema de governança com vários interessados é a ICANN.

Desta forma, a ICANN representa uma clara manifestação da teoria do transconstitucionalismo no campo da *lex digitalis,* de tal modo que, sua atuação regulamentar e a aceitação das suas diretrizes e regras por outros atores globais, demonstra que esse contexto de transferência de poder do campo público(estatal) para o privado, afeta as questões regulatórias no âmbito dos direitos humanos digitais de forma expressiva.

A autonomia da vontade, elemento informador do Direito Transnacional e, por via reflexiva, do Direito Digital, deve ser interpretada em conjunto com os demais direitos envolvidos nos fatos transfronteiriços que cingem questões digitais, impondo condicionantes que implicam em limites, restrições e respeito aos valores contemporâneos que o Direito Internacional Privado alberga.

Sistematizar as forças jurídicas transnacionais *da lex digitalis (costume dos internautas*, política digital desenvolvida por empresas, códigos de ética criados por ONGs e etc.), também ampliará seu alcance, em particular, com referência a debates recentes sobre

[6] O caso GlobalSantaFe exemplifica a complexidade na relação entre a lex digitalis e as leis internas dos Estados. No início dos anos 2000, as empresas Global Marine Inc. e Santa Fe International Corp. fundiram-se na GlobalSantaFe Corp. e, consequentemente, pleitearam, perante a VeriSign (uma das entidades de registro autorizadas pela ICANN nos Estados Unidos), a utilização do domínio GlobalSantaFe.com para representar a empresa na internet. Porém, tão logo foi anunciada a fusão, o cidadão sul-coreano Jongsun Park registrou o referido domínio na Hangang (também entidade de registro autorizada pela ICANN, na Coreia do Sul).

aspectos jurídicos e normativos legais. Esses debates culminaram recentemente na Reunião Global Multissetorial da NETmundial sobre o Futuro da Governança da Internet, realizada em São Paulo, Brasil, em maio de 2014. A ONU, por sua vez, também se mantém na linha de negociação através do Fórum de Governança da Internet (IGF)[7].

Não obstante, percebemos que nesse contexto de disputa de poder, o indivíduo isolado ou comunitariamente representado, é considerado o cerne de todo este processo normativo baseado na autonomia e na percepção da vontade. Razão pela qual, também devem ser buscadas medidas e alternativas em que haja espaço para a discussão popular ou pública sobre os rumos a serem adotados pelos Estados e pelos outros atores globais, preferencialmente, utilizando as Tecnologias da Informação e Comunicação (TICs) para garantir maior abrangência e participação popular.

Para acompanhar tal evolução, os governos começam a investir na melhoria de seus próprios serviços, por meio das chamadas "Hackatons" ou "Hackfests", maratonas hackers que buscam soluções para problemas sociais reais. Esta iniciativa governamental reafirma a necessidade de que sistemas de proteção aos direitos humanos em múltiplos níveis sejam pensados e construídos com base nas expectativas, nas opiniões e nos posicionamentos dos cidadãos.

Com tantas funções e aplicações, a Internet se torna um mecanismo apto a conjugar o universalismo dos direitos humanos com o relativismo das tradições nacionais, permitindo uma forma de autonomia mitigada aos Estados-Membros, já que há a possibilidade de controle supranacional, especialmente quanto à legalidade e/ou proporcionalidade da medida, a possibilidade de impetração de recursos em face da decisão, entre outros.

A possibilidade de conversação entre as ordens jurídicas e normativas estatais, internacionais e transnacionais representa a construção de diálogos entre Parlamentos, Cortes e cidadãos, principalmente através do desenvolvimento de mecanismos de solução de conflitos aptos a regular e proteger de forma efetiva os direitos dos indivíduos na Sociedade Digital.

---

[7] O Fórum de Governança da Internet (IGF) é um fórum multissetorial, democrático e transparente, que viabiliza debates sobre questões de políticas públicas relativas a elementos importantes da governança da Internet. O IGF foi proposto pela Cúpula Mundial sobre Sociedade da Informação em novembro de 2005, e criado após consultas convocadas pelo Secretário-Geral das Nações Unidas em 2006. Desde então, anualmente o IGF acontece em cidades-sede escolhidas para tanto. Proposto e coordenado pelo CGI.br, o Brasil sediou o IGF de 2007 na cidade do Rio de Janeiro (RJ) e o de 2015 na cidade de João Pessoa (PB). Este fórum é extremamente importante, pois, fornece uma plataforma facilitadora para discussões entre todos os setores do ecosistema de governança da Internet, incluindo as entidades credenciadas pela Cúpula Mundial sobre a Sociedade da Informação (CMSI), bem como outras instituições e indivíduos com especialidade comprovada e experiência em assuntos relacionados à governança da Internet.

Conclui-se, portanto, que na evolução da ordem normativa transnacional, a *lex mercatória* foi utilizada como pressuposto e ponto de partida para o estudo da regulação privada ou, como alguns defendem, foi o instituto normativo que propiciou a origem do direito global. Sendo assim, a apreciação e aceitabilidade da *lex digitalis* com suas ordens normativas específicas, termos de uso (contratos de adesão) inovadores e contratos-tipo, além dos costumes e códigos de ética desenvolvido pelos internautas, só foi possível, pois, a *lex mercatória* "preparou o terreno" para tais discussões, abrindo espaço para um campo fértil de abordagens normativas.

Deste modo, a *lex digitalis* simboliza o dinamismo que a tecnologia possibilitou para as relações jurídicas, propiciando uma maior liberdade de negociação, harmonização social e segurança jurídica entre os envolvidos nas relações digitais.

3 PROTEÇÃO DOS BENS JURÍDICOS NO CONTEXTO DA SOCIEDADE DIGITAL

3.1 Bens Tangíveis *versus* Bens Intangíveis: um novo paradigma na proteção de bens jurídicos

No decorrer da evolução histórica percebe-se que diversos bens foram considerados preciosos de acordo com a época vivenciada. Na sociedade feudal, o bem mais valioso era a terra; na sociedade industrial capitalista os bens mais preciosos eram as máquinas e o dinheiro, na atualidade constatamos que na sociedade digital o bem mais valioso é o dado, ou seja, a informação organizada.

Para Silva (2003), a informação é importante para a atualidade, pois, representa um diferencial competitivo e, assim, reflete diretamente na capacidade das sociedades de se sobreporem às outras, estabelecendo uma hierarquia de poder: quanto maior o grau de informação e as melhorias nas condições tecnológicas para a sua obtenção, maior seria o poder desta sociedade em relação às outras que não gozam deste mesmo privilégio.

Nesse sentido, a informação passou a ser um elemento relevante na construção social, devido a sua capacidade em influenciar as ações humanas e não tão somente estas, como também as ações dos computadores, já que os mesmos só realizam as tarefas que lhes são atribuídas através das informações constates nos códigos digitais. A partir desta realidade, conclui-se que o dado é apenas uma informação que foi organizada e devidamente considerada, processada, operada e transmitida por um sistema de computador ou programa de computador para a consecução de um determinado fim.

A palavra informação deriva do latim *informare*, que significa “dar forma”. Segundo Wiener (1984), esse termo designa o conteúdo daquilo que permutamos com o mundo exterior ao ajustar-nos a ele, e que faz com que o nosso ajustamento seja nele percebido. O processo de receber e de utilizar informações é o processo de nossos ajustes as contingências do meio ambiente e de nosso efetivo viver nesse ambiente.

A fusão entre a informação e automação proporcionou a digitalização da informação, possibilitando o tratamento racional e automático da linguagem através da transformação do que é materialmente palpável em objetos virtuais. Assim, digitalizar uma informação significa traduzir sua mensagem em códigos (dígitos binários), o que equivale dizer que o suporte armazenado não conterá texto legível pelo homem, mas códigos que, ao serem traduzidos e apresentados pelo equipamento eletrônico, exibirão, em tela, uma reserva potencial.

Diante disso, percebe-se que tudo o que é tido no mundo físico como uma "coisa" tangível e material, pode ser idealizado no mundo virtual, passando a ser uma "coisa" intangível e imaterial sem perder o seu valor agregado. Tomemos como exemplo a cifra constante na tela do caixa eletrônico que traduz uma realidade intangível para o cliente, no entanto, você sabe que ali está apenas a representação do valor numérico expresso em dinheiro, ou seja, é apenas a representação ideal das cédulas de dinheiro. Nesse sentido, o dinheiro que antes era apenas palpável passou a ser expresso também em *bits*[8] e não tão somente em cédulas de papel, pois, naquela mensagem eletrônica está expresso o valor do crédito do cliente da agência bancária. Deste modo, o computador potencializa a informação individualizando-a para cada operador da máquina.

Como vemos, neste cenário de rara complexidade, a moeda que é considerada um dos elementos basilares do capitalismo, já está se digitalizando, não só como representação de um valor monetário em um caixa eletrônico, mas tendo o algoritmo como o próprio valor monetário a ser contabilizado, à exemplo dos *Biticoins*[9], numa perspectiva crescente de adesão a novos métodos de pagamento, como e-wallets[10], carteiras digitais e a utilização de códigos QR[11].

Com a evolução das transações comercias via internet passou-se a comercializar não apenas bens/serviços corpóreos/tangíveis, mas também, os seus correspondentes incorpóreos/intangíveis, como, por exemplo, o uso dos serviços de entretenimento disponibilizados por *streaming*. Antigamente, comprávamos discos de vinil, *cds* e *dvds* para ter

---

[8]*Bit* (simplificação para dígito binário, " *Binary digit* " em inglês) é a menor unidade de informação que pode ser armazenada ou transmitida, usada na Computação e na Teoria da Informação. Um bit pode assumir somente 2 valores: 0 ou 1, corte ou passagem de energia respectivamente. Embora os computadores tenham instruções (ou comandos) que possam testar e manipular bits, geralmente são idealizados para armazenar instruções em múltiplos de bits, chamados bytes.

[9]*Bitcoins* (símbolo: Ƀ; abrev: BTC ou XBT, *peer-to-peer electronic cash system*) é uma moeda digital criada por Satoshi Nakamoto em 2008. O *Biticoin* é uma criptomoeda descentralizada responsável pela elaboração de um sistema econômico alternativo que permite a transação financeira anônima e sem intermediários, mas que pode ser verificada por todos através da rede *peer-to-peer* por consistir em um programa de código aberto. É considerada a primeira moeda digital mundial descentralizada e é tida como responsável pelo ressurgimento do sistema bancário livre.

[10]*E-wallets* são carteiras digitais, ou seja, um sistema de pagamento móvel que permite aos seus usuários armazenar cartões de crédito, cartões de fidelização, entre outras informações bancárias para facilitar o pagamento de suas compras *on line* ou em lojas físicas, além de inibir o uso inadequado e vazamento de dados pessoais.

[11]Semelhantes aos códigos de barra tradicionalmente impressos nos produtos, os códigos QR são códigos bidimensionais que podem ser facilmente escaneados utilizando as câmeras dos *smartphones*. Esse código facilita a conversão e propagação da mensagem, seja, de texto (interativo), um endereço URL, um número de telefone, uma localização georreferenciada, um *e-mail*, um contato ou um SMS. O termo QR deriva de *Quick Response*, que em inglês significa resposta rápida, transparecendo a intenção do criador de montar um objeto de fácil decodificação e em alta velocidade, via de regra, por imagem, sendo bastante utilizado em estratégias publicitárias de *marketing*.

acesso a conteúdo audiovisual, mas agora passamos a abandonar estes suportes físicos para termos acesso, apenas, ao conteúdo e ao seu uso através dos serviços de *streaming* como o *Spotify* e a *Netflix*.

Nesse cotejo, observamos que se antes o ativo tangível (patrimônio, bens materiais, terrenos, maquinários, estoque, prédios) era considerado como parte principal da indústria, atualmente, o valor de elementos intangíveis como Marca, Reputação, Cultura Corporativa, Talentos, Capital intelectual, Imagem, *Royalties*, Patentes, Tecnologia da Informação, Governança Corporativa, Sustentabilidade, Relacionamento com Clientes e Consumidores, dentre outros atributos não materiais, vem sendo considerados e contabilizados como recursos estratégicos de diferenciação e potencializadores de crescimento econômico das empresas.

Segundo Costa (2016), a construção do Estado Moderno é baseada em uma estrutura de poder com raízes no monismo juspositivista, e por tal razão, tem relação intrínseca com a defesa do direito de propriedade. No entanto, se antes a propriedade era majoritariamente territorial, física; palpável, atualmente ela é intelectual, virtual, intangível. Nada mais lógico, então, que o Estado defenda ferrenhamente a propriedade intelectual, porque, além de garantir o direito de propriedade, vigiar o tráfego de dados que circula na rede ainda proporciona vantagem estratégica, já que o conhecimento e a informação se tornaram o "Ouro Negro (Petróleo)" da Era da Informação.

A informação organizada (estruturação de dados) gera o conhecimento produzido pelas empresas, sendo este, consequentemente, o seu maior bem. O conhecimento consubstanciado nos intangíveis demonstra que esses ativos além de possuírem valores intrínsecos claros, transferem e potencializam valor para os ativos tangíveis numa relação de trocas mútuas, pois, os produtos e mesmo os serviços deixaram de ser considerados diferenciais competitivos exclusivos, sustentáveis e perenes, necessitando das características distintivas dos ativos imateriais (singularidade, inimitabilidade, intransferibilidade) para ganharem força no mercado.

Na era da informação, a empresa do conhecimento surge em um cenário onde as organizações tornam-se dependentes do conhecimento como pressuposto para o sucesso e da tecnologia como um importante instrumento no controle gerencial. Como exemplo dessa nova dinâmica organizacional, temos algumas empresas que funcionam apenas com base na criação do valor atribuído aos seus ativos intangíveis, como o Uber que é uma empresa de transporte particular, que não possui um único carro próprio; o Airbnb que é uma das maiores empresa de hospedagem, sem possuir um único bem imóvel e o Facebook, que é a maior empresa de mídia do mundo, sem criar sequer um conteúdo.

Nestes casos, segundo Stewart (1998), a rigor as empresas não possuem conhecimento. Seu capital intelectual está na competência/profissionalização de seus empregados (capital humano), nas características e opiniões de seus clientes (capital do cliente), e na forma como as informações de ambos são gerenciadas (capital estrutural), portanto, estas empresas são exemplos evidentes de que o mundo vem se transformando através de regras ditadas pelos consumidores, por meio do valor gerado pelo conhecimento de suas informações por parte das empresas.

Nesse diapasão, a estrutura material das "coisas" se modifica para que estas componham o mundo virtual, o que de fato não as tornam irreais, necessitando, tão somente, de atualização para serem utilizadas no mundo físico. Atualizando e virtualizando as informações de forma particular, transcendemos as barreiras físicas para possibilitar um maior alcance da experiência humana, convertendo esta apreciação para um nível coletivo//global e, não tão somente, local/individual no que tange a produção de capital intelectual.

Deste modo, podemos esperar a digitalização e, consequente, intangibilidade de outros elementos e bens inerentes as transações comerciais capitalistas. Os contratos são um grande exemplo desta quebra de paradigma, pois, cada vez mais, passam a adquirir forma eletrônica e utilizar suportes físicos diferentes do papel. A ideia de comércio eletrônico transmuta-se para englobar, não apenas, a compra e venda de mercadorias, mas, toda relação, bens e documentação, tangível ou intangível, que traduza vantagem econômica.

Seguindo a evolução do pensamento capitalista, se nos anos 90, falava-se sobre a Economia da Informação e do Conhecimento como preconizou Stewart (1998), contemporaneamente, as discussões giram em torno do que seria a Economia da Colaboração, analisando os seus desdobramentos e métodos de uberização que geram valor através do compartilhamento de informações.

Esse novo modelo de produção baseado nos conceitos de comunidade, colaboração e auto-organização, distancia-se cada vez mais dos controles hierárquicos, mostrando-se bastante poderosa e eficiente para atuar frente a alguns mercados, visto que este modelo está em sinastria com a velocidade das mudanças tecnológicas, com a diversidade de gerações nos ambientes profissionais e com a necessidade de solucionar as novas demandas globais. Desta maneira, vivenciamos na atualidade, um processo inexorável de rediscussão global dos modelos atuais de produção e valoração dos ativos tangíveis/intangíveis, com incessante reflexão sobre como estes bens devem ser protegidos pelo direito. Nesse sentido, acreditamos que inseridos no contexto de Economia Colaborativa devemos observar com primazia a influência da confiança

e a observância do princípio da boa fé para consolidação destas novas oportunidades de mercado.

3.2 Segurança Digital entre Estados (*Government Cybersecurity*): proteção dos ativos intangíveis governamentais.

A tecnologia digital e o desenvolvimento de novas mídias (smartphone, tablets,) trouxe significativo avanço no campo da troca de informação e disseminação de formas mais eficientes de se conectar à internet. Com isso, os indivíduos, e até mesmo, os Estados passaram a depositar suas informações, confidenciais ou não, no espaço cibernético.

