CRIMES CIBERNÉTICOS, PRIVACIDADE E CIBERSEGURANÇA

Cybercrimes, privacy and cybersecurity

Loreci Gottschalk Nolasco
Universidade Estadual de Mato Grosso do Sul, Mato Grosso do Sul – Brasil
Lattes: http://lattes.cnpq.br/8817250711332244 ORCID: https://orcid.org/0000-0002-5867-6412
E-mail: lorecign@gmail.com

Bruno Dutra Maciel Silva
Universidade Estadual de Mato Grosso do Sul. – Brasil
Lattes: http://lattes.cnpq.br/7511216231962585
E-mail: bruno16dutra@gmail.com

Trabalho enviado em 07 de junho de 2022 e aceito em 14 de outubro de 2022

RESUMO

A pesquisa tem por objetivo analisar a temática da segurança informacional no Brasil, entendida como necessária para defesa de dados particulares diante do avanço da criminalidade virtual a partir do advento da internet. Pretende-se ainda, entender os avanços sediados pelo ordenamento jurídico brasileiro, ademais dos empenhos executivos e empresariais, no sentido de promover maior segurança jurídica na alçada de dados e informações.
Utilizando o método bibliográfico, através da literatura científica e documental, observa-se que a edificação de um novo meio ambiente integralmente virtual, deu origem a chamada sociedade da informação, a qual interliga globalmente sujeitos pela cibercultura e pelo ciberespaço, sem limitações físicas, fatores responsáveis pela estruturação de circunstâncias até então não experimentadas pela humanidade e, consequentemente, pelo Direito.
A emergência de novos fatos e valores pessoais e institucionais relacionados à informação na sociedade contemporânea, tem exigido do Direito a adequação e/ou reconstrução de categorias jurídicas, a partir da equação constitucional, que é clara e aplicável a qualquer tipo de informação: o detentor da informação deve o máximo respeito à privacidade dos indivíduos e a máxima transparência dos atos que envolvam interesses públicos. Todavia, em relação à produção legislativa, é apontado um alargamento e uma desformalização dos procedimentos, quanto maior a complexidade e o risco apresentado pelas matérias a se normatizar.

Palavras-chave: Informação. Dados. Cibercriminalidade. Cibersegurança. Governança.

ABSTRACT

The research aims to analyze the issue of information security in Brazil, understood as necessary for the defense of private data in the face of the advance of virtual crime from the advent of the internet. It is also intended to understand the advances made by the Brazilian legal system, in addition to the executive and business efforts, in order to promote greater legal certainty in the scope of data and information.
Using the bibliographic method, through scientific and documentary literature, it is observed that the construction of a new fully virtual environment gave rise to the so-called information society, which globally interconnects subjects through cyberculture and cyberspace, without physical limitations, factors responsible for the structuring of circumstances hitherto unexperienced by humanity and, consequently, by the Law.
The emergence of new facts and personal and institutional values related to information in contemporary society, has demanded from the Law the adequacy and/or reconstruction of legal categories, based on the constitutional equation, which is clear and applicable to any type of information: the holder of information owes the utmost respect to the privacy of individuals and the maximum transparency of acts involving public interests. However, in relation to legislative production, an extension and deformalization of procedures is pointed out, the greater the complexity and risk presented by the matters to be standardized.

Keywords: Information. Data. Cybercrime. Cybersecurity. Governance.

INTRODUÇÃO

> (...) "há tempos se fala em um processo de digitalização dos direitos fundamentais (...), bem como de uma digitalização do próprio Direito (daí se falar também de um Direito Digital), o que, à evidência, inclui (...) o reconhecimento gradual, na esfera constitucional e no âmbito internacional, de um direito humano fundamental à proteção de dados" (SARLET, 2021).

O longo processo de evolução tecnológica experimentado pela raça humana, certamente, tem seu ápice com a revolução digital desencadeada pelo advento dos computadores e da Internet, que possibilitou a edificação de um novo meio-ambiente integralmente virtual, onde os indivíduos "on-line" compõem uma nova comunidade, originando a "Sociedade da Informação" (CASTELLS, 2003, 2013). Nesse cenário, os sujeitos encontram-se globalmente interligados pela cibercultura e pelo ciberespaço, sem limitações físicas, fatores responsáveis pela estruturação de circunstâncias até então não experimentadas pela humanidade e, consequentemente, pelo Direito.