O grande depósito de informações relevantes no ciberespaço ampliou, proporcionalmente, o nível de prejuízo causado por um ataque cibernético. Por tal razão, os Estados continuam direcionando altos investimentos no setor de segurança da informação e defesa cibernética, para garantir o sigilo e a integridade de informações estatais sensíveis.

Por manterem a guarda de ativos intangíveis importantes, os Estados tornam-se alvos potenciais da atuação dos *hackers*, sendo vítimas do ataque, ou, simplesmente, da espionagem destes programadores especializados em atacar e invadir sistemas de forma anônima e difusa, seja para fins lucrativos ou políticos, e que podem atuar por conta própria ou à serviço de instituições, e até mesmo de outros Estados.

Embora, os estudos sobre ciberguerra e ciberdefesa ainda sejam pouco expressivos na legislação e na doutrina, verificamos que com o avanço da tecnologia o tema ganha cada vez mais espaço na agenda de defesa dos Estados, de modo que os setores de inteligência e as forças militares passam a explorar estratégias de defesa e de governança interna, estruturando a política de segurança dos países e alargando a compreensão de proteção de fronteiras a nível geográfico e digital. No entanto, é impossível proteger todos os ativos de uma nação sem trabalho colaborativo. Portanto, os Grupos de Gerenciamento de Risco e *Compliance* – GRC trabalham incansavelmente para reduzir as vulnerabilidades e prevenir ataques, bem como coibir os eventuais incidentes de segurança.

Como exemplo de alguns desses incidentes de segurança a nível estatal, identificamos o caso *Stuxnet,* no qual um vírus supostamente desenvolvido pelos serviços de inteligência estadunidense e israelense, infectou a instalação nuclear Iraniana de Natanz em 2010, causando a destruição de aproximadamente mil centrífugas de urânio, e consequentemente, atrasando o programa nuclear iraniano em 2 anos.

Não muito longe, tivemos no Brasil uma experiência semelhante, envolvendo a interferência direta dos serviços de inteligência estadunidense em assuntos estatais, através da espionagem realizada pela Agência Nacional de Segurança dos Estados Unidos da América (NSA na sigla em inglês) sobre o governo e setores estratégicos do Estado brasileiro no ano de

2013, sendo este caso conhecido mundialmente por meio das revelações do ex-agente americano Edward Snowden. (CALDEIRA, 2013).

Não obstante, apesar do governo dos Estados Unidos ser identificado como suposto autor de inúmeros escândalos envolvendo espionagem digital, estudos realizados pelo próprio governo federal americano, por meio de um relatório recente do Escritório de Administração e Orçamento da Casa Branca, em parceria com a empresa de autoria de software Veracode, apontam as vulnerabilidades das agências de segurança estatais reforçando a extrema necessidade de mudança em dezenas dessas agências.

Segundo Newman (2018), o estudo expõe o fato de que das 96 agências federais avaliadas, o relatório considerou 74% "*At Risk*" (Em risco) ou "*High Risk*" (Alto risco), o que significa que elas precisam de melhorias cruciais e imediatas. De tal modo, que mais da metade das agências sequer tem a capacidade de determinar qual software é executado em seus sistemas, e apenas uma em cada quatro agências pode confirmar que elas têm a capacidade de detectar e investigar sinais de uma violação de dados, tendo em vista que em 38% dos incidentes de segurança digital do governo, as agências não conseguem identifica o "vetor de ataque", ou seja, não podem apontar como o *hacker* teve acesso ao sistema.

Nesse diapasão, percebemos que priorizar a defesa digital é uma exigência de ordem iminente dos Estados-nação. Outro caso bastante peculiar que corrobora com tal entendimento é o do *Vatileaks*, site dedicado à publicação de informações confidencias do Vaticano, cujo nome faz clara alusão ao famoso site *WikiLeaks*. No caso *Vatileaks,* jornalistas italianos estariam divulgando documentos com informações, propositalmente, ocultadas ao povo pelo alto clero do Vaticano, numa tentativa de esconder a verdade sobre o seu passado, sendo nesta ocasião revelada suposta corrupção envolvendo o alto escalão da igreja católica no ano de 2015 (CHAOUQUI, 2017).

As informações relevantes e confidenciais requerem, por parte do Estado, maior vigilância contra atos terroristas de espionagem, sequestro ou divulgação de dados, pois, da mesma forma que os *hackers* éticos dos GRCs existem para assegurar a proteção dos dados sensíveis, outros grupos de hacker, não tão éticos assim, trabalham para encontrar as vulnerabilidades dos dados governamentais, como pode ser observado nos casos de incidentes de segurança supra mencionados.

No Brasil, verificar se as estratégias aplicadas pelo governo correspondem às suas reais ameaças e necessidades em âmbito digital é uma das competências do Ministério da Defesa, que por meio do Exercício Guardião Cibernético, conduzido pelo Comando de Defesa Cibernética (ComDCiber), tem a finalidade de promover o treinamento das Forças Armadas

para proteção de ataques virtuais, atuando em três setores que abrangem dados governamentais sensíveis: Defesa, Financeiro e Nuclear.

O Exercício utiliza o Simulador de Operações de Guerra Cibernética (Simulador Virtual – SIMOC[12]), no qual foram inseridos prováveis incidentes digitais, como uma grande quantidade de ações de hackers no setor financeiro, no setor de defesa e no setor nuclear. Cada grupo, por meio de seus gabinetes de crise, utilizando um software livre, o Request Tracker, desenvolvido pelo ComDCiber, analisa, toma decisões e se prepara para responder aos crimes virtuais. Ao agir dessa forma, treinam procedimentos para as vulnerabilidades de seus sistemas.

Depois de ser alvo de espionagem digital, o Brasil passou a investir em defesa cibernética com convênios, projetos e compra de equipamentos de defesa. No entanto, o país ainda dá os primeiros passos e está longe de garantir uma segurança cibernética eficiente, apesar de o tema já figurar como prioridade na Estratégia Nacional de Defesa.

Segundo Caldeira (2013), a fragilidade do sistema de segurança cibernético brasileiro foi escancarada pelo escândalo envolvendo o vazamento promovido por Edward Snowden, ex-colaborador da Agência Nacional de Segurança dos Estados Unidos (NSA, na sigla em inglês). Documentos mostraram que a presidente foi alvo de espionagem, assim como o Ministério das Minas e Energia, e a maior estatal do país, a Petrobras, com suspeitas de espionagem comercial nesse último caso.

Existem suspeitas de outros incidentes digitais expressivos no Brasil, à exemplo dos dois apagões elétricos que afetaram milhões de brasileiros em 2005 e 2007, e que segundo fontes da CIA, que afirmaram através da rede telecomunicação americana CBS, foram causados por ataques de hackers contra os sistemas de controle da rede de fornecimento brasileiro. Outro incidente bastante complexo, foi o que ocorreu em 2011, quando o site da Presidência e de vários ministérios e órgãos da administração federal foram alvo de ataques ao longo de vários dias. Neste último caso, o movimento de hackers Lulz Security, abreviado por LulzSec, assumiu a ofensiva que, segundo o grupo, tinha a intenção de mostrar a vulnerabilidade do sistema.

No âmbito de defesa nacional, o governo brasileiro, por meio do Ministério da Defesa, publicou a Doutrina Militar de Defesa Cibernética através da Portaria Normativa Nº 3.010/MD, de 18 de novembro de 2014, que traz em seu bojo vários conceitos bastante esclarecedores sobre segurança digital, como o que é defesa cibernética, espaço cibernético, ameaça

[12]SIMOC (Simulador de Operações de Guerra Cibernética): Simulador virtual que foi desenvolvido com tecnologia 100% nacional pelo Centro de Instrução de Guerra Eletrônica (CIGE), do Exército Brasileiro, em parceria com uma empresa de Tecnologia da Informação, a Rustcon. É voltado para treinar e simular situações em que as tropas militares necessitem atuar contra possíveis ataques cibernéticos.

cibernética e guerra cibernética (BRASIL, 2014).[13] Logo em seguida, também foi publicada a Portaria Normativa Nº 1.688/MD, de 5 de agosto de 2015, que é mais específica e trata da Política de Segurança da Informação e Comunicações da Administração central do Ministério da Defesa. Esta última portaria aborda conceitos importantes, como o que é ativo de informação, tratamento de incidentes de rede, gestão de risco, dentre outras definições importantes (BRASIL, 2014).[14]

Diante de todas estes casos e estratégias, podemos concluir que embora não exista um estado total de segurança cibernética, pois, nenhum país está 100% protegido dos perigos da ação de hackers, sejam estes ativistas, integrantes de grupos criminosos ou funcionários de agências de inteligência de outros países, ainda assim, do ponto de vista de Defesa e Segurança Nacional, até mesmo para evitar possíveis guerras cibernéticas, é fundamental investir em desenvolvimento científico e tecnológico para a obtenção de maior autonomia estratégica e de melhor capacitação operacional, visto que os incidentes digitais são resultado do aproveitamento das vulnerabilidades dos sistemas de segurança informatizados.

---

[13] Algumas definições contidas na Portaria Normativa Nº 3.010/MD, de 18 de novembro de 2014:1) Defesa Cibernética - conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente; 2) Espaço Cibernético - espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas; 3) Ameaça Cibernética - causa potencial de um incidente indesejado, que pode resultar em dano ao Espaço Cibernético de interesse; 4) Guerra Cibernética - corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C^2 do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC

[14] Algumas definições contidas na Portaria Normativa Nº 1.688/MD, de 5 de agosto de 2015: 1)Ativo de informação: patrimônio composto por dados, informações e conhecimentos obtidos, gerados e manipulados durante a execução dos sistemas e processos de trabalho; 2) Gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse processo fornece estrutura para que se desenvolva uma resiliência organizacional capaz de responder efetivamente e salvaguardar os interesses das partes envolvidas, a reputação e a marca da organização, assim como seus processos e seu valor agregado. É o resultado da fusão dos Planos de Contingência e dos Planos de Recuperação de Desastres, que objetiva garantir a recuperação de um ambiente de produção, independentemente de eventos que suspendam suas operações e de danos nos componentes (processos, pessoas softwares, hardware, infraestrutura etc.) por ele utilizados; 3) Gestão de Segurança da Informação e Comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à Tecnologia da Informação e Comunicações (TIC); 4) Gestão de Riscos em Segurança da Informação e Comunicações: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação; 5) Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores.

3.3 Segurança da Informação em âmbito Privado

A tecnologia digital e o uso massivo da internet mudaram a maneira como as empresas conduzem seus negócios e os indivíduos conduzem as relações sociais. Vimos no tópico anterior que o aparato de segurança e inteligência cibernética dos Estados encontra-se em constante expansão. Não obstante, o setor privado também está investindo na capacidade de segurança e proteção de ativos intangíveis.

Conforme aduz Domeneghetti e Mier (2009), nesta era de mercados globalizados "internetizados", altamente dinâmicos e passíveis de imitação, os ativos tangíveis perderam relativa relevância, passando a ser imperativo a uma empresa tornar-se capaz de identificar, categorizar, qualificar e quantificar os seus ativos intangíveis, exigindo-se a sua gestão sistemática, visto que muitas vezes são negligenciados em sua administração e defesa por falta de percepção ou por falta de instrumentos eficientes.

Diante deste cenário, a segurança da informação assume um papel estratégico na proteção contra vários tipos de ameaça aos ativos intangíveis de uma corporação, para poder garantir a continuidade do negócio, minimizar os riscos e danos comerciais, além de maximizar o retorno sobre investimentos e oportunidades,

Nesta perspectiva, é importante estabelecer o papel das empresas, e sobretudo, das grandes empresas privadas, no estabelecimento de diretrizes nesse setor. Como o sistema de segurança cibernética inclui a proteção de dados de instituições governamentais, privadas e dos cidadãos em geral, todos os atores devem unir esforços contra ameaças preponderantemente externas, potenciais ou manifestas. Para as empresas, a segurança digital é extremamente importante, pois, viabiliza a atividade empresarial e assegura a sua própria existência, na medida que, a digitalização está afetando cada aspecto da produção, do comércio e da consecução de serviços, desde as grandes corporações às pequenas empresas.

Segundo o relatório "Economia da Informação 2017" publicado pela Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD), as novas tecnologias de informação e comunicação (TIC), o comércio eletrônico e outras aplicações digitais estão ajudando um crescente número de pequenas empresas e empreendedores nos países em desenvolvimento a se conectar com mercados globais e criar novas formas de geração de renda.

Assim, percebemos que as atividades humanas, principalmente, as atividades comerciais, estão cada vez mais dependentes do uso da tecnologia e da internet. Essa adesão maciça às novas mídias digitais e as possibilidades inovadoras de conectividade, geram um grande volume de dados com valor agregado, que necessitam ser tratados e protegidos pelas

instituições que possuem a sua guarda. Deste modo, é interessante observar que a segurança da informação no âmbito privado perpassa por dois pontos essenciais, o da proteção dos dados pessoais, ou seja, as informações sobre clientes/usuários e a proteção dos ativos intangíveis das empresas, sendo que esta última engloba a primeira. Enquanto que para as empresas é estatisticamente interessante partilhar os dados de clientes/usuários para identificar preferências e padrões de conduta, o mesmo não se pode dizer de compartilhar informações sigilosas e confidenciais, como segredos industriais, *know-how* e comunicações internas.

Com a tecnologia do *Big Data* e o aumento da concorrência, inclusive ensejando casos de concorrência desleal, a preocupação acerca da segurança da informação é extremamente plausível. O tratamento de grande volume de dados tem um potencial incrível para gerar novas oportunidades, modelos de negócio, empregos, habilidades e formas de compreensão, porém, em oposição a isto, existe a possibilidade de ocasionar exclusão social e discriminação, em virtude da ampliação da desigualdade de renda, além do fato de que os usuários estão deixando de ser os "clientes" para se tornarem os "produtos" dos provedores de aplicação, havendo, assim, a capitalização do próprio ser humano, e um processo de "coisificação" das pessoas e de tudo que possa apresentar valor agregado.

Toda esta conjuntura é propícia para que o aumento do número de crimes digitais esteja em evidência no cenário de riscos corporativos, tornando os debates sobre a proteção da informação, uma questão frequente na pauta dos conselhos empresariais, tendo como foco principal os perigos e as vantagens da automação industrial, para oferecer novas arquiteturas de segurança e identificar, responder, bloquear e contra-atacar tentativas de invasão aos sistemas corporativos.

Nesse diapasão, Steffanini (2016) esclarece que o aumento dos ataques virtuais está levando várias empresas a investir no segmento de *cybersecurity*. De modo que, a América Latina tem sido alvo crescente de crimes cibernéticos e o Brasil aparece como um dos principais focos de criminalidade digital. O autor explica ainda, que de acordo com o estudo realizado pela *Cybersecurity Ventures*[15] e divulgado durante uma das principais feiras de segurança no Rio de Janeiro, a LAAD Security[16], o País perde mais de US$ 8 bilhões por ano em função de crimes na internet, o que o torna a segunda maior fonte de crimes cibernéticos no mundo e o

[15]Cybersecurity Ventures é a principal pesquisadora e página da internet que disponibiliza fatos estatísticas confiáveis sobre segurança digital e economia mundo (https://cybersecurityventures.com

[16]A LAAD Security – Feira Internacional de Segurança Pública e Corporativa é considerada a maior feira de Defesa e Segurança da América Latina, sendo realizada anualmente para discutir e apresentar soluções tecnológicas voltadas para a defesa pública e privada.

primeiro na América Latina. O mesmo estudo citou que o Brasil está entre os cinco países com mais crimes cibernéticos – os outros são Rússia, China, Nigéria e Vietnã.

A fragilidade brasileira em termos de segurança digital corporativa pode ocorrer devido à preterição e falta de gestão dos ativos intangíveis. Por não contabilizarem corretamente os seus ativos intangíveis, muitas empresas ainda não sabem o que estão perdendo por não investir na segurança dos mesmos. “Se a administração conhecesse as atividades daquela área, poderia ter reconhecido indícios de necessidade de maior atenção, investigado as operações e tomado providências para reduzir as perdas prováveis.” (ASSI, 2014, pag.48).

Acontece que, na medida em que a tecnologia se aperfeiçoa, ataques maliciosos tornam-se cada vez mais criativos e sofisticados, encontrando formas para enfrentar as barreiras de segurança de softwares e hardwares. O avanço da tecnologia e a consequente dependência das companhias por sistemas mais conectados esbarram no fato de que a invasão de um ambiente digital corporativo pode provocar consequências drásticas, que muitas vezes, podem não ser esperadas, mas podem ser previstas e prevenidas.