Para Castells (2001), o que caracteriza a atual revolução tecnológica não é a centralização do conhecimento e da aplicação, senão o uso da informação para a gestão de todo o processamento da informação e gerenciamento, num processo de retroalimentação eterno, promovendo a passagem de três estágios das novas tecnologias de telecomunicações nas últimas décadas, quais sejam: a automação das tarefas, as experiências de usos e a reconfiguração das aplicações. "Nos dois primeiros estágios, os avanços tecnológicos se caracterizam pelo learn by using, isto é, pelo aprender usando. No último, são os usuários que aprenderam a tecnologia fazendo, o que acabou resultando na configuração das redes e na descoberta de novas aplicações" (CASTELLS, 2001, p. 51).

Essas conjunturas se estendem das benesses que a tecnologia proporciona ao ser humano, como melhorias na telecomunicação, facilitação de processos, economia de espaço físico e assim por diante, a experiências socialmente desagradáveis como os delitos, que, em razão da virtualização de riquezas até então físicas e do surgimento de novos bens imateriais próprios do meio digital, passam a suceder no mundo informático, colocando em xeque construções tradicionais do Direito, especialmente na seara penal.

A internet conectou o mundo, diminuindo as distâncias e ampliando o acesso à informação em uma espécie de teia. Conforme Molinaro e Sarlet (2014), a liberdade de informação é um assunto que permeia a doutrina mundial desde o século XVIII, com o The Freedom of the Press Act, da Suécia, e o Código de Organización Política y Municipal, de 1888, originário da Colômbia. Esses diversos caminhos da contemporaneidade, todavia, tornaram-se preocupantes à medida que a segurança pessoal se tornou questionável nesses canais. É preciso entender que, do mesmo jeito que

a informação chega, ela acaba saindo e, nisso, podem ser levados dados importantes do usuário.

Segundo Bittar (2019), "a era digital corresponde ao período histórico em que a vida social, as relações de trabalho e boa parte das interações humanas passam a estar determinadas por 'algoritmos' e 'operações digitais'". Para ele, "A emergência da era digital impõe novos desafios ao Direito. Diante da tecnologia avançada, da inteligência artificial e da aceleração da vida, entra-se de fato numa 'nova era', a era da revolução digital, num novo estágio de desenvolvimento do capitalismo, e, portanto, do mundo moderno".

Conforme Pinheiro (2015) "o avanço tecnológico na comunicação sempre perseguiu o objetivo de criar uma Aldeia Global, permitindo que todas as pessoas do mundo pudessem ter acesso a um fato de modo simultâneo", ou seja, através da internet, os indivíduos poderiam exercer alguns de seus direitos mais importantes como cidadãos, a liberdade de expressão, a manifestação do pensamento e o desenvolvimento de conhecimentos de forma ampla e irrestrita.

No entanto, principalmente quando o assunto envolve as redes sociais, empresas e política, o assunto é marginalizado e grande é a preocupação. Consoante a Hostert (2018), "o problema é ainda mais complexo uma vez que as pessoas não tem conhecimento da quantidade de informações que despejam na internet, e muito menos o que acontece posteriormente". Kadow & Camargo (2016, p. 155) explicam que no estilo de vida atual, pautado pelas relações digitais, "é fundamental estabelecer o mínimo de segurança e privacidade das nossas informações".

O que se sabe, é que, diante da facilidade de acesso e troca de informações via internet e o avanço abrangente de tecnologias, que deu origem ao que se pode chamar de aldeia global, nas últimas décadas, esse fato tem imposto desafios e chama a atenção de reguladores em todo o Globo, a fim de evitar riscos a direitos fundamentais. A disrupção tecnológica que ocorre pela incorporação de padrões e esquemas novos de atuação, provoca o desarranjo de esquemas de produção e regulatórios vigentes, inaugurada pela Quarta Revolução Industrial.

A partir disso, ampla literatura científica (entre os quais, SCHWAB, SMITH, TAYLOR, CHRISTENSEN, CASTELLS), chama a atenção para a chamada "interrupção regulatória", dado que o novo produto, a tecnologia ou a prática comercial podem não se encaixar bem no marco regulatório vigente. Apesar disso, legislações de vários países endureceram e responsabilizaram as empresas prezando pela proteção de dados pessoais (consumidores, empregados, visitantes etc), sujeitando-as a multas e outras penalidades e possivelmente deixando-as mais propensas a enfrentar litígios jurídicos. Mas uma questão que de longa data preocupa juristas, é justamente a proteção dos dados pessoais (RODOTÀ, 1995, p. 101-2; DONEDA, 2006, p. 141-147).

O fato é que diplomas legais, também a jurisprudência e a doutrina, são insuficientes em matéria de proteção de dados pessoais, entendida essa proteção "uma forma de proteção da privacidade e da vida íntima", segundo o Min. Ricardo Villas-Bôas Cueva, do Superior Tribunal de Justiça do Brasil (CANÁRIO, 2017). Razão disso, é primordial que o Estado e o Direito, na sua função de mantenedor da ordem social e da segurança jurídica, se adaptem às novas circunstâncias, respondendo às demandas atuais, seja através de medidas legislativas ou pela singela atualização de princípios já consolidados a fim de escoltar o desenvolvimento tecnológico.

Saliente-se que, mesmo que a legislação brasileira seja insuficiente quanto ao campo de estudos, criação e aplicação envolvendo robótica avançada, inteligência artificial e tecnologias delas decorrentes, a Constituição Federal de 1988 e da Lei de inovação federal indicam estímulo da pesquisa científica e tecnológica para o ambiente produtivo. Por esse motivo, faz-se primordial a análise dos avanços do direito brasileiro no sentido de zelar pelos bens próprios da Era Digital, assim como por aqueles, já consagrados, que agora se encontram frente à ameaças inéditas, consubstanciada em uma criminalidade sem limites físicos e de difícil rastreio e combate.

Através da realização de pesquisa exploratória e bibliográfica e do levantamento de dados encontrados na literatura, que permitiu a construção da fundamentação teórica do estudo, a investigação objetivou tratar do direito à privacidade na sociedade da informação e da proteção aos dados particulares na seara penal, mediante análise das modalidades de delitos informáticos, cujo alvo ou meio consiste na violação de direitos fundamentais. Ademais, pretendeu levantar se a legislação brasileira tem apresentado suficiência e eficácia, ou se há necessidade de sua adaptação aplicável às relações jurídicas na área, considerada a velocidade das mudanças tecnológicas, ademais de instrumentos de autorregulamentação de cooperação público-privado, com métodos eficazes de combate às violações de dados pessoais.

1. SOCIEDADE DA INFORMAÇÃO: NOVOS PARADIGMAS

Precipuamente, a pesquisa se debruçou sobre a chamada "sociedade da informação", objetivando elucidar o novo contexto socioeconômico no qual a humanidade se encontra após a aurora do mundo virtual. Kofi Annan, então Secretário Geral da ONU,[i] definiu o termo sociedade da informação: "Nós entendemos que é uma sociedade na qual a capacidade humana seja expandida, edificada, alimentada e libertada, dando às pessoas o acesso às ferramentas e tecnologias que elas necessitam, com a educação e treinamento para usá-las de modo eficiente". Surgida no contexto da pós-modernidade, a sociedade da informação é essencialmente informática e comunicacional,

constituída principalmente pelos avanços da microeletrônica, optoeletrônica e multimídia. Adquirir, armazenar, processar e disseminar informações são as metas básicas do novo sistema.

Assim, trata da valorização dos dados e informações particulares, sob uma lente histórica a fim de verificar sua relevância para a sociedade do século XXI. Por esta razão, obras que referenciam o amanhecer do meio-ambiente digital e sua repercussão no Direito se mostraram essenciais: Antropologia Jurídica (1987), de Robert Weaver Shirley, Sociedade em Rede (1999) e A Era da Informação: Economia, Sociedade e Cultura (1999), de Manuel Castells e, Sociedade de Risco, de Ulrick Beck (*apud* BOSCO, 2011).

Os assuntos abordados nessas obras, marcados pela interdisciplinaridade entre Direito e Sociologia, corroboraram para o estabelecimento do seguinte entendimento: as revoluções industriais experimentadas pela humanidade desde o século XVIII, transformaram o arquétipo global em diversos aspectos, social e economicamente. Esses processos disruptivos, marcados pela implementação de novas tecnologias, repercutiram na cadeia produtiva não apenas ao ponto de modificar processos, mas também de consagrar novas riquezas que, indubitavelmente, transformaram o quotidiano do ser humano, impulsionando-o, paulatinamente, à Era Digital experimentada nos dias correntes.