No entanto, algumas empresas subestimam a capacidade destrutiva de um ataque hacker, negligenciando o fato de que estes ataques podem gerar prejuízos incalculáveis em decorrência da interrupção dos negócios, de eventual indenização a terceiros por reparação de danos, além do grave dano reputacional à própria empresa ou marca, e das mudanças que podem provocar no mercado e na cadeia produtiva das corporações.

A revolução tecnológica e o desenvolvimento da economia digital permitiram às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes. Tal contexto, aliado a episódios recorrentes de violação da privacidade, tem desafiado órgãos reguladores globalmente. Embora, alguns países tenham publicado leis sobre a regulação da internet e a proteção de dados, nenhum desses países consegue ter uma regulamentação tão expressiva quanto a General Data Protection Regulation – GDPR da União Europeia.

As regras europeias sobre proteção à privacidade e tratamento de dados pessoais foram elaboradas em 2016 através do GDPR, mas, só entraram em vigor a partir de 25 de maio de 2018. Estas regras são bastante relevantes, pois, incrementaram o cenário de proteção de dados pessoais, através da sua aplicação extraterritorial, passando a exigir conformidade as empresas situadas dentro e fora da União Europeia, que ofereçam bens, serviços ou que monitorem o comportamento de consumidores residentes no bloco europeu.

Moraes e Teffé (2017), prelecionam que no Brasil, o MCI traz o conceito de dados pessoais positivado no seu regulamento (Decreto nº 8.771/16[17]), o qual estipula que será considerado dado pessoal o "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa". Desta forma, a noção brasileira seguiu a mesma lógica do Regulamento nº 2016/679 (General Data Protection Regulation – GDPR) do Parlamento Europeu e do Conselho, que define dado pessoal como "informação relativa a uma pessoa singular identificada ou identificável ('titular dos dados').

Cabe ressaltar que o governo brasileiro avançou nesta temática ao promulgar uma lei específica sobre dados pessoais, sua proteção e privacidade, qual seja, a Lei nº 13.709, de 14 de agosto de 2018, regulamentando-a por meio da Medida Provisória nº 869, de 27 de dezembro de 2018. De modo que, embora a referida lei só entre em vigor 24 (vinte e quatro) meses após a data da sua publicação, já traz reflexos expressivos ao definir uma Autoridade Nacional de Proteção de Dados – ANDP e regulamentar o tratamento de dados, tendo a sua publicação sido impulsionada pelas exigências regulamentares contidas no GDPR europeu.

O GDPR também orienta as empresas para que estabeleçam padrões de governança, incentivando a prevenção de incidentes digitais através de boas práticas de segurança digital. Por meio de controles internos é possível garantir que os dados confidenciais das empresas sejam preservados, que a linha de produção industrial fique menos vulnerável e que a nossa infraestrutura crítica dos serviços essenciais não seja paralisada por ataques virtuais.

Por todo o exposto, observamos que a segurança da informação no âmbito privado deve decorrer não apenas pela melhoria de processos e controles internos, mas, principalmente, pela mudança cultural relativa a conscientização e aceitação do prejuízo potencial que um incidente digital pode causar, seja em virtude de um ataque hacker ou até mesmo por negligência dos próprios *stalkeorders*.

3.4 Teoria da Antijuridicidade: entre a retórica e a racionalidade na proteção penal dos bens jurídicos intangíveis.

Partindo do pressuposto de que novas situações merecem novas respostas, torna-se inteiramente natural pensar que um crime cometido em ambiente virtual, tanto pode como deve ensejar um ato protetivo da vítima na defesa de seus interesses e bens, sejam estes tangíveis ou

[17] Art. 14, I, do Decreto nº 8.771/16, que regulamenta a Lei no 12.965/2014(MCI).

não. Nestes termos, o Direito Digital assume uma postura principiológica e autorregulamentar, tendo em vista que a obsolência e o vazio legislativo ocasionados por essa estrutura tradicionalmente positivista são problemas constantes neste campo de atuação.

No direito constitucional brasileiro não há referência expressa acerca da cibervigilância e ciberespionagem como conduta criminal. No entanto, tal omissão legislativa é natural, uma vez que as mudanças trazidas pelas tecnologias digitais não haviam começado no Brasil ao tempo da promulgação da Constituição Federal de 1988, de modo que as atenções voltaram-se para os problemas cibernéticos após o Bug do Milênio[18], no final do século XX, entre a transição do ano 1999 para o ano 2000.

Mas, apesar de não reconhecer expressamente tais delitos, a Constiuição de 1988 reconheceu em seu art.5 um rol não taxativo de direitos fundamentais, de sorte que passou a ratificar os principais tratados internacionais de direitos humanos, incorporando-os ao direito brasileiro. "Nesse sentido, a intimidade, a vida privada e o sigilo de dados e das comunicações, exatamente os direitos que podem ser violados por atividades de vigilância e espionagem digital, restam protegidos consoante o art.5." (WOLOSZYN, 2016, pag. 103).

Nesse sentido, avocando o direito à proteção de dados como um direito fundamentalmente humano, temos a percepção de que deve haver um maior comprometimento e interação internacional entre os Estados a fim de desenvolver um padrão de conduta efetivo e uma estrutura legal coerente contra a cibervigilância em massa. No entanto, enquanto esses padrões de conduta e de legislação não são criados, harmonizados e contemplados pelos diversos atores internacionais, devemos orientar nossa atuação protetiva em ambientes digitais, de modo que, a tecnologia sirva aos valores fundamentais da humanidade.

Para Cannataci[19](2018), infelizmente não vislumbramos nenhuma legislação de vigilância nacional que cumpra e respeite perfeitamente o direito à privacidade, visto que, os mecanismos de supervisão doméstica para a vigilância das comunicações e do uso da Internet nem sempre existem e, quando ocorrem são geralmente ineficazes ou não oferecem transparência e prestação de contas adequadas.

---

[18] O Bug do Milênio representa a histeria coletiva e mundial originada pelos boatos (Fake News) de que após a virada do milênio, os sistemas informáticos reconhecessem o ano 2000 como o ano 1900. Isso realmente causaria uma enorme desordem no sistema econômico mundial. Os Bancos teriam suas aplicações dando juros negativos, os investidores iriam ter enormes prejuízos, milhares de empresas iriam à falência, etc., significando uma crise maior ainda do que a crise americana de 1929, por isso, nos Estados Unidos muitas pessoas estocaram comida devido ao pânico do desequilíbrio econômico que poderia ser gerado se esta situação se confirmasse.

[19] Joseph Cannataci é relator especial da ONU sobre direito à privacidade.

Mas como os Estados poderiam se unir para coibir as ações de ciberespionagem/cibervigilância se, muitas vezes, eles mesmos as praticam? Seguindo uma linha argumentativa idêntica, Piovesan (2014) afirma que uma alternativa viável seria a criação de um marco regulatório internacional firmado entre os países da ONU para normatizar questões pontuais sobre a proteção de dados.

Por esse ângulo, também observamos a existência de problemas de jurisdição que demostram a imprescindibilidade de uma ação conjunta dos Estados membros da ONU, provavelmente, na forma de um instrumento legal internacional destinado a respeitar e proteger o direito à privacidade no ciberespaço, especialmente em relação a atuação do Estado no âmbito da internet.

A legislação internacional carece de referências à ciberespionagem e, por conseguinte, tal delito não figura, a priori, no rol de crimes previstos pelo Tribunal Penal Internacional–TPI, portanto, não fazem parte da sua competência material jurisdicional, já que de acordo com o artigo 5º do Estatuto de Roma, o TPI apenas julga quatro tipos de crimes: crimes contra a humanidade, crimes de genocídio, crimes de guerra e crimes de agressão.

No ordenamento jurídico brasileiro existem algumas normas infraconstitucionais que tratam de forma esparsa da proteção de dados, (ciber)espionagem/vigilância e dos crimes digitais: o Código Penal(1940) e as alterações realizadas pela Lei Carolina Dieckmann (Lei nº 12.737/12) que tipificaram a invasão de sistema informático[20], o Código Penal Militar (1969), a Lei de Segurança Nacional (1983), a Lei de Responsabilidade Civil e Criminal por atos Relacionados à Atividade Nuclear (1977), a Lei da Interceptação das Comunicações Telefônicas, Informáticas ou Telemáticas (Lei nº 9.296/96), Lei de Acesso à Informação – LIA (Lei nº 12.527/11), a Lei das Comunicações de Dados da Administração Pública Federal Direta, Autárquica e Fundacional (Decreto nº 8.135/13), o Marco Civil da Internet – MCI (Lei nº 12.965/14) , a Lei sobre as condições de permanência e trânsito de forças estrangeiras no território nacional (LC nº 149/2015 que altera a LC nº 90/97), e mais recentemente, a Lei de Proteção de Dados (Lei nº 13.709/18).

A partir desta percepção sobre a proteção de dados, buscamos racionalizar o direito de defesa, ampliando a sua abrangência para alcançar os bens jurídicos intangíveis, pois, na

[20] Invasão de dispositivo informático : Art. 154-A. Invadir 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. (Lei Carolina Dieckmann – Lei nº 12.737/12)

medida que existem condutas reputadas como crimes digitais, também deve existir a possibilidade de agir pautadas através do uso da legítima defesa digital, utilizando-a como técnica de combate aos *cibercrimes* e método de pacificação social, principalmente, em ambientes corporativos onde a informação adquire extrema valorização.

Na realidade, o direito de defesa é algo tão inerente ao ser humano que o próprio instinto encarrega-se de exteriorizá-lo quando torna-se necessário proteger sua integridade física, e bem como, os seus interesses, de tal forma, que pode ser compreendido como princípio e direito fundamental, sendo este potencializado pela tecnologia ao passo que a mesma permite a emancipação do cidadão na gerência dos seus direitos e bens.

Nesse sentido, Pinheiro (2016) preleciona que a prerrogativa da autodefesa é uma causa de justificação que se baseia no princípio de que o Direito não precisa retroceder diante de um injusto. Assim, a defesa não funciona apenas só para proteger o bem jurídico ameaçado, mas também, simultaneamente, para a afirmação da ordem jurídica.

Diante da necessidade de respostas ágeis e eficientes, a legítima defesa digital torna-se a medida mais plausível para prevenir e solucionar os incidentes digitais, pois, nem sempre a atuação estatal poderá ocorrer para inibir de forma hábil e tempestiva estes delitos, de sorte que, até mesmo, o próprio ente estatal pode ser o agente causador destes cibercrimes, pois, os governos estão cada vez mais invasivos ao legitimar medidas intrusivas à privacidade e violadoras de direitos fundamentais, perpetuando um cultura de medo no que tange o combate ao (ciber)terrorismo com o propósito de justificar uma atuação governamental desproporcional e abusiva, muitas vezes, realizada com a colaboração de empresas que detém a geração de conteúdo e de tecnologia digital.

Para exemplificar esta questão, Woloszyn (2018) relembra o caso da Government Communications Headquarters–GCHQ, agência de espionagem britânica, que em conjunto com a NSA, grampeou as comunicações realizadas por cabos de fibra ótica, que incluiam ligações telefônicas e mensagens via e-mails em todo o Reino Unido, no qual, as provas, de caráter documental, apontavam para a estreita colaboração de empresas privadas no fornecimento de dados pessoais ao governo; e o caso Snowden, que comprovou situações de ciberespionagem internacional cujo principal alvo eram as comunicações on-line de autoridades governamentais e até mesmo de cidadãos comuns, sob pretexto de garantir a segurança nacional norte-americana contra o terrorismo e a proteção preventiva contra o uso de armas de destruição em massa por agentes não estatais.

Desta forma, agindo sob a égide da Legítima Defesa Digital, apesar de inicialmente a conduta protetiva poder ser caracterizada como antijurídica ou ilícita, tendo em vista a sua

relação antagônica com o ordenamento jurídico, excepcionalmente, pode ensejar modelos de conduta que servem como justificantes para repelir agressões injustas, inclusive no meio ambiente digital.

Seguindo este entendimento, Greco (2016) afirma que a legítima defesa tem aplicação na proteção de qualquer bem juridicamente tutelado pela lei, seja um bem imaterial ou não, desde que estejam presentes os seus requisitos, estando amparada em critérios de razoabilidadade, proporcionalidade, tempestividade e efetividade da resposta.

Logo, compreendemos que atuar sob a guarida de uma justificante é de extrema relevância para evitar uma eventual responsabilização penal, pois, para que se possa concluir pela constatação do crime conforme a concepção analítica, é preciso que o agente tenha cometido um fato típico, antijurídico e culpável.

Nesse diapasão, as situações jurídicas decorrentes da Era Digital, caracterizam o direito pós-moderno e pós-positivista, convergindo para uma nova possibilidade de hermenêutica jurídica. Desta maneira, o papel da jurisdição ganha ênfase, em geral no que tange a argumentação jurídica e discricionariedade do Poder Judiciário, pois, a norma jurídica se consolida através do intérprete julgador, e é este último o principal responsável por definir e declarar a natureza legal da conduta.

Dentro da nova realidade imposta pela sociedade digital, há a exigência de que o direito reflita na apreciação e julgamento do caso concreto, a respectiva valoração da realidade social, posto que o "Estado se apresenta como catalizador das mudanças sociais e possui a função de efetivar os preceitos constitucionais. Nesse contexto, o Poder Judiciário é o responsável pela vontade da nação consagrada na Constituição." (SIQUEIRA JR., 2013, pag.217).

Os juízes, como expressão do Poder Judiciário, garantem o suporte axiológico decorrente da atividade interpretativa em face da abstração da lei, corporificando-a. Neste ponto, há uma aproximação do direito e da ética, com o consequente afastamento da neutralidade jurídica, pois a obediência cega à lei não encontra mais guarida no direito contemporâneo.

Neste prisma, a prerrogativa da autodefesa em face da sua interpretação volitiva, deve estar de acordo com as exigências das novas situações penais que emergem da sociedade digital, sendo fundamental repensar o papel do Poder Judiciário e da empregabilidade da legislação em consonância com os princípios e os direitos humanos, para cumprir com a função de resgatar valores sociais e proteger os bens jurídicos mais relevantes.

No contexto atual, invadir o sistema informático de *hackers* para recuperar os dados sigilosos furtados pelos cibercriminosos pode resultar na incriminação das próprias vítimas.

Embora, a ciberespionagem internacional seja classificada como delito contra a segurança do Estado, sob a égide da legislação nacional e internacional, conforme aludimos anteriormente no tópico 3.2, observamos que grande margem da sociedade permanece vulnerável a estes ataques.

A ciberespionagem adquire expressividade quando evidencia a prática perpetrada por governos contra governos à obtenção de segredos governamentais, mas por outro ângulo, percebemos que outros dados de cunho relevante são deixados em segundo plano, como os segredos pessoais, comerciais e industriais.

Sendo assim, a Legítima Defesa Digital surge como um recurso legal que não se apresenta apenas como um mero argumento retórico e utilitarista (*The greatest happiness principle*[21]), mas, sobretudo, fundamenta-se na racionalidade jurídica impedindo a violação de normas constitucionais e infraconstitucionais, sejam estas de proteção do indivíduo e/ou da comunidade, preconizando a possibilidade de defesa das vítimas aos ataques criminosos de hackers, sob a égide do direito penal.

[21]Princípio do bem-estar, conforme doutrina ética defendida principalmente pelo jurista e filósofo inglês Jeremy Bentham e pelo economista e filósofo inglês John Stuart, cujo fundamento encontra-se na busca do bem-estar coletivo mesmo que haja sacrifício individual.

4 LEGITIMA DEFESA DIGITAL: NOVAS ABORDAGENS, NOVAS PERSPECTIVAS

4.1 Novo Direito Penal aplicado a Sociedade Digital e privatização da investigação criminal (*criminal compliance*)

As condutas criminosas cometidas através da rede mundial de computadores são cada vez mais comuns. No entanto, o Direito, sobretudo o Penal, com as ferramentas que dispõe hoje, não está totalmente preparado para fazer frente aos desafios do desenvolvimento cibernético em face da criminalidade digital.

Não obstante, ao reconhecer esta debilidade jurídica, observamos uma tendência crescente à funcionalização e expansão do Direito Penal, por meio da administrativização e internacionalização do mesmo, de sorte que este fenômeno vem sendo impulsionado pela globalização, pelo combate à corrupção e pela internet.

A utilização da informática e aumento da conectividade, por meio da internet e dos dispositivos móveis, promove transformações sociais importantes e benéficas, porém, concomitantemente, pode aumentar a criminalidade e provocar o surgimento de novas formas de delitos.

O alcance global e a tecnologia de troca de dados proporcionada pela rede mundial de computadores, possibilitam o dinamismo comercial através da eficiência e rapidez na troca de informações e da inexistência de fronteiras, mas, também “atraem” a prática de crimes, por ser um meio de indução ao anonimato e por trazer algumas características intrínsecas, como a generalidade, as dificuldades de rastreamento, a abrangência potencialmente ilimitada de vítimas e a fragilidade dos meios de tutela penal.