Inúmeras conjecturas são tecidas para delimitar este processo evolutivo da tecnologia, o fato é que o estopim deste encadeamento se deu na Inglaterra, em meados de 1700, onde assistiu-se a substituição da força animal pela não-animal, abastecida pelo carvão e adotada em técnicas de produção massiva, o que em pouco tempo se difundiu pelo Globo, modificando a associação entre o capital e o trabalho (SHIRLEY, 1987, p. 73).

No século XX, a ascensão da eletricidade e o desenvolvimento científico possibilitaram uma nova metamorfose, que Crespo (2011) explica como “a substituição da atividade intelectual pelas máquinas”, fenômeno intrinsecamente vinculado ao advento dos computadores e, a posteriori, da internet cuja importância é indelével para a edificação de todo o cenário ora estudado.

A rede mundial de computadores, criada a partir da necessidade de uma linguagem unificada para a transmissão de informações a um nível global, é o cerne da revolução informacional e pode ser determinada com base em três elementos, quais sejam: “a) uma cadeia de redes interligadas entre si, b) escala mundial, c) comunicação através de uma nova linguagem permitindo-se a circulação de informações através de conversões sequenciais” (SYDOW, 2015), que dão forma ao chamado ciberespaço, um cenário intangível que na obra Direito Digital Aplicado 4.0 (PINHEIRO, 2021), é qualificado como um “ambiente complexo resultante da interação de pessoas, software e serviços na Internet por dispositivos de tecnologia e redes conectadas a ele, ao qual não existe em

qualquer forma física".

Com o surgimento desse novo meio-ambiente e de seus diversos aspectos, a sociedade, outrora concentrada na agricultura e, posteriormente, na indústria, assume uma nova fonte de produtividade, o processamento de informações, ensejando a valorização de novas riquezas, mormente os dados, que, diferente das apreciadas dantes, manifesta-se e impulsiona um contexto social marcado pela globalização.

Para Fuller e Soares (2018, p. 414), esse novo meio vivencia um novo paradigma, a saber:

> [...] desenvolvimento está baseado em dados, informação e conhecimento, ou seja, calcada em bens imateriais, marcada pelo avanço tecnológico, passando a fornecê-los como bases da economia em geral. Através da tecnologia, viabilizou-se o acesso à informação a um público cada vez maior, de forma ágil e quase que instantânea. Além de reduzir distâncias entre os interlocutores e possibilitar a troca rápida de informações, a tecnologia também permite armazená-las e gerenciá-las, agregando-lhes um grande valor quando devidamente tratadas.

Decerto, o aspecto informacional, global e em rede da sociedade pós-industrial (CASTELLS, 2003, 2013), caracterizada pela transação de informações, acaba por evidenciar o prestígio do recurso em comento.

Em suma, pode-se afirmar que a intitulada "Sociedade da Informação" caracteriza-se, entre outros fatores, pela valorização de bens imateriais, a exemplo do segredo industrial e da propriedade intelectual, que, como riquezas tradicionais, requerem a tutela de seus proprietários e, consequentemente, do Direito, sobretudo pela vulnerabilidade do meio em que se encontram, o ciberespaço, onde estão propensos a violações.

Não só os dados e informações são valorizados pelo alvorecer do meio cibernético, mas também o direito à privacidade (previsto na Constituição Federal em seu artigo 5º, inciso X), que, agora, descobre-se em um novo paradigma. Outrora, relacionava-se à ideia de isolamento, compreendendo o "direito de ser deixado só", e sua violação se dava por meios como a intrusão em domicílio alheio (Art. 150, Código Penal), violação de correspondências (Art. 151, Código Penal) e divulgação de notícias na imprensa, mas, hodiernamente, com a fundação desta nova sociedade e o alargamento do fluxo de dados, correspondem, majoritariamente, à violações virtuais, uma vez que as informações particulares de indivíduos, empresas e Estados encontram-se predominantemente depositados em aparelhos tecnológicos e/ou na nuvem de arquivos (DONEDA, 2020).