Em particular, a mineração de dados em larga escala e a digitalização dos processos produtivos, tornou-se o foco usual para práticas delituosas. Neste cenário, busca-se mecanismos e procedimentos de prevenção, detecção e remediação de condutas ilícitas para evitar ou minimizar os riscos negociais relativos à segurança da informação.

No campo jurídico, fomenta-se a troca da burocratização, da ausência de infraestrutura técnica policial, da morosidade legislativa e da falta de celeridade dos tribunais, por soluções legalmente palpáveis no que concerne a adaptação prática de institutos já consagrados pelo Direito. “A tendência mundial é promover o desenvolvimento de mecanismos para a gestão dos riscos operacionais, tanto para a sobrevivência da empresa quanto para atender aos órgãos supervisores nacionais e internacionais “(COIMBRA, 2007, p.20).

Logo, para que haja uma eficaz prevenção e repressão dessas condutas modernas, se faz necessária uma maior colaboração entre o setor público e o privado, transferindo, em alguma medida, as incumbências essencialmente estatais de investigação de condutas contrárias ao ordenamento jurídico, sobretudo, as condutas que envolvam ativos intangíveis e sistemas digitais, para a iniciativa privada, principalmente nos casos que envolvam corrupção.

A elaboração de leis contra corrupção, lavagem de dinheiro e proteção de dados em vários países, inclusive no Brasil, demonstra como os governos estão empenhados em eliminar os prejuízos sociais e econômicos decorrentes destes delitos, admitindo para tanto, até mesmo, o compartilhamento da tutela dos bens jurídicos penais com outros *players*. "Deste modo, as funções estatais devem ser preenchidas e repassadas a outros organismos políticos que assumam, de algum modo, uma economia transnacional (HABERMAS.2001, p. 69)".

Assim, a privatização da investigação criminal, também, denominada de *criminal compliance*, vai surgindo como instrumento de prevenção criminal corporativa e de transparência de responsabilidade penal, ao passo que possibilita a individualização das condutas praticadas por todos os *stakeholders* envolvidos na empresa, por meio de princípios e regras básicas instituídas por um contrato profissional, em que há a adesão formal às responsabilidades.

Para Benedetti(2014), a adesão a normas legais(objetivas) e de condutas(subjetivas) torna possível a individualização de ilícitos nas corporações com maior segurança jurídica, possibilitando que o Direito Penal cumpra o seu real papel, respeitando os princípios, sem que haja a flexibilização de garantias humanas, e evitando a sua expansão exagerada, através do Direito de Intervenção e do Direito Penal do inimigo, pois, de fato, a sociedade contemporânea necessita de um Direito Penal forte e efetivo, que tenha caráter cientifico e preventivo, e não fragilizado por medidas epistemologicamente rasas, que não beneficiam e protegem a atual sociedade de risco.

Particularmente, o perfil político-constitucional brasileiro aponta que o Estado Democrático de Direito decorre de um princípio maior, qual seja, a dignidade da pessoa humana, valor supremo e fundamento de nossa República, do qual infere-se que o Direito Penal não deverá ser instrumento de opressão, mas uma ferramenta necessária à correta e adequada aplicação da justiça e proteção dos bens jurídicos, sejam estes bens tangíveis ou intangíveis.

De fato, a controvérsia sobre a possibilidade de responsabilização penal da Pessoa Jurídica emerge em vários países, sendo objeto de profundo debate no âmbito europeu. Segundo Pineda (2018), no direito comparado encontramos modelos distintos de responsabilidade, posto que na Alemanha a punição da Pessoa Jurídica é apenas administrativa, enquanto que a Itália

adota um sistema híbrido, já em Portugal as mesmas só poderão ser responsabilizadas penalmente por determinados delitos, no entanto, na França, Bélgica e Holanda, as Pessoas Jurídicas poderão ser responsabilizadas por qualquer infração prevista na legislação penal, todavia, na Espanha, estas só serão punidas pelos delitos expressamente previstos na lei penal.

Essas diferentes interpretações existiam, pois, não havia um consenso no bloco europeu sobre como responsabilizar as Pessoas Jurídicas por ataques a sistemas de informação, de modo que, ficaria a critério de cada Estado definir a sua forma de responsabilização conforme o art. 8 da DM 2005/222/JAI[22] do Conselho da União Europeia.

De acordo com Pineda (2018), embora os instrumentos internacionais não exigissem a responsabilização penal da pessoa jurídica, a Espanha foi precursora na criminalização dos incidentes informáticos, adaptando o seu ordenamento jurídico penal, para incorporar ciberdelitos puros de *hacking* e danos a sistemas informáticos, abandonando o princípio "*societas delinquere non potest"* para incorporar o "*societas delinquere et puniri potest*", por meio da reforma realizada pela LO 5/2010 e posteriormente pela LO 1/2015, tendo está ultima influência da Diretiva 20123/40 do Parlamento Europeu e do Conselho da União Europeia, que substitui a DM 2005/222/JAI, e aborda como tema os ataques contra sistemas de informação.

De certo é importante lembrar, que o presente trabalho não tem por objeto dissecar o instituto da Pessoa Jurídica e de sua responsabilidade penal, no entanto, propõe-se a demonstrar as mudanças na persecução penal introduzidas pelos fenômenos da sociedade digital.

Nesse sentido, "*se trata de incentivar que las personas jurídicas suman uma autoorganización para impedir modelos delictivos com el fin de lograr sus objetivos sociales, intentando así que la persona jurídica sea quien adopte las medidas para investigar y evitar las conductas que le puedan favorecer pero que sean delictivas*[23]. (DOPICO GÓMEZ-ALEER, 2010,p.12). De tal modo que, "*La estrutura compleja de las empresas dificultaba la*

[22] Artigo 8. Responsabilidade das pessoas colectivas: 1) Cada Estado-Membro deve tomar as medidas necessárias para assegurar que as pessoas colectivas possam ser consideradas responsáveis pelas infracções referidas nos artigos 2., 3. 4. e 5., praticadas em seu benefício por qualquer pessoa, agindo individualmente ou enquanto integrando um órgão da pessoa colectiva, que nela ocupe uma posição dominante baseada: a) Nos seus poderes de representação da pessoa colectiva; ou b) No seu poder para tomar decisões em nome da pessoa colectiva; ou c) Na sua autoridade para exercer controlo dentro da pessoa colectiva; 2) Para além dos casos previstos no n.o 1, os Estados-Membros devem assegurar que uma pessoa colectiva possa ser considerada responsável sempre que a falta de vigilância ou de controlo por parte de uma pessoa referida no n.o 1 tenha tornado possível a prática, por uma pessoa que lhe esteja subordinada, das infracções referidas nos artigos 2., 3., 4. e 5., em benefício dessa pessoa colectiva; 3) A responsabilidade de uma pessoa colectiva nos termos dos n.os 1 e 2 não exclui a instauração de procedimento penal contra as pessoas singulares envolvidas na qualidade de autoras, instigadoras ou cúmplices nas infracções referidas nos artigos 2., 3., 4. e 5.

[23]Trata-se de incentivar que as pessoas jurídicas adquiram uma auto-organização para impedir modelos delitivos com o fim de alcançar seus objetivos sociais, possibilitando que a pessoa jurídica adote medida para investigar e evitar condutas criminosas que possam lhe favorecer.

investigación de los delitos cometidos em su seno o desplazaba la responsabilidade hacia niveles inferiores. Por ello, se intenta evitar su impunidad y, además de la previsión de uma pena, se obliga a las sociedades a sumir determinadas medidas, actuando también desde el plano preventivo.[24]*"* (JUANES PECES, 2015, Pag 183).

Em consonância com a tendência europeia, que corrobora com a responsabilização da pessoa jurídica em matéria penal por cibercrimes que violam o sistema informático, e em conformidade com as orientações internacionais sobre sistema de controles internos que foram propagadas pelas leis americanas Sarbenes Oxly, também conhecida como Sox, e a Foreing Account Tax Compliance Act (FATCA), que visam combater a corrupção e a evasão fiscal, juntamente com a GDPR, criada pela União Europeia para propiciar a proteção de dados, está sendo desenvolvida no Brasil, uma crescente atividade legislativa e regulamentar, a fim de adaptar o modelo legislativo brasileiro ao novo padrão de segurança empresarial internacional.

Embora estas leis, geralmente, possuam jurisdição apenas nos países onde foram elaboradas, a partir de uma visão geral, observamos uma certa convergência em relação a outros governos e países na criação de leis mais rígidas, não, simplesmente, por estes países seguirem os modelos americanos e europeus, posto que são países mais desenvolvidos, mas, por verificar que as economias e sociedades contemporâneas enfrentam desafios comuns, e que a movimentação em massa de dados pertencentes a industrias, empresas, consumidores e governos exige uma legislação que possa ser aplicada em todos os setores da economia, e também, em outros países, pois, os padrões de *compliance* devem ser observados por quem atua nas matrizes e em suas filiais, sendo estas filiais, muitas vezes, estrangeiras.

O Brasil seguiu este padrão de fiscalização e criou a Lei Contra Corrupção ou Lei da Empresa Limpa (Lei nº 12.846/13), por sua vez, alterando a Lei dos Crimes de Lavagem ou Ocultação de Bens, Direitos e Valores (Lei nº 9.613/98), a fim de criar o Conselho de Controle de Atividades Financeiras – Coaf para disciplinar, identificar e punir atividades ilícitas neste setor, bem como, definir uma série de deveres de *compliance* a serem seguidos pelas corporações, muito embora, não tenha utilizado este termo na dicção legal.

Seguindo este importante passo, em virtude dos escândalos de corrupção envolvendo empresas (nacionais e estrangeiras) e o governo brasileiro, muitos deles desvencilhados a partir da Operação Lava Jato, foi criada pelo governo do Distrito Federal, a Lei nº 6.112/18 que exige

[24] A estrutura das empresas dificultava a investigação de condutas criminosas cometidas no seu interior ou deslocava a sua responsabilidade para níveis hierárquicos inferiores. Portanto, tentando evitar a impunidade, além da previsão de uma penalidade, as empresas são obrigadas a tomar certas medidas, atuando também a partir do plano preventivo.

a obrigatoriedade da implantação de programas de integridades nas empresas que contratem com todas as esferas de Poder da Administração Pública do Distrito Federal, definindo como deverá ser desempenhado o trabalho do *compliance officer* nestas empresas, de sorte que os Estados brasileiros devem, a longo prazo, seguir esta mesma tendência fiscalizatória em suas contratações.

Além de exigir a obrigatoriedade da implementação de programas de integridade nas empresas a partir de 1 de junho de 2019, a Lei do Distrito Federal aproxima-se das recomendações internacionais traçadas pela Lei Modelo da UNCITRAL sobre Comércio Eletrônico[25], quando passa a dar preferência a documentos em meios digitais, para avaliar e comprovar a conformidade dos programas de integridade, em harmonia com o disposto no art.9[26] da referida Lei Modelo, que afirma a admissibilidade e força probante das mensagens de dados.

Ressalte-se que a Lei Modelo da Comissão das Nações Unidas para o Direito do Comércio Internacional criada em 1996, não definiu especificamente o significado de "comércio eletrônico". (FARIAS, 2002, pag. 198). Contudo, esta lei reconhece que a maioria das informações e comunicações comerciais, empresariais e institucionais são realizadas por meio digital, de modo que devemos zelar pela sua integralidade, disponibilidade, confidencialidade, autenticidade, legalidade e aceitabilidade como meio de prova.

No âmbito brasileiro, embora o Marco Civil da Internet – MCI (Lei nº 12.965/2014 c/c Decreto nº 8.771/2016), não seja uma lei geral de proteção de dados pessoais, tem-se que algumas regras principiológicas já deviam ser observadas pelas empresas em nível de *compliance* para evitar a criação de um "passivo digital" por meio da busca de um modelo de negócio menos invasivo a privacidade. Agora, com a publicação e regulamentação da Lei Geral de Proteção de Dados Pessoais Brasileira – LGPDP (Lei nº 13.709/18 c/c a MP nº 869/18) que alterou o MCI, estas regras passam a ter caráter normativo, de modo que, as empresas devem obrigatoriamente se adequar aos padrões legais de *compliance* exigidos.

---

[25] Resolução 51/162 criada pela Comissão das Nações Unidas sobre o Direito do Comércio Internacional – UNCITRAL, na Assembléia Geral da Organização da Nações Unidas, em 16 de dezembro de 1996, na cidade de Nova York – USA.

[26] Artigo 9 - Admissibilidade e força probante das mensagens de dados: 1) Em procedimentos judiciais, administrativos ou arbitrais não se aplicará nenhuma norma jurídica que seja óbice à admissibilidade de mensagens eletrônicas como meio de prova: a) Pelo simples fato de serem mensagens eletrônicas; ou, b) Pela simples razão de não haverem sido apresentadas em sua forma original, sempre que tais mensagens sejam a melhor prova que se possa razoavelmente esperar da pessoa que as apresente; 2) Toda informação apresentada sob a forma de mensagem eletrônica gozará da devida força probante. Na avaliação da força probante de uma mensagem eletrônica, dar-se-á atenção à confiabilidade da forma em que a mensagem haja sido gerado, armazenada e transmitida, a confiabilidade da forma em que se haja conservado a integridade da informação, a forma pela qual haja se haja identificado o remetente e a qualquer outro fator pertinente.

No entanto, para Silva (2017), quanto a este aspecto, vale frisar que o Marco Civil da Internet, como lei que determina a guarda de dados de conexão no Brasil, apresenta alguns vícios, pois, foi inspirado na legislação anterior ao regulamento europeu General Data Protection Regulation – GDPR[27], qual seja a Diretiva nº 2006/24/CE do Parlamento Europeu, publicada no dia 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas, sendo esta invalidada pelo próprio Tribunal Europeu, logo após o Tribunal Constitucional Federal da Alemanha questionar a sua aplicação no âmbito interno, declarando a Diretiva nº 2006/24/CE inconstitucional por violar de maneira grave e desproporcional os direitos da vida privada e a proteção de dados pessoais, por não delimitar regras e prazos razoáveis sobre o gerenciamento desses dados.

Neste caso, a LGPDP brasileira ingressou no mundo jurídico em um momento bastante propício, posto que, foi sancionada pelo presidente Michel Temer em 14 de agosto de 2018, posteriormente a entrada em vigor da GPDR Europeia em 25 de março de 2018, colocando o Brasil em grande avanço nas discussões sobre proteção de dados e incentivando a rápida a adequação das empresas as novas regras, apesar de entrar em vigor efetivamente apenas em 2020, pois, precisará passar por um período de adaptação de 18 meses.

Fato é, que em apertada síntese, observamos um movimento uníssono de renovação do Direito Penal, que acaba por ensejar a edição de novas leis e novos tipos penais, mas, também torna possível a aplicação dos institutos jurídicos já existentes. Como exemplo, temos a adaptação da legítima defesa tradicional à ótica do Direito Penal Digital, que se apresenta como uma das alternativas de *criminal compliance* e de defesa cibernética, para assegurar a atuação de grupos de respostas a incidentes, combater a impunidade gerada pelos crimes digitais, propiciar a colheita de provas por meio do rastreamento de condutas e resguardar a inviolabilidade das informações através do uso da Legítima Defesa Digital (*Digital Self Defense*).

4.2 Legítima defesa digital: Conceito e elementos

O instituto da legítima defesa não é algo novo. O próprio instinto humano encarrega-se de exteriorizá-lo quando necessário para defesa de sua integridade física e bem como dos

[27] Lei de Proteção de Dados da União Europeia que visa incentivar o Mercado Único Digital no bloco econômico europeu, estabelecendo a confiança dos consumidores nas empresas e nos serviços on line ao definir novos requisitos de compliance, no setor.

seus interesses. Sendo algo inerente ao homem, vem sofrendo modificações, buscando adequar-se à evolução humana e as suas necessidades.

Dentro de uma nova perspectiva da sociedade digital, faz-se mister repensar e aprimorar alguns princípios jurídicos, muitos deles considerados basilares para a ciência do direito, bem como suscitar os valores inerentes a tais princípios, já que os mesmos motivaram a existência das leis que se encontram em vigor.

As novas situações jurídicas decorrentes da Era Digital convergem para uma nova possibilidade de hermenêutica jurídica. Partindo do pressuposto de que as novas situações merecem novas respostas, torna-se inteiramente natural pensar que uma infração ou conflito de direito cometido em ambiente virtual, pode e deve ensejar um ato protetivo da vítima na defesa de seus interesses.

Com a proliferação do fenômeno da internet passa a serem comuns situações ilícitas contra pessoas físicas e jurídicas em ambientes eletrônicos e informatizados (espionagem, sequestro de dados, roubo de informações e etc.). Enquanto os números de crimes virtuais crescem, gradativamente percebemos que as ações de legítima defesa digital também evoluem, de modo que, se estas ações não forem disciplinadas e praticadas de maneira responsável, contribuirão para formar uma conjuntura de instabilidade e insegurança no meio digital.

Os cibercrimes não afetam apenas os bens jurídicos individuais como também os coletivos (lesão a direitos difusos), à exemplo da liberdade informática e a segurança no tráfico de informação. Deste modo, a cibernética para a doutrina majoritária está inserida nos direitos de 3ª dimensão, embora que para alguns doutrinadores seja considerada como direito pertencente a 5ª dimensão de direitos e garantias fundamentais.

A Terceira geração ou terceira dimensão de direitos e garantias fundamentais foram desenvolvidas no século XX, e estão ligados aos Direitos da Fraternidade, relacionando-se a um profundo humanismo e ao ideal de uma sociedade mais justa e solidária, ou seja, são os direitos difusos ou coletivos (ex.: direito a um meio ambiente equilibrado, uma saudável qualidade de vida, progresso, dentre outros). Deste modo, tornar-se-á pertinente questionar sobre a legítima defesa em ambientes de sistemas informatizados, como, por exemplo, na internet, sendo de fundamental importância traçar os limites da atuação de defesa para que esta não seja considerada infração.

Tomando como parâmetro a legislação brasileira, sabemos que no Brasil, o princípio da inafastabilidade da jurisdição está consagrado constitucionalmente no art.5, XXXV da Constituição Federal/88. Entretanto, nem sempre o Estado estará presente para exercer a sua função pacificadora. Deste modo, foi resguardado pela lei ao cidadão o direito à legítima defesa.

Contudo, Grecco (2016) afirma que tal permissão não é ilimitada, pois que encontra suas regras na própria lei penal. Desta forma, a legítima defesa jamais poderá ser confundida com vingança privada, pois seria preciso que o agente estivesse diante de uma situação de total impossibilidade de recorrer ao Estado, responsável constitucionalmente pela segurança pública, e, só assim, uma vez presentes os requisitos legais de ordem objetiva e subjetiva, agir em sua defesa ou na defesa de terceiros.

Nesta senda, nos filamos à teoria da legítima defesa digital que é a mesma preceituada no art. 25 do Código Penal Brasileiro, tendo os mesmos pressupostos (agressão injusta, atual ou iminente; meios necessários e a defesa de direito seu ou de outrem – animus defendi), porém, ocorrida em meio diverso, qual seja o meio virtual ou não presencial.

Sendo assim, o art.25 do Código Penal Brasileiro define: "Entende-se em legítima defesa quem, usando moderadamente dos meios necessários, repele injusta agressão, atual e iminente, a direito seu ou de outrem". Partindo do princípio de que o crime de acordo com a teoria analítica é uma estrutura que pode ser tripartida em fato típico, antijurídico e culpável, assim, a legítima defesa sendo causa de justificação e bem como discriminante putativa exclui a possibilidade de caracterização do ilícito, muito embora o fato possa ser considerado típico.

Nesse diapasão, se existem situações ocorridas em ambiente virtual e, portanto não presencial, que podem ser compreendidas como crime, amoldando-se ao sistema analítico, então estas situações denominadas como cibercrimes também podem abrigar-se sob a guarida das excludentes, pois, o direito não deve retroceder diante de um injusto.

Na realidade da sociedade digital, o conceito de legitima defesa em *stricto sensu* adequa-se juridicamente as situações lesivas ocorridas virtualmente. "A defesa vale, pois, não só para o bem jurídico ameaçado, mas também, simultaneamente, para a afirmação da ordem jurídica". (PINHEIRO, 2016, p 242).

Pretende-se declinar com o acima exposto, que utilizando do conceito legal desprendido do art. 25 do Código Penal Brasileiro, temos os pressupostos da legítima defesa em *stricto sensu* (agressão injusta, atual ou iminente; meios necessários e a defesa de direito seu ou de outrem – animus defendi), podendo ser compreendido em *lato sensu*, como elementos da legítima defesa digital, já que o único diferencial é que esta ocorre em meio diverso, qual seja o meio virtual ou não presencial, sendo a teoria da legítima defesa digital perfeitamente compatível com a visão garantista do ordenamento jurídico brasileiro.

4.2.1 Agressão injusta: crimes digitais (Incidentes de Segurança)

O sistema informático, como fruto da revolução tecnológica, vem provocando inúmeras indagações no campo jurídico, principalmente no que diz respeito ao Direito Penal. A internet, por sua vez, torna-se um campo fértil para a proliferação da marginalidade digital, devido à noção errônea de anonimato que paira sobre o meio cibernético.

São altos os índices de pedofilia, espionagem, fraude, estelionato, extorsão, entre outros crimes cometidos através da internet que nos leva a constatação de que a maioria dos crimes realizados em ambiente virtual são condutas já tipificadas no mundo real, apresentando modalidades distintas dependendo do bem jurídico tutelado. “Portanto, as questões quanto ao conceito de crime, delito, ato e efeito são as mesmas, quer sejam aplicadas para o Direito Penal ou para o Direito Penal Digital”. (PINHEIRO, 2016, p.226).

Em decorrência do alcance extraterritorial das condutas delitivas e da cooperação público-privada que resulta na privatização da investigação criminal, percebemos que as principais inovações jurídicas trazidas no âmbito digital para o Direito Penal se referem a territorialidade e a investigação probatória, bem como a necessidade de tipificação de algumas modalidades que, em razão de suas peculiaridades merecem ter um tipo penal específico, até porque o princípio da legalidade deve ser rigorosamente observado neste setor. Não obstante, a especialização do tema é evidente quando tratamos do aspecto criminológico em sistemas teóricos e operacionalmente complexos. Tal fator gera certa apreensão social, econômica e política por evidenciar as vulnerabilidades e armadilhas encontradas no mundo virtual. De modo que, muitas vezes os usuários assumem a postura de vítimas potencias devido à pouca formação intelectual, a falta de habilidade com o hardware ou, simplesmente, por negligenciarem aspectos mínimos de segurança, como não compartilhar senhas, ler atentamente termos de uso e confirmar em várias fontes a veracidade das informações.

Nesse sentido, a complexidade dos sistemas informatizados é apontada como um dos fatores que provocam a insegurança nos ambientes virtuais, porém, a insegurança não constitui um óbice para que as pessoas interajam neste ambiente, tendo em vista que a conectividade e o uso fluem sem que haja uma preocupação com o uso de boas práticas e regras de conduta. “O comércio eletrônico, por exemplo, não irá esperar por clientes com plataformas ótimas em segurança, ou usuários altamente treinados”. (MARTINI. 2008, p.152).

Para Westerman e Hunter (2008), quase todo processo e relacionamento comercial é sustentado pela TI, portanto, há muito mais em jogo na gestão do risco de TI do que todo o capital que as empresas investem em tecnologia. Quando o risco de TI é tratado como uma

questão de observância, ele é apenas um custo a ser administrado. Mas se for tratado da maneira certa, discutindo-se o risco de TI em termos comerciais, ele passa a ser mais do que isso. Ele pode gerar valor aos negócios de três maneiras: reduzindo "incêndios" da TI, tornando o alicerce mais eficiente e capacitando a empresa a buscar oportunidades comerciais valiosas que os concorrentes poderiam considerar arriscadas demais para tentar.

A fim de facilitar a compreensão, faremos uso de um caso clássico. Imaginemos que uma grande corporação fez altos investimentos financeiros em P&D para melhorar o seu produto. Após longo período de tempo e trabalho na pesquisa, a empresa obteve êxito com a inciativa, porém, seus sistemas eletrônicos foram invadidos ilicitamente, tendo seus dados sigilosos "furtados" por um hacker contratado por uma empresa concorrente; ao constatar-se vítima de referido crime, a corporação aciona o departamento de gerenciamento de riscos e resposta a incidentes, que localiza o criminoso digital através dos rastros deixados e invade seus sistemas com o propósito de trazer de volta os dados que pertenciam à corporação.

Sob uma primeira análise leiga, a conduta acima descrita seria tão somente a prática da justiça, contudo sob o aspecto legal, se considerarmos a possibilidade de responsabilização, a questão não é tão simples assim. A perda financeira ou perda de reputação que uma instituição pode sofrer como resultado de falhas no cumprimento de leis, regulamentações, códigos de conduta e Gestão de Riscos poderá ser minimizada em virtude da velocidade e qualidade da resposta a tais contingências. Tendo em vista que cada ação fora do procedimento pode colocar o negócio em risco é preciso alinhar o perfil do profissional com o perfil da organização a fim de evitar processos judiciais.

Para realização deste feito, os setores (Jurídico, *Compliance* e Tecnologia da Informação – TI) devem estar em completa sinergia no combate à criminalidade digital e repressão aos incidentes de segurança. Um dos fatores que legitimam a situação de defesa é a caracterização de uma agressão injusta, ou seja, um ato humano que lese direito/bem seu ou de outrem e que não esteja amparado pelo ordenamento jurídico, sendo necessário um ato efetivo e não tão somente uma provocação para possibilitar ao agredido defender-se de acordo com os limites legais.

No campo digital, esta agressão injusta se consubstancia na maioria das vezes em um incidente de segurança, ou seja, numa ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo tratado pela política de segurança sobre um sistema informático. Estes incidentes podem ser ocasionados por ataques externos a partir de uma ação hacker, mas, principalmente, pode advir de fragilidades internas ocasionadas por negligência ou ações ilícitas desenvolvidas pelos próprios envolvidos na atividade empresarial e seus colaboradores.

Ante tal cenário, não surpreende o anacronismo vivido pelo Direito Penal. Fundamentado nos princípios liberais do iluminismo e de cunho marcadamente antropocêntrico. O Direito Penal foi elaborado para tutelar bens jurídicos tradicionais como a vida, a integridade física, a saúde e o patrimônio tangível, enquanto que, no atual universo pós-moderno, as ações humanas, potencializadas pelo desenvolvimento da razão técnico-instrumental, alcançam novas dimensões, em relação de espaço-tempo peculiares, em que os riscos globalizam-se e geram danos muitas vezes diferidos, atingindo novos bens jurídicos, sendo estes bens não necessariamente tangíveis.

Na opinião de Greco (2016), a proteção de bens intangíveis não obsta a legítima defesa, pois, tem-se entendido que o instituto podes ser aplicado para proteger qualquer bem juridicamente tutelado pela lei. Assim, pode-se, tranquilamente, desde que presente seus requisitos, alegar a legítima defesa no amparo daquelas condutas que defendam seus bens, materiais ou não.

É cediço, que quanto a esta regra de que todos os bens são suscetíveis de defesa pelo ofendido, para tanto, deve-se trazer a colação a peculiaridade existente no caso dos bens comunitários, em que tais bens constituem exceção à regra, a menos que para sua defesa o ofendido não tenha tempo suficiente ou não possa procurar o necessário amparo das autoridades constituídas para tanto.

Embora a rede mundial de computadores seja aberta e, portanto, considerada um bem comunitário, é notório que nela há esferas privadas, pois, as instituições que regulam o seu funcionamento concedem permissões ou promovem concessões de uso, bem como é inegável que os usuários da rede devem ter a sua privacidade e integridade moral-psicológica resguardada em face das agressões, ataques e vandalismos frequentes na rede, de certo que estes incidentes não podem ficar impunes e podem ser suscetíveis do uso da legítima defesa digital.

Já é pacífico nos tribunais o entendimento de que a pessoa jurídica pode sofrer dano moral em conformidade com o art. 52 do Código Civil Brasileiro[28] e da Súmula 227 do Superior Tribunal de Justiça – STJ. Em frequentes julgados, o próprio STJ vem reafirmando o entendimento de que a condenação por danos morais sofridos por pessoa jurídica exige comprovação fática, ainda que seja possível a utilização de presunções e regras de experiência para configuração do dano, de sorte que deve haver a comprovação de danos à imagem e honra objetiva da empresa, algo que varia de caso a caso e precisa ser observado pelo magistrado

[28]Art. 52 CC/02 (Lei nº 10.406/02): Aplica-se às pessoas jurídicas, no que couber, a proteção dos direitos da personalidade.

responsável pela demanda.[29] Tendo em vista que os incidentes digitais podem gerar danos financeiros e reputacionais, o instituto da legítima defesa digital seria a medida mais plausível para tentar coibir crimes digitais e colher provas eletrônicas.

No caso das intranets, por estas serem redes coorporativas se enquadram perfeitamente ao instituto da legitima defesa e são alvos potenciais da atividade criminosa dos hackers, tendo em vista que muitos destes são contratados por empresas concorrentes ou até mesmo por entidades governamentais rivais para promover incidentes de segurança. Nesse caso, diante da dificuldade operacional e técnica para proteger estes bens, o conceito de legítima defesa digital ganha força e passa a estar inserido nas diretrizes de segurança da informação como elemento estratégico de *compliance* corporativa, visto que, o fenômeno de expansionismo e Administrativização do Direito Penal aumenta a responsabilidade dos gestores das empresas.

Conforme salienta Benedetti (2014), a chamada "Sociedade do Risco", aumenta cada vez mais a exposição dos gestores de uma empresa em responder, na qualidade de réus, a condutas delitivas que não necessariamente foram por eles praticadas, mas que o expansionismo do Direito Penal tem frequentemente determinado como resposta aos anseios da sociedade moderna, contemporânea e globalizada.

Ressalte-se que, não devemos confundir os erros humanos e falhas técnicas eventuais com a atividade com fim delituoso. Neste caso, a problemática maior seria a descrença da sociedade não só na apuração e punição destes cibercrimes como também nos delitos em geral, culminando na ausência de denúncias e consequente dificuldade em traçar um perfil real sobre criminosos, vítimas e crimes mais frequentes. No entanto, são poucas as equipes de profissionais preparados para a investigação dos casos de delinquência informática, ou seja, daqueles crimes que ocorrem em sistemas informáticos ou que utilizam o meio virtual para a consecução do intento criminoso, sendo indispensável a criação de setores de "polícia privada" para prevenir e coibir a criminalidade digital.

Tal mudança de postura é necessária para que possamos ter uma sociedade digital segura; caso contrário, coloca-se em risco o próprio ordenamento jurídico, já que assim como os civis e as empresas, os criminosos aderiram as facilidades e maravilhas do mundo digital e

[29]RECURSO ESPECIAL nº 1.637.629 - PE (2014/0019878-8) – Acórdão/ Relatora: Ministra Nancy Andrighi. https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1560960&num_registro=201400198788&data=20161209&formato=PDF

principalmente da Internet, concorrendo para a proliferação vertiginosa da marginalidade neste ambiente.

4.2.2 Respostas aos Incidentes de segurança: meios necessários para evitar incidentes

A profunda deficiência de conhecimentos mínimos de linguagem informática de grande parte da sociedade brasileira, que ocorre também no meio jurídico, e a discrepância da velocidade existente entre o desenvolvimento das Ciências da Computação e do Direito tornam ainda mais complexa a possibilidade de resposta aos incidentes de segurança digital.

A agressão injusta nos delitos informáticos assume o conceito de incidente de segurança, devendo haver proporcionalidade entre o incidente de segurança sofrido e o meio utilizado para cessá-lo, para não incorrermos na hipótese de excesso de legítima defesa punível.

"A legítima defesa, porém, é uma reação humana, e por tal razão, não se pode medi-la com um transferidor, milimetricamente, quanto à proporcionalidade de defesa ao ataque sofrido pelo sujeito". (MIRABETE, 1994. p.177). No caso dos crimes informáticos esta aferição é bastante complexa, pois, existe uma linha bastante tênue que separa a moderação do seu excesso.

Para Greco (2016), os princípios reitores, destinados à aferição da necessidade dos meios empregados pelo agente na sua defesa, são o da proporcionalidade e o da razoabilidade. A reação deve ser proporcional ao ataque, bem como deve ser razoável. Caso contrário, devemos nos perguntar se o meio utilizado é necessário e, como consequência lógica, afastar a exclusão da ilicitude.

Assim, a legítima defesa digital consiste na utilização pelo agente, contra incidentes de segurança, de uma resposta moderada e necessária, na defesa da integridade e resguardo de informações dispostas em um sistema informatizado. Para a incidência da causa excludente de ilicitude em comento, deve o ofendido agir com moderação para repelir a injusta agressão.

Jesus e Milagre (2016), prelecionam que as vítimas, sejam estas pessoas físicas ou jurídicas, podem, em caso de detecção de um ataque ou incidente informático em andamento, constituindo, pois, uma agressão injusta, buscar interromper o ataque, mas também apurar a autoria por meio de provas que podem ser produzidas em uma espécie de contra-ataque realizado com supedâneo na tecnologia digital existente, considerando que muitas empresas atualmente têm conhecimentos e equipes de resposta a incidentes aptas a identificar ataques em tempo de execução.