Razão disso, Tércio Sampaio Ferraz Júnior (1993) já assegurava:

> A privacidade é regida pelo princípio da exclusividade, cujos atributos principais são a solidão (o estar-só), o segredo, a autonomia. Na intimidade protege-se sobretudo o estar-só; na vida privada, o segredo; em relação à imagem e à honra, a autonomia. A privacidade tem, pois, a ver com a inviolabilidade do sigilo, porém, não significa um impedimento absoluto à autoridade fiscal. O acesso aos dados é permitido ainda que seja proibida a interceptação da comunicação.

Privacidade então, está relacionada a muitas questões distintas, como a liberdade e habilidade de definir o espaço pessoal separado do espaço público; de se proteger de intromissões indesejadas; e de controlar o acesso ou a divulgação não autorizada de informações pessoais. Esse direito também se encontra associado aos conceitos de identidade e confidencialidade, anonimato e dignidade humana. Na Internet, existem outros assuntos relacionados, desde a proteção de dados pessoais e propriedade intelectual até a mineração de dados e a cibersegurança. Também está relacionada à coleta, ao armazenamento, ao uso e à circulação de informações conceituadas, de forma variável, como "dados pessoais", ou, às vezes, como "dados pessoais sensíveis", tais como registros de saúde, que exigem formas mais eficientes de proteção e que se distinguem pela diferença do que é considerado "público" ou "proprietário" por sua natureza ou função. O artigo 12 da Declaração Universal dos Direitos Humanos afirma: "Ninguém será sujeito a interferências em sua vida privada, na sua família, no seu lar ou na sua correspondência, nem ataque à sua honra e reputação. Todos os seres humanos têm direito à proteção da lei contra tais interferências ou ataques".

Essas novas perspectivas, oportunizam diversas discussões no âmbito do Direito que, frente à uma realidade, fundada na intitulada "Indústria 4.0", em construção acelerada, se esforça para responder às necessidades da sociedade. Entre as questões proporcionadas pela valorização da virtualidade, verifica-se a do surgimento de uma possível quinta dimensão de direitos humanos.

Fundado na classificação de direitos humanos apresentada por Karel Vasak na década de 70, Sydow (2015, p. 71), em seu "Curso de Direito Penal Informático", aponta uma potencial nova dimensão que, como a quarta, não é unanimemente aceita. Segundo o autor, ao passo em que os direitos humanos de primeira dimensão correspondem àqueles que devem ser garantidos pelo Estado, sem que haja intervenção governamental, e os de segunda, àqueles ditos "de sociedade", os de quinta estariam correlacionados à realidade virtual, de modo a reconhecer a necessidade de proteção dos elementos que existem no ciberespaço:

> Há, pois, um direito humano a exercer as preferências virtualmente sem embaraços e impedimentos, há um direito de possuir uma personalidade virtual e tê-la respeitada, há um direito de comunicar-se virtualmente sem filtros ou controle governamental, há um direito à criação de avatares e personagens em jogos eletrônicos, há um direito a de associar-e livremente de modo coletivo em

> jogos e comunidades virtuais, há um direito a ser respeitado pela imagem, honra e fama virtuais, há um direito a acessar a Internet, há direito de personalização de sua inteligência artificial, direito de personalização de assistentes pessoais virtuais e assim sucessivamente.

No entendimento de Bobbio (1992, p. 34), "(…) o desenvolvimento da técnica, a transformação das condições econômicas e sociais, a ampliação dos conhecimentos e a intensificação dos meios de comunicação poderiam produzir mudanças na organização da vida humana e das relações sociais, criando condições favoráveis para o nascimento de novos carecimentos." Razão pela qual aduz Carvalho (2014, p. 89): "[...] o espaço virtual possui características que demandam uma normatização própria, sob pena de eliminar a possibilidade de identificação dos infratores quando alguém tiver um direito violado, e ao mesmo tempo, de forma a respeitar os direitos fundamentais".

Nessa perspectiva, é inimaginável falar em acesso a informação, sem ressaltar que no âmbito jurídico houve uma crescente evolução no que concerne a inclusão e adequação do direito material ao meio virtual. Regras claras sobre a forma de se obter o consentimento válido, bem como quanto à transferência de dados entre diferentes *players,* é medida que se impõe para que o Brasil entre definitivamente na rota da inovação, garantindo segurança jurídica aos investidores. Para o cidadão, mais do que regras claras, é fundamental que haja uma definição de competência quanto a quem caberá fiscalizar toda a cadeia produtiva de tecnologias emergentes.