Nesse sentido, as grandes empresas e corporações, principalmente os bancos, já se utilizam da política de governança empresarial em que se contrata uma equipe multidisciplinar, denominada de grupo de gerenciamento de risco para coibir as atividades criminosas realizadas por meios computacionais. Os grupos de gerenciamento de risco geralmente são compostos por analistas de sistemas, cientistas da informação, administradores, economistas e advogados, formando então, um grupo de profissionais especialistas em tecnologia da informação – TI e segurança da informação – SI como uma verdadeira "liga da justiça" dos delitos virtuais.

A existência de um grupo de resposta a incidentes é extremamente necessária para evitar que quem se utilize da legítima defesa digital recaia em excessos, sendo, consequentemente, responsabilizado por eles. De fato, a legítima defesa digital por analogia pode ser entendida como legítima defesa em sentido stricto, porém, deve ser mais bem regulamentada para não gerar arbitrariedades e dar ensejo ao tão temido caos jurídico-virtual.

É necessário, pois, a criação de um grupo responsável para coibir os incidentes de segurança, de modo que, não devemos aprovar as ações de "justiceiros virtuais". Assim, combatemos, também, como forma de prevenção, os leigos que pretendem fazer justiça sob a excusa da legítima defesa digital, mas que, no entanto, se igualam aos criminosos digitais, por utilizarem-se das mesmas práticas ilícitas de maneira irresponsável e arbitrária.

Deste modo, percebemos que a legítima defesa digital já é uma realidade no ambiente corporativo de grandes empresas transnacionais. E com razão, as empresas e corporações se utilizam deste instituto. pois, a legítima defesa atinge o propósito de proteção dos ativos intangíveis da empresa, bem como resguarda a corporação de qualquer prejuízo econômico, reputacional ou penalidade jurídica que venha a sofrer por ilícitos perpetrados através de suas atividades, pois, estará agindo em completa conformidade com a lei nas suas atividades de defesa cibernética.

Como bem nos lembra Pinheiro (2016), a defesa da vítima ou a ação de outro que venha a responder ao ataque, não será passível de punição se sua atitude se enquadrar em legítima defesa. Neste sentido aplica-se o brocardo jurídico que afirma "*nemo expectare tenetur donec percutietur*", que significa que ninguém (para defender-se) está obrigado a esperar até que seja atingido por um golpe.

É bem verdade que, o Direito Digital não evolui na mesma velocidade que o desenvolvimento tecnológico. No entanto, deve-se reconhecer que se faz mister a regulamentação de aspectos jurídicos já identificados a nível corporativo e empresarial. De sorte que, a legítima defesa digital merece ser regulamenta pois já faz parte do cotidiano das grandes empresas e corporações transnacionais.

Sendo assim, por merecer uma maior habilidade técnica e operacional, esta ação responsiva deverá ser ampliada aos poucos, restringindo-se inicialmente aos ambientes corporativos, para que no futuro possa atingir o meio social em sua totalidade, pois, a comunidade em geral ainda não está preparada para a utilização deste instituto, de modo que, devemos restringir o uso da legítima defesa digital à atuação de profissionais competentes, sendo iminente a regulamentação desta atividade.

4.2.3 Atualidade e iminência da agressão: a relativização do conceito de tempo e espaço na Era Digital

Na era digital mudanças são cada vez mais frequentes, ocorrendo tão velozmente que as esferas político-econômico-jurídicas custam a acompanhá-las. Adequamos ao sistema tridimensional (fato, valor e norma) criado por Realle (1999), o elemento temporal, formando um sistema quadrimensional (fato, valor, norma e tempo) para facilitar a abordagem do direito no mundo tecnológico e, para nos adequarmos, assim, a mais nova especialização do direito: o Direito Digital.

Neste sentido, Pinheiro (2016, p 37) aduz que a aplicação da fórmula tridimensional do direito adicionada do elemento "Tempo" resulta no Direito Digital. Esse quarto elemento é determinante para estabelecer as obrigações e limites de responsabilidades entre as partes, quer seja no aspecto dos contratos, serviços, direitos autorais, quer seja na proteção da própria credibilidade jurídica quanto a sua capacidade em dar soluções efetivas e ágeis aos conflitos oriundos da Era da Informação.

Do mesmo entendimento comunga o Dr. Renato da Silveira Martini, Ex-Diretor Presidente do Instituto Nacional de Tecnologia da Informação (Casa Civil), órgão federal que executa as políticas de certificação digital no Brasil, ao asseverar que devemos sair do labirinto clássico da Filosofia do direito que representa a mera e simples escolha entre as dimensões (fatos-normas-valores), pois, "se a desmaterialização é um fato, um estado das coisas (*Sachverhalt*), com seus sistemas técnicos e informatizados, encontra-se, também aos seu lado, as regras jurídicas."(MARTINI, 2008,p.08)

Portanto, os termos "atualidade" e "iminência" passam a ser entendidos sob uma nova dinâmica hermenêutica, pois, atual é a agressão que está acontecendo; e iminente é aquela que está prestes a acontecer. Tais conceitos não resolvem, em determinadas situações, casos de ordem prática que podem ocorrer no dia-a-dia daqueles que militam perante a Justiça Criminal,

de modo que, é necessária uma atualização destes conceitos à realidade vivenciada na Era Digital (GRECO, 2016, p.350).

O próprio jurista Miguel Reale (1999), preleciona que a integração dos três elementos na criação da experiência jurídica (o axiológico, o fático e o técnico-formal) revela-nos a precariedade de qualquer compreensão do Direito isoladamente como fato, valor ou como norma, e, de maneira especial, o equívoco de uma compreensão do Direito como pura forma, insuscetível de albergar as infinitas e conflitantes possibilidades dos interesses humanos.

Deste modo, o Direito não pode ser interpretado como uma fórmula matemática, devendo a respeitável tricotomia, cuja compreensão do Direito tem em vista a sua vinculação social e aos valores, ser encarada sob mais um aspecto, qual seja o temporal. Os pontos de vista sociológico, lógico, filosófico e temporal, possibilitam entender o Direito na sua totalidade como atualização frequente do sentido de Justiça e dos valores, determinando, com possível rigor, o significado do Direito à luz da experiência social e histórica do homem.

Sob o ângulo axiológico do direito, Reale (1999) declara que a conhecida parêmia *ex fato oritur jus* não deve ser interpretada no sentido físico, como uma causa que gera um efeito, mas no sentido valorativo que se encerra no encontro ideal do justo, com o fato concreto posto como sua condição, buscando a adequação da norma jurídica as circunstâncias espaço-temporais.

Composição de valores socialmente vividos, o direito é dever ser, mínimo ético, ou uma espécie de moral objetiva, portanto, deve se adequar a realidade vivida, qual seja a Era Digital e "a sociedade de risco". Na Era digital os incidentes de segurança ocorrem constantemente e num curto período de tempo, o que demonstra a relativização destes dois conceitos (tempo e espaço), visto que o espaço passa a ser imaginário intangível, virtual, e o tempo passa a correr de forma mais vertiginosa que os ponteiros do relógio, características estas que emergem da "sociedade de risco".

Segundo Dias (2001), a sociedade industrial foi substituída "por uma sociedade exasperadamente tecnológica, massificada e global, onde a ação humana, em grande parte anônima, revela-se suscetível de produzir riscos também globais ou, tendendo a isso, suscetíveis de serem produzidos em tempo e lugar completamente distintos de onde provém a ação que os originou. Neste contexto, os perigos na "sociedade de risco" mostram-se abstratos e incalculáveis, sendo primordial que o direito penal e a instituições jurídicas se adequem a esta realidade, pois, na maioria das ocasiões será impossível socorre-se de imediato da proteção estatal, ademais o estilo de processo judicial não é compatível com a celeridade exigida para a resolução de cibercrimes.

No entanto, como nem sempre o Estado estará presente para exercer a sua função pacificadora, foi resguardado pela lei ao cidadão o direito à legítima defesa. Contudo, tal permissão não é ilimitada, pois que encontra suas regras na própria lei penal.

Assim, para que se possa falar em legítima defesa digital, que não pode jamais ser confundida com vingança/justiça privada é preciso que o agente se veja diante de uma situação de total impossibilidade de recorrer ao Estado, responsável constitucionalmente pela nossa segurança pública, e, só assim, uma vez presentes os requisitos legais de ordem objetiva e subjetiva, agir em sua defesa ou na defesa de terceiros.(GRECCO,2016, p. 340)

Sendo assim, a legítima defesa digital surge como uma importante aliada, juntamente com o arsenal legislativo pátrio e internacional, para auxiliar as delegacias, principalmente as especializadas em crimes informáticos, e os tribunais, na resolução destes delitos, podendo neutralizar ou dirimir os incidentes de segurança, além possibilitar a colheita de provas no sentido de punir os cibercriminosos.

4.2.4 Defesa do direito próprio ou de terceiro: a importância social da resposta em uma sociedade de risco

A preocupação maior da sociedade, não só no Brasil, mas como também em todo o mundo é a de combater os crescentes níveis de criminalidade por meios virtuais, pois, no campo dos meios de comunicação de massa, esses malefícios se refletem de diversas formas. Assim, a resposta as contingências virtuais devem se mostrar eficientes para garantir a proteção dos ativos intangíveis na esfera eletrônica, o que se consubstancia em boas práticas de governança corporativa e *compliance* a serem seguidas por todos os s*takeholders,* a fim de propiciar maior eficiência na gestão de riscos.

Com efeito, a boa gestão de riscos está no cerne das empresas de sucesso e a informação tem papel impactante na tomada de decisões. Se riscos são inevitáveis e inerentes a própria atividade empresarial, faz-se necessidade iminente converter as ameaças em oportunidades.

Conforme preleciona Damodaran (2009), à medida que as interconexões entre as economias e os setores produtivos se tornavam cada vez mais complexas com o auxílio do fenômeno da automação e da digitalização de processos/procedimentos, as empresas foram se tornando mais expostas ao risco, e a necessidade de gerenciar este risco aumentou concomitantemente. Ainda que esta crescente exposição à mudança tenha colocado as empresas

em situação de vulnerabilidade constante, ela também abriu novas fronteiras que podem ser exploradas com vistas à capitalização de lucros.

Por tal razão, Cruz (2006) afirma que em relação ao uso abusivo da informática, a salvaguarda de informações corporativas é de fundamental importância devido ao alto valor que está agregado as mesmas. O roubo e o sequestro de informações, ou simplesmente, o acesso não autorizado a dados informatizados representam condutas que podem trazer graves consequências às relações sociais, pois, em geral, serve de meio para a realização de outras atividades ilícitas de maior gravidade.

Em virtude da crescente monetização da informação e dos riscos que se ampliam com a sua operacionalização na era digital como, por exemplo, as falha nos controles internos e os crimes digitais (ataques de *hackers*, vazamentos de informações confidenciais, concorrência desleal, desvios de conduta; infrações aos Direitos Humanos, corrupção, fraudes e etc), se faz necessário estabelecer novos parâmetros frente a problemática da segurança da informação e do seu papel na governança corporativa.

Se considerarmos as estatísticas sobre os mais importantes tipos de risco operacional, veremos que estes evidenciam graves problemas ensejando a definição de padrões de controles internos e de governança corporativa. Nesse sentido, a contribuição da gestão de risco operacional para o desenvolvimento dos mecanismos de governança internamente às empresas, com a adoção das práticas de gestão de risco, e externamente com a atuação dos órgãos reguladores, contribui para o desenvolvimento de uma responsabilidade social corporativa, por meio do incentivo ao comportamento ético e socialmente responsável, evitando condutas e atitudes indesejadas ou inadequadas.

Coimbra (2007) ressalta que vivemos uma época em que os escândalos e fraudes corporativos diminuíram a confiança da sociedade nas empresas. De sorte que, a disciplina de gestão de riscos operacionais pode contribuir para o crescimento da própria atividade empresarial, principalmente, no que tange o enfrentamento da corrupção em ambientes corporativos, resultando em última análise numa melhoria da sociedade como um todo. Embora em princípio estas estratégias dependam de um grande investimento inicial, de sorte que pequenas e médias empresas restam prejudicadas por estas adequações regulatórias, o retorno destes investimentos pode ser sentido com a maximização dos lucros e o aumento da confiança de investidores e consumidores nestas empresas.

Nesse sentido, a expressão “legítima defesa” cobra interpretação extensiva, não estando restrita à integridade física do ofendido ou ao seu patrimônio tangível, abrangendo, também, a honra, no caso do emprego de calúnias, injurias ou difamações em ambientes

virtuais, ou ainda, os bens intangíveis, como a informação confidencial ou segredo industrial, no que concerne o tráfico de dados; uma vez que o alcance global da internet amplia a capacidade delitiva, e que a abrangência de um crime pode extrapolar seus efeitos na esfera privada e atingir uma quantidade incalculável de indivíduos diante da sua fácil propagação, até porque muitas vezes as próprias vítimas propagam as iniciativas criminosas.

Os marcos tecnológicos sempre deixam uma nova impressão no contexto social, por promoverem uma alteração no plano histórico, industrial e mercadológico. O Direito Penal não pode ignorar essas sensíveis mutações sociais, sob pena de tornar-se obsoleto perdendo sua função precípua de tutela aos bens jurídicos penais mais relevantes. Para tal, os conceitos penais devem passar por uma atualização para se adequarem a sociedade de risco.

Nessa esteira de entendimento, Atheniense (2006) aduz que curiosamente agimos com naturalidade quando um indivíduo reage a um assalto, em legítima defesa, mas nos causa estranheza quando alguns executivos de bancos, apoiados em pareceres jurídicos, começam a reagir e a contra-atacar os criminosos digitais, *crackers* e/ou *hackers,* antes mesmo de terem em mãos uma autorização judicial.

Nesta perspectiva cumpre observar que a legítima defesa digital já vem sendo utilizada como política de segurança em grandes empresas transnacionais, e principalmente em bancos. Logo, alguns executivos apoiados em pareceres jurídicos, começam a reagir e a contra-atacar os hackers antes mesmo de terem em mãos uma autorização judicial.

No entanto, a Federação Brasileira dos Bancos (Febran), não admite que esta seja uma prática corriqueira nas agências bancárias, afirmando que nenhum banco usa do contra-ataque aos hackers como forma de proteção. Mas entre os especialistas sobre o tema é corrente a aceitação e a utilização camuflada da defesa digital, salientando que muitas vezes o alvo principal não são os bancos, mas sim os seus clientes quando o ataque é feito por e-mails com links ou anexos que chegam as caixas postais com algum código malicioso. Também é comum o roubo de senhas através de *keyloggers*, quando o usuário realiza alguma operação no *internet banking* em um computador que tenha este artifício malicioso.

O fato é que estes incidentes de segurança não ocorrem apenas em bancos, mas também em empresas e corporações. Qualquer usuário de computador seja de intranet ou internet, está suscetível de ser vítima de um ataque informático. No entanto, na esfera empresarial não é tão simples revelar publicamente que seus sistemas são vulneráveis a um ataque, porque, tal afirmação implicaria em perca de clientela, ou seja, inibiram os "consumidores virtuais" ou usuários destas lojas, bancos, livrarias e redes sociais.

Todo esse contexto contribui para gerar um ambiente de instabilidade sobre o uso da legítima defesa na internet. Cria-se uma situação polêmica, na qual, a legítima defesa digital é tratada como um tabu entre os empresários das mais variadas áreas econômicas, como entre os próprios advogados e juristas, mas é apoiada até mesmo por policiais que acreditam que este pode ser um bom dispositivo não só para evitar que crimes digitais se concretizem e se perpetuem na internet, bem como, para evitar que os criminosos virtuais e o seu rastro desapareçam.

As empresas, corporações e bancos estão contratando grupos de gerenciamento de risco para inibirem os ataques em seus sistemas informáticos. Neste caso, o direito/bem protegido por este grupo pertence a terceiro, ora contratantes dos seus serviços. É preciso utilizar deste artifício porque não há tempo para esperar uma autorização judicial, que leva em média 48 (quarenta e oito) horas, para interceptar os criminosos digitais e se possível recapturar os dados.

Conforme assevera Pinheiro (2016), visando aumentar a segurança da informação, muitas empresas no Brasil já possuem profissionais especializados em combater delitos virtuais, especialmente os cometidos por *hackers*. Em muitos casos, é formado um time de resposta a incidentes, ou há um grupo de monitoramento e gerenciamento de riscos para tomar uma série de medidas protetivas denominadas de *Ethical Hacking*[30].

Apesar do receio que paira sobre uso da legítima defesa, principalmente, no ambiente digital, consideramos que o direito de defesa do cidadão não pode se tornar obsoleto em meio a tantas mudanças comportamentais, pois, de fato, "a autotutela já é permitida em algumas ocasiões., embora, seja meio ordinário para a satisfação de pretensões em benefício do mais forte ou astuto, para certos casos excepcionalmente a própria leia abre exceções à proibição". (CINTRA, GRINOVER e DINAMARCO, 2008, p.35) .

Com efeito, via de regra, a autodefesa é vedada no nosso ordenamento jurídico pátrio com a finalidade de evitar o exercício arbitrário das próprias razões. Tal atitude de defesa, quando não prevista legalmente, consubstancia-se num crime contra a administração da justiça, como assim dispõe os artigos 345 e 346 do Código Penal. Assim, devemos estar atentos aos treinamentos e certificações que são dados aos profissionais que irão atuar no âmbito de segurança digital para que estes não cometam ilícitos em vez de evitá-los.

[30] Atividade com fundamento ético desempenhada por programadores ou profissionais da ciência da computação e de sistemas de informação.

4.3 Excesso de legítima defesa digital

No contexto da sociedade digital, a Legítima Defesa Digital se apresenta como alternativa viável para proteger, a priori, as empresas e seus ativos intangíveis contra ataques internos ou externos, que tenham como objeto material o sistema informático e como bem jurídico a segurança da informação, de tal forma que a própria tecnologia poderá ser empregada como meio e o alvo do ataque.

Como esta atividade defensiva demanda determinados conhecimentos técnicos, incialmente, a sua utilização poderá ser mais perceptível nos ambientes corporativos, no qual se exige um maior aparato protetivo na defesa da propriedade, que agora assume contornos invisíveis ou intangíveis.

Com efeito, a realidade em que o país enfrenta de altos índices de analfabetismo não é o único fator que impede a disseminação segura da ideia de legítima defesa digital, pois, constata-se que existem muitas pessoas intelectualizadas e competentes que ainda caem em ciladas virtuais. Portanto, é inegável a necessidade de conhecimento especializado para a resolução destes conflitos, para que o agente não incorra em excesso de legítima defesa, podendo ser punido por tal excesso.

No futuro, será possível encontrar usuários comuns agindo sob a guarida da legítima defesa digital com o propósito de defender seus direitos ou bens do ataque de Cibercriminosos, porém, nos limitamos a apoiar a utilização do instituto apenas por profissionais especializados, devido a evidente caracterização do *animus defendi* nestes últimos, tendo em vista todo o aparato técnico e intelectual que eles carregam.

Não obstante, é mister observar que no que tange a legítima defesa “toda conduta praticada em excesso é ilícita, devendo o agente responder pelos resultados dela advindos” (GRECO; 2016, p. 360). Sendo assim, os resultados que dizem respeito as condutas praticadas nos limites permitidos pela legítima defesa são amparados por esta causa de justificação, porém, os outros resultados que surgirem em virtude do excesso, por serem ilícitos, serão atribuídos ao agente, devendo o mesmo em virtude destes ser responsabilizado.

Logo, quando há um incidente informático, a legítima defesa digital deve ser realizada pelos Grupos de Resposta a Incidentes de modo que esteja direcionada à atender aos seguintes objetivos: 1) bloquear ou minimizar o ataque ou a vulnerabilidade; 2) descobrir quem é o causador, ou seja, a identidade do infrator; 3) coletar provas que possam ser utilizadas para responsabilização do mesmo; e 4) tomar medidas para normalizar a situação para que ela volte a ser como era no momento anterior ao incidente.

Deste modo, embora o artigo 23, inciso II do Código Penal, preconize que não há crime quando o agente pratica o fato em legítima defesa, essa atividade defensiva deve estar respaldada em boas práticas de direito digital e computação forense para que as provas coletadas não sejam rejeitadas por serem consideradas como provas obtidas por meio ilícito (artigo 213 do Código Civil, artigo 332 do Código de Processo Civil e artigo 386 e outros do Código Processo Penal) e para que a empresa não seja responsabilizada civilmente e o profissional seja responsabilizado criminalmente devido aos excessos.

No entanto, segundo Blum (2006), a legítima defesa digital pode ser uma atividade de alto risco para as empresas e profissionais que dela fazem uso, pois, estariam praticando um crime posterior para coibir um outro crime anterior com base na excludente, passando a vítima à condição de criminoso. Ademais, existe ainda o grave risco do excesso de conduta na reação de legítima defesa, excesso esse punível, o que geraria ainda maiores riscos para os envolvidos.

No âmbito do Congresso Nacional, esta discussão já gerou grande polêmica no Brasil, pois o projeto de Lei nº 84/1999 do senador Eduardo Azeredo (PSDB-MG) sobre o controle da internet, tencionava obrigar provedores a informar eventuais crimes e criar o conceito de defesa digital, no qual permitiria que técnicos e profissionais de informática invadissem comunicações de terceiros, em caso de suspeita de ataques de hackers, para prevenir ou barrar ataques a seus sistemas. No entanto, o projeto de lei brasileiro foi nesta parte rejeitado e comparado aos projetos de lei norte-americanos Stop Online Piracy Act – SOPA (Ato para Acabar com a Pirataria Online) e Protect IP Act–PIPA (Ato para a Proteção da Propriedade Intelectual) e, o projeto de lei europeu Anti-Counterfeiting Trade Agreement – ACTA (Acordo Comercial Anticontrafacção), pois ambos permitiam rastrear conexões e implantar filtros de navegação para inibir a criminalidade digital.

Para Azevedo (2007), a legítima defesa digital, segundo a qual um profissional de informática contratado por empresa poderia realizar a interceptação de dados, caso a companhia se sinta lesada de alguma maneira pela internet (por exemplo: caso um *spammer* utilizasse o logo da corporação para propagar um golpe virtual), seria uma prática inconstitucional, pois possibilitaria a interceptação de dados sem autorização judicial.

Crespo (2011), pelo contrário, aduz que em verdade, não é possível vislumbrar tantos impedimentos a repulsa à agressão injusta perpetrada em ambiente digital se utilizarmos dos meios necessários e agirmos de forma moderada, até mesmo porque o instituto das excludentes de ilicitude servem justamente para que não sejam consideradas antijurídicas condutas que, normalmente, seriam amoldadas as normas penais incriminadoras.

Seguindo a mesma linha argumentativa, Greco (2018) explica que a legítima defesa é um direito que permite criar uma barreira contra o arbítrio de um outro indivíduo, pois, conforme expõem, um direito subjetivo que não opera como um bloqueador ao arbítrio de um outro, não é um direito subjetivo, esvaziando-se no mundo jurídico, portanto, se existem direitos subjetivos, tem de existir também o direito de defendê-los. Esse direito é a legítima defesa.

Vimos no capítulo anterior, que a responsabilização penal das Pessoas Jurídicas passa a ser ampliada diante das exigências legislativas e regulamentares que incidem sobre o sistema econômico e financeiro atual. As empresas que atuam no setor econômico-financeiro possuem caráter nitidamente internacional, porém, com o advento da internet, o simples fato de uma empresa física possuir uma representação *on line* e disponibilizar seus produtos e serviços em sítios eletrônicos, implica na internacionalização desta atividade comercial, posto que, em tese, se coloca à disposição de potenciais consumidores conectados em uma rede mundial, podendo ser acessada por consumidores de qualquer lugar do mundo.

As exigências legais pela implementação de programas de integridade em ambientes corporativos denota a necessidade de conformidade (*compliance*) da sua atuação na cadeia produtiva e de consumo. Para adequar-se a esta realidade, as empresas precisam entender como funcionam as regras jurídicas que vigoram nos mercados que os seus serviços e produtos alcançam ou que pretendem alcançar.

Uma destas exigências é a proteção de dados e segurança informática. Visando treinar profissionais e estabelecendo diretrizes gerais para aumentar a capacidade de detecção de incidentes e a correlação de eventos de risco, várias empresas transnacionais vem preparando seus funcionários por meios de treinamentos, regimentos internos e códigos de conduta. No entanto, além da atividade preventiva, estas empresas também atuam protetivamente através de Grupos de Resposta a Incidentes e *Compliance*.

É cediço que os crimes digitais podem provocar consequências nefastas em ambientes corporativos e na dinâmica econômica de um ou de vários países, por meio da queda de competitividade mercadológica e do aumento dos níveis de desemprego, da evasão de divisas resultantes da violação de segredos industriais e tecnológicos, acarretando na perda de patentes e perdas de recursos financeiros em pesquisas, do desequilíbrio da balança comercial, em especial, na exportação e importação de produtos, o que trará consequências diretas no Produto Interno Bruto (PIB) e na taxa de crescimento do país, além da perda da credibilidade reputacional e da consequente redução dos lucros e investimentos externos, e de outras consequências que poderão ser visualizadas caso a caso, por isso é tão importante investir em segurança da informação, *compliance* e grupos de gerenciamento de riscos.

Assi (2013) afirma, que no Brasil, a função do *compliance oficcer* surgiu com as instituições financeiras, por meio de legislações específicas, que passaram a instituir ações (deveres) que foram reconhecidas como boas práticas, sendo, consequentemente, incorporadas a instituições não financeiras. Originalmente, a função de *compliance* foi direcionada para o setor jurídico, pois, acreditava-se que esta atividade seria composta apenas por normas e regulamentos. Com o passar do tempo, verificou-se que a atuação restrita ao jurídico, minimizava os impactos dos processos de integridade, passando a promover a implementação da gestão de *compliance* através de profissionais específicos, capacitados para atuarem nessa área da governança corporativa.

O ser humano é naturalmente falível em suas ações podendo correr em erro sobre os limites de uma causa de justificação, e nesse caso, como em qualquer modalidade de erro, deve-se aferir se era evitável ou não. Se inevitável, o agente, embora atuando em excesso, será considerado isento de cumprir a pena; se evitável o erro, embora o fato por ele praticado seja típico, ilícito e culpável, produzirá o efeito de redução da pena entre os limites de um sexto a um terço, nos termos da parte final do art.21 do Código Penal.

Nesse diapasão, devemos preparar os profissionais que atuaram nessa área. O Centro de estudos, resposta e tratamento de incidentes de segurança no Brasil – CERT/BR, órgão mantido pelo Núcleo de Informação e Coordenação do Ponto BR – NIC.br. e do Comitê Gestor da Internet no Brasil, desenvolve esse papel, incentivando e mantendo projetos de análise sobre tendências de ataques, com o objetivo de melhor entender suas características no espaço da Internet Brasileira, visto que o CERT/BR tem a responsabilidade de atender a qualquer rede brasileira conectada à Internet.

O CERT/BR tem como objetivo fundamental impedir a caracterização de excessos na atividade de gerenciamento de risco. Por ser um grupo de resposta a incidentes de segurança para a internet brasileira, o CERT/BR tem um software que dá suporte a atividade deste grupos de gerenciamento de riscos no Brasil, disponibilizando no seu site, publicações, cursos, palestras, projetos, links e estatísticas sobre o quadro de gerenciamento de segurança a nível brasileiro de internet.

Sendo assim, devemos nos guiar pela legislação nas atividades de gerenciamento de riscos, pois, a resposta ao incidente dada pelo agente, embora inicialmente legítima, poderá transforma-se em uma agressão injusta, ou seja, em um incidente de segurança para o agressor inicial, podendo ensejar a caracterização de um ato de legítima defesa sucessiva no que diz respeito a este, pois, quem viu repelida a agressão que inicialmente era injusta, pode alegar a excludente a seu favor, considerando que a vítima, neste caso, passa a ser o agressor. Portanto,

devemos ter cautela ao utilizarmos a excludente de legítima defesa digital, visto que os limites entre a defesa e o ataque são bastante tênues.

5 CONCLUSÃO

Neste trabalho, a legítima defesa digital foi concebida com o propósito de incentivar a criação de políticas de segurança da informação, tendo em vista a regulação informática e a atuação de grupos de resposta a incidentes em instituições públicas e privadas, como por exemplo, bancos, empresas e a própria Administração Pública consubstanciada nos seus órgãos, de modo que, todos os colaboradores devem atuar em *compliance* (conformidade) com os procedimentos de segurança, recebendo treinamento para tanto.

Através de uma interpretação extensiva, é possível recorrer aos preceitos penais tradicionais para resolver questões acerca da adequação das condutas ilícitas que representam a criminalidade informática. Entretanto, para tal interpretação, não se podem utilizar operações axiológicas ou valorativas. Se assim o fosse, estaríamos diante de uma interpretação analógica proibida em Direito Penal, visto que se aplicaria a uma hipótese não regulada por lei, a legislação de um caso semelhante para criar um tipo penal. No entanto, deve-se observar que não existe analogia de norma penal incriminadora – in malam partem, restando, apenas, o recurso analógico para beneficiar o acusado – in bonam partem.

Nos casos de crimes informáticos é elementar a necessidade de criação de legislação específica para evitar estes questionamentos que só servem para entravar a resolução dos delitos. Entretanto, quando nos referimos a hipótese de defesa cibernética, esculpimos por analogia a legítima defesa digital, baseando-se na legítima defesa em *stricto sensu*, sendo a primeira realizada em meio digital como resposta mais viável as exigências regulamentares e mercadológicas para proteção da privacidade e manutenção da segurança em ambientes digitais.

Este trabalho acadêmico tenciona demonstrar que a legítima defesa digital já é uma realidade. No entanto, o instituto necessita ser melhor regulamentado para não gerar arbitrariedades e consequentemente dar ensejo ao caos jurídico-virtual, devendo ser utilizada como estratégia competitiva de GRC (Governança, Risco e *Compliance*) para garantir a preservação dos contratos e a continuidade dos negócios.

Com o desenvolvimento da tecnologia e estabelecimento de novos meios de comunicação, a economia global rompeu barreiras territoriais possibilitando a realização de transações comerciais de forma quase que ilimitada. Esse panorama denota o surgimento de novas condutas, as quais são reputadas dignas de tutela penal pelo legislador, sendo alçadas, assim, à categoria de bens jurídicos penais.

É bem verdade que a prática forense e a legislação sobre assuntos digitais ainda precisam avançar, pois, diante da ordem jurídica capitalista e de um ambiente tecnológico

globalizado, a regulamentação a nível corporativo e empresarial da defesa digital é inevitável e indispensável, de tal forma, que muitas empresas já desenvolvem mecanismos de auto-regulamentação diante da ausência de regulamentação estatal, enquanto pressionam os governos e autoridades internacionais a criarem legislações mais uniformes e globais sobre proteção de dados e outros assuntos que envolvam tecnologias digitais.

Para compreender a amplitude dessa nova realidade, surge a criação de contratos simplificados e mais intuitivos com cláusulas dispostas diretamente na tela do computador e visível nos sites para navegação (termos de uso) como alternativa para educar e conscientizar os usuários. Outra proposta bastante oportuna, para solucionar tais problemas, principalmente no que concerne as relações consumeiristas seria a publicação de "normas digitais", no formato de vídeo, aúdio ou *disclaimer*, uma vez que o Direito Digital traz a obrigação de atualização tecnológica para as empresas e demais atores e colaboradores do setor, de modo a propriciar que o consumidores e demais players entendam e assumam suas responsabilidades nos negócios e demais relações jurídicas realizadas na internet.

Outro aspecto relevante, é a contribuição da gestão de risco operacional na criação de valor para os *stakeholders*, evitando ou diminuindo perdas, tornando processos mais eficientes, permitindo respostas rápidas e adequadas a contingências provocadas pelos crimes digitais, reduzindo ou eliminando riscos, melhorando o desempenho do negócio como um todo e alinhando a relação risco-retorno à estratégia da organização, de sorte que nos contratos internacionais estes incidentes de segurança podem ser abrangidos pela cláusula de força maior e pela cláusula *hardship* garantindo o equilíbrio econômico-financeiro do contrato e a estabilidade do negócio.

Dessarte, a legítima defesa digital representa um indício de vantagem competitiva no mercado globalizado, à medida que é utilizada como mecanismo para gestão de riscos. Por conseguinte, é de tal forma abrangente que, além de evitar a reparação indenizatória, evita ainda a responsabilização penal, tendo em vista que a prerrogativa da autodefesa é uma causa de justificação que vem manifestada no art.23, I c/c art.25 do CP.

Este tipo permissivo indica todos os elementos caracterizadores do instituto, divergindo da legítima defesa tradicional apenas quanto ao meio em que será empregada, qual seja o meio digital, sendo definida nos seguintes termos: Art. 25: "Entende-se em legítima defesa quem, usando moderadamente dos meios necessários, repele injusta agressão, atual e iminente, a direito seu ou de outrem". (BRASIL. Código Penal – Decreto Lei 2848 de 07.12.1940.).

O Direito Penal tem como escopo fundamental a proteção aos bens jurídicos considerados relevantes pela sociedade. Sendo assim, em nome da segurança jurídica e do bem estar social faz-se necessário a tipificação legal destas condutas nocivas, impondo-se as suas respectivas sanções. Em alguns crimes o bem jurídico é o patrimônio, em outros é a integridade física das pessoas ou a honra destas, enquanto que no crime informático a tutela jurídica recai sobre o sistema informático, ou seja, o bem jurídico é a informação informatizada.