Com isso, é possível dizer que hoje, a inclusão digital é um direito fundamental e que a segurança digital é um novo direito humano. Isso porque são poucas as ações cotidianas de pessoas que não requerem a informatização e, apesar disso, a regulamentação ainda é deveras rudimentar. Em outra senda, a Constituição Federal de 1988 estimula o fomento ao desenvolvimento tecnológico (art. 218), a Lei de Inovação (10.273, de 2004, alterada em 2016) dispõe sobre a pesquisa científica e tecnológica para o ambiente produtivo, e a Lei n. 12.965, de 2014, conhecida como o Marco Civil da Internet, regula os direitos e deveres dos usuários da rede mundial de computadores. Cita-se ainda , a Lei Geral de Proteção de Dados e a Lei de Acesso à Informação, as quais importam em inovações ímpares para a tratativa dos dados enquanto bens jurídicos a serem tutelados. Contudo, não regulam o funcionamento nem a criação de robôs e suas nuances atuais e problemas futuros que possam ocorrer.

Ao se compreender, portanto, que a facilidade de acesso e da troca de informações via internet, pode colocar em risco direitos fundamentais consagrados no artigo 5º, X da Constituição Federal de 1988, tais como, a privacidade, a intimidade e a segurança de pessoas e instituições, recentemente, promulgada pelo Congresso Nacional brasileiro, a Emenda a Constituição nº 115, de

10 de fevereiro de 2022, consagrou o *direito fundamental constitucional à proteção de dados*, inclusive no âmbito virtual, estabelecendo uma nova visão do direito à privacidade, atrelada à perspectiva da sociedade da informação. A inclusão desse direito na Constituição Federal, segundo Sarlet (2020), é relevante, pois, "ainda que o artigo 5º, XII, da CF refira o sigilo de comunicações de dados, e o inciso LXXII permita a garantia do procedimento de autodeterminação informacional, este não possui o condão de sustentar a proteção de dados como um direito fundamental autônomo – teríamos, no máximo, um direito implícito".

2. INFORMAÇÃO E DADOS: OBSERVAÇÕES PRELIMINARES

Antes de se aprofundar na temática abordada, faz-se pertinente a elucidação de detalhes relativos à proteção de informações particulares, lidando, especialmente, com os conceitos de dado e informação, e a forma como são tratados pelo Direito, visto que, por vezes, são confundidos, acarretando certa licenciosidade em seu emprego. Na sequência, buscamos averiguar as concepções já estabelecidas pela legislação e pela doutrina, bem como por outras áreas do conhecimento, sobre outros termos e elementos relevantes para o estudo da cibersegurança.

Indubitavelmente, a privacidade, na sociedade pós-industrial, encontra-se, progressivamente, mais vinculada aos dados pessoais e à informação propriamente dita, o que torna inviável o seu estudo sem antes tratar tais elementos à ela inerentes.

Em "Da Privacidade à Proteção de Dados Pessoais", Doneda (2020) leciona que o significado de "informação" é estipulado como o elo entre um emitente e seu destinatário. Trata-se de uma definição simplória que, porventura, pode propiciar a formação da hipótese de que a informação, só, não representa valor ao Direito. Isso tanto é verdade que, a priori, a informação, por si mesma, apresentava-se, para o direito, como uma "categoria alheia à análise jurídica", de modo que as primeiras abordagens sobre ela tivessem natureza mais fenomenológica do que funcional, ou seja, sua relevância, para o mundo jurídico, se dava, tão somente, em virtude de ser comunicada ou por ser suscetível a tal. Assim, não é considerada de maneira direta, mas apenas em suas manifestações específicas, isto é, enquanto elemento da "liberdade de expressão", da "liberdade de imprensa", das "patentes industriais", da privacidade, entre outras.

No entanto, apesar da importância da informação ser notada, principalmente, quando essa se encontra vinculada à outras liberdades individuais, pode ser compreendida como um elemento independente. Por este ângulo, como propõe Pierre Catala (1983, p. 22), a informação não necessita de um suporte ou meio material para ser comunicada, e assim granjear relevância, uma vez que é

"um produto autônomo e anterior a todos os serviços dos quais pode ser o objeto" (*apud* DONEDA, 2020).

Essa visão autônoma da informação é compartilhada pela Lei Geral de Telecomunicações (Lei 9.472/97), que, no parágrafo