Assim, neste caso se faz necessária a intervenção do Direito Penal na Informática, partindo do pressuposto de que existe o crime informático. Percebe-se que o desenvolvimento das tecnologias possibilitou não somente a prática de novos crimes, como potencializou alguns outros tradicionais, no entanto, aqui, o enfoque se resume aos primeiros, quais sejam os crimes informáticos, pois, a proteção à informação informatizada traz consigo inúmeros desafios e questionamentos para os estudiosos do direito.

A "privatização" da investigação criminal e a política da *Criminal Compliance* tem um objetivo claro, qual seja, mitigar a prática de crimes através de vários mecanismos de controle interno e prevenir a responsabilização criminal. Todavia, ao invés de mitigar as chances de responsabilização, a *Criminal Compliance* criou condições para a caracterização de condutas delitivas dentro das empresas e instituições financeiras e a possibilidade de individualização dos responsáveis, de forma que agora existe e exige-se que haja uma cadeia de responsabilização penal dentro das empresas.

Assim, o chefes dos setores de *Criminal Compliance*,ou seja, os *Compliance Officers*, funcionam como verdadeiros garantistas da ordem e integridade empresarial, pois respondem objetivamente como se tivessem agido de forma positiva no caso de situações em que venham a se omitir. De sorte que, todo o corpo da empresa é colocado na mira da persecução criminal pois na verdade a *Criminal Compliance* e a responsabilidade de denunciar, abrange todos os dirigentes, funcionários ou supervisores integrantes da empresa ou instituição financeira.

Esse ponto é interessante, pois gera um sistema sólido de fiscalização, onde há uma regra básica da fiscalização conjunta, não importando de quem ela venha. Assim, cada integrante da empresa ou instituição financeira pode ser o denunciante ou o denunciado, independente da posição eu ocupa na empresa, sendo essa posição estratégica ou não, a fim de mitigar riscos dentro da empresa e garantir o progresso social.

Portanto, o presente trabalho não pretende esgotar a investigação sobre o instituto da legítima defesa digital, tendo em vista que a própria legítima defesa no seu aspecto tradicional revela-se como um fenômeno passível de controvérsias, apesar dos vários estudos sobre o tema, mas propõe um ampliação da interpretação da legítima defesa *stricto sensu* no sentido de

adapta-la as fenômenos digitais, propondo uma atividade proativa das empresas e uma reflexão jurídica, não só para advogados e juízes, como, também, para todos os demais participantes do processo.

REFERÊNCIAS

ASSI, Marcos. **Gestão de *compliance* e seus desafios:** como implementar controles internos, superar dificuldades e manter a eficiência dos negócios. 1. ed. São Paulo: Saint Paul Editora, 2013.

ASSI, Marcos. **Controles internos e cultura organizacional:** como consolidar a confiança na gestão de negócios. 2. ed. São Paulo: Saint Paul Editora, 2014.

ATHENIENSE, Alexandre. **Os bancos partem para a legítima defesa diante dos ataques hackers.** O direito e novas tecnologias. Disponível em: http://www.dnt.adv.br/noticias/direito-penal-informatico/os-bancos-partem-para-a-legitima-defesa-diante-dos-ataques-hackers. Acesso em: 05 mar. 2018.

AZEVEDO, Reinaldo. **Internet**: o inferno das boas intenções de Eduardo Azeredo. Revista Veja. Blog Reinaldo Azevedo. Disponível em: https://veja.abril.com.br/ blog/reinaldo/internet-o-inferno-das-boas-intencoes-de-eduardo-azeredo/. Acesso em: 04 jul. 2018

BARBOSA, Luiza Nogueira. **O processo civil brasileiro como veículo de concretização e juridicização de normas globais ("Global Law")**. 2017. Dissertação (Mestrado em Direito Processual), – Centro de Ciência Jurídicas e Econômicas, Universidade Federal do Espírito Santo, Vitória, 2017. Disponível em: http://portais4.ufes.br/posgrad/teses/tese_11341 _LUIZA20170829-114120.pdf . Acesso em: 23 ago. 2018.

BELL, Daniel. **O advento da sociedade pós-industrial:** uma tentativa de previsão social. Tradução Heloysa de Lima Dantas. São Paulo: Editora Cultrix, 1973.

BENEDETTI, Carla Rahal. **Criminal compliance:** instrumento de prevenção criminal corporativa e transferência de responsabilidade penal. São Paulo: Quartier Latin, 2014.

BLUM, Renato Opice. **Crimes virtuais:** O Risco da "Legítima Defesa". Disponível em: http://www.telesintese.com.br/crimes-virtuais-os-riscos-da-qlegitima-defesaq/. Acesso em: 17 mar. 2018.

BRANDÃO, Lucas. **A sociedade da informação em rede aos olhos de Manuel Castells.** Disponível em: https://www.comunidadeculturaearte.com/a-sociedade-da-informacao-em-rede-aos-olhos-de-manuel-castells/. Acesso em: 10 abr. 2018.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. *In*: VADE mecum saraiva compacto. 21. ed. São Paulo: Saraiva Educação, 2019.

BRASIL. Código Penal. Decreto Lei nº 2.848 de 7 de dezembro de 1940. *In*: VADE mecum saraiva compacto. 21. ed. São Paulo: Saraiva Educação, 2019.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Lei da interceptação telefônica. *In:* VADE mecum saraiva compacto. 21. ed. São Paulo: Saraiva Educação, 2019.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Lei Carolina Dieckmann. Disponível em: http://www.planalto.gov.br/ ccivil_03/_ato2011-2014/2012/lei/l12737. Acesso em: 14 jun. 2018.

BRASIL. Decreto nº 8.135, de 4 de novembro de 2013. Comunicação de dados da administração pública. *In:* VADE mecum saraiva compacto. 21. ed. São Paulo: Saraiva Educação, 2019.

BRASIL. Lei Complementar nº 149, de 12 de janeiro de 2015. Dispõe sobre forças estrangeiras no território nacional. Disponível em: http://www.planalto.gov.br/ccivil_03 /leis/lcp/Lcp149.htm. Acesso em: 25 jul. 2018.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco civil da internet. *In:* VADE mecum saraiva compacto. 21. ed. São Paulo: Saraiva Educação, 2019.

CALDEIRA, João Paulo. **A discussão sobre o sistema de defesa cibernética do Brasil.** O Jornal de todos Brasis. Disponível em: https://jornalggn.com.br/noticia/a-discussao-sobre-o-sistema-de-defesa-cibernetica-do-brasil. Acesso em: 22 fev. 2018.

CANABARRO, Diego R. **A contribuição do Brasil para o Marco Civil da Internet na Itália.** Disponível em: http://observatoriodainternet.br/post/a-contribuicao-do-brasil-para-o-marco-civil-da-internet-na-italia. Acesso em: 10 abr. 2018.

CANATACCI, Joseph. **Urgent action needed to protect privacy in cyberspace**, UN rights expert warns. Disponível em: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22762&LangID=E. Acesso em: 02 dez. 2018.

CHAOUQUI, Francesca Immacolata. **Nel nome di Pietro:** Riccheze,Affari, Intrighi e Scandali. Dalle Carte Segrete Della Comissione Del Papa. Segrati: Sperling & Kupfer, 2017.

CINTRA, Antonio Carlos de Araujo; GRINOVER, Ada Pellegrini; DINAMARCO, Cândido Rangel. **Teoria geral do processo.** 24. ed. São Paulo: Malheiros, 2008.

COIMBRA, Fábio. **Riscos operacionais:** estrutura para gestão em bancos. São Paulo: Saint Paul Editora, 2007.

COMITÊ GESTOR DA INTERNET NO BRASIL (São Paulo)**. Resolução CGI.br/RES/2009/003**. Princípios para governança e uso da internet no Brasil. Disponível em: https://www.cgi.br/resolucoes/documento/2009/003. Acesso em: 21 jun. 2018.

CONSELHO DA UNIAO EUROPEIA (Bruxelas). **Decisão 2005/222/JAI de 24 de fevereiro de 2005.** Dispõe sobre ataques contra sistemas de informação na União Europeia. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32005F0222. Acesso em: 26 jul. 2018.

COSTA, Cynara de Barros. **Direito transnacional do comércio:** uma teoria afirmativa da natureza jurídica das normas do Comércio transnacional. 2016. Tese (Doutorado em Direito Internacional) – Faculdade de Direito do Recife, Universidade Federal de Pernambuco, Recife, 2016. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/18084/1/TESE%20-%20DEP%C3%93SITOFINALBIBLIOTECACENTRAL.pdf. Acesso em: 16 mar. 2018.

COSTA, Cynara de Barros. **A verdadeira lex mercatória:** o direito além do estado. Um estudo sobre as antigas e novas teorias da lex mercatoria. 2011. Dissertação (Mestrado em Direito Internacional) – Faculdade de Direito do Recife, Universidade Federal de Pernambuco, Recife, 2011. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/4772/1/arquivo6701_1.pdf. Acesso em: 16 mar. 2018.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais.** São Paulo: Saraiva, 2011.

CRUZ, Danielle da Rocha. **Criminalidade informática:** a tipificação penal das condutas ilícitas realizadas com cartões de crédito. Rio de Janeiro: Forense, 2006.

DIAS, Jorge de Figueiredo. **O direito penal entre a "sociedade industrial" e a "sociedade de risco"**. Revista brasileira de ciências criminais, São Paulo, v.9, n. 33. jan/mar. 2001.

DISTRITO FEDERAL. Lei n 6.112 de 02 de fevereiro de 2018. Lei de Compliance do Distrito Federal. Sistema Integrado de Normas Jurídicas do Distrito Federal – SINJ/DF. Disponível em: https://www.sinj.df.gov.br. Acesso em: 17 out. 2018.

DOPICO GÓMEZ-ALLER, J. **Responsabilidad de personas jurídicas.** Madrid: Editora Francis Lefebvre, 2010.

DAMODARAN, Aswath. **Gestão estratégica do risco:** uma referência para a tomada de riscos empresariais. tradução Félix Nonnenmacher. Porto Alegre: Bookman, 2009.

DOMENEGHETTI, Daniel; MEIR, Roberto. **Ativos intangíveis:** o real valor das empresas. Rio de Janeiro: Editora Elsevier, 2009.

FIORILLO, Celso Antônio Pacheco. **Princípios constitucionais do direito da sociedade da informação:** a tutela jurídica do meio ambiente digital. São Paulo: Saraiva; 2015.

GRECO, Luís. **Professor Luís Greco apresenta reflexões sobre legítima defesa no congresso internacional realizado pelo Ministério Público.** Disponível em: http://www.mpgo.mp.br/portal/noticia/professor-luis-greco-apresenta-reflexoes-sobre-legitima-defesa-no-congresso-internacional-realizado-pelo-mp#.XEPeziOr-Y. Acesso em: 26 nov. 2018.

GRECO, Rogério. **Curso de direito penal (parte geral):** artigos 1 a 120 do Código Penal. 18. ed. Niterói: Impetus, 2016.

HABERMAS, Jürgen. **A constelação pós-nacional:** ensaios políticos. Tradução Márcio Seligmann-Silva. São Paulo: Littera Mundi, 2001

IANNI, Octavio. **A sociedade global.** 8. ed. Rio de Janeiro: Civilização Brasileira, 1999.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos.** São Paulo: Saraiva, 2016.

JUANES PECES, A. **Introducción a la responsabilidad de las personas jurídicas:** consideraciones generales y problemas substantivos y processales que dicha responsabilidade suscita. Madrid: Editora Francis Lefebvre, 2015.

LEVY, Pierre. ***Cibercultura*.** Tradução de Carlos Irineu da Costa. São Paulo: Editora 34 Ltda, 1999.

LORENZETTI, Ricardo Luis. **Comércio eletrônico.** Tradução de Fabiano Menke. São Paulo: Revista dos Tribunais, 2004.

MASUDA, Yoneji. **A sociedade da informação como sociedade pós-industrial.** Rio de Janeiro: Editora Rio, 1982.

MARS, Amanda. **Relatório sobre influência russa na eleição dos EUA é entregue após dois anos:** Documento aborda o possível conluio entre Trump e o Kremlin nas eleições presidenciais de 2016. Disponível em: https://brasil.elpais.com/brasil/2019/03/22/internacional/1553288700_091103.html. Acesso em: 04 abr. 2018.

MARTINI, Renato da Silveira. **Tecnologia e cidadania digital:** ensaio sobre tecnologia, sociedade e segurança. Rio de Janeiro: Brasport, 2008.

MIRABETE, Júlio Fabbrini. **Manual de direito penal**. 8. ed. São Paulo: Atlas, 1994.

MORAES, Maria Celina Bodin de; TEFFÉ, Chiara Spadaccini de. **Redes sociais virtuais:** privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. Pensar, Fortaleza, v. 22, n 1, p. 108-146, jan./abr. 2017.

NEWMAN, Lily Hay. **The bleak state of federal government cybersecurity**. Disponível em: https://www.wired.com/story/federal-government-cybersecurity-bleak/. Acesso em: 12 jun. 2018.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (Brasil). **Era digital precisa garantir prosperidade para todos, diz relatório da ONU.** Disponível em: https://nacoesunidas.org/era-digital-precisa-garantir-prosperidade-para-todos-diz-relatorio-da-onu/. Acesso em: 03 nov. 2018.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (Nova York). **Resolução 51/162 de 16 de dezembro de 1996.** Lei modelo da UNCITRAL sobre comércio eletrônico. Disponível em: http://www.lawinter.com/1uncitrallawinter.htm. Acesso em: 26 set. 2018.

PACHECO, Leonardo Serra de Almeida. **Marco civil da internet:** o que mudou para sua startup? *In*: Direito das Startups. Curitiba: Juruá, 2016.

PARLAMENTO EUROPEU (Estrasburgo). **Decisão 2006/24/CE de 15 de março de 2006.** Dispõe sobre a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32006L0024. Acesso em: 26 jul. 2018.

PARLAMENTO EUROPEU (Bruxelas). **Regulamento 2016/679 de 27 de abril de 2016.** Regulamento Geral sobre a Proteção de Dados (GDPR). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 26 nov. 2018.

PINEDA, Francisco Almenar. **Ciberdelincuencia:** Teoría y Práctica. Curitiba: Juruá, 2018.

PINHEIRO, Patrícia Peck. **Direito digital**. 6. ed. São Paulo: Saraiva, 2016.

PIOVESAN, Flávia. **Direitos humanos e justiça internacional:** um estudo comparativo dos sistemas regionais europeus, interamericano e africano. 5. ed. São Paulo: Saraiva, 2014.

RAMOS, André de Carvalho. **Direito internacional privado e direito transnacional:** entre a unificação e a anarquia. Revista de Direito Internacional, Brasília, v.13, n. 2, 2016, p.504-520.

REALE, Miguel. **Filosofia do direito.** 19. ed. São Paulo: Saraiva, 1999.

RODEGHERI, Letícia Bodanese. **Cosmopolitismo e proteção internacional dos direitos humanos:** perspectiva da União Europeia e da necessidade de diálogo com os cidadãos. Rev. Fac. Direito UFMG, Belo Horizonte, n. 66, pp. 457 - 497, jan./jun. 2015.

SANTAELLA, Lúcia. **Da cultura das mídias à cibercultura:** o advento do pós-humano. In: Revista Famecos: mídia, cultura e tecnologia. Faculdade de Comunicação Social, PUCRS, Porto Alegre, n. 20, 2003.

SILVA, Alexandre Assunção e. **Sigilo das comunicações na internet.** Curitiba; Juruá, 2017.

SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático**. São Paulo: Revista dos Tribunais – RT, 2003.

SIQUEIRA JR. **A nova ordem constitucional (O direito na sociedade da informação III):** a evolução do direito digital. São Paulo: Atlas, 2013.

STEAWART, Thomas A. **Capital intelectual:** a nova vantagem competitiva das empresas. Tradução de Ana Beatriz Rodrigues e Priscila Martins Celeste. Rio de Janeiro: Campus, 1998.

STEFANINI. Marco. **No mundo da internet das coisas, defesa cibernética é prioridade.** TI Inside Online Segurança. Disponível em: http://tiinside.com.br/tiinside/seguranca/artigos-seguranca/26/04/2016/no-mundo-da-internet-das-coisas-defesa-cibernetica-e-prioridade/. Acesso em: 26 abr. 2018.

TAKAHASHI, Tadao. **Sociedade da informação no Brasil:** livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000.

TEUBNER, Gunther. **Fragmentos constitucionais:** constitucionalismo social na globalização. São Paulo: Saraiva, 2016.

WESTERMAN, George; HUNTER, Richard. **O risco de TI:** convertendo ameaças aos negócios em vantagem competitiva. São Paulo: M. Books do Brasil Editora Ltda, 2008.

WIENER, Nobert. **Cibernética e sociedade:** o uso humano de seres humanos. Tradução José Paulo Paes. 3. ed. São Paulo: Cultrix, 1984.

WOLOSZYN, André Luís. **Vigilância e espionagem digital:** a legislação internacional e o contexto brasileiro. Curitiba: Juruá, 2016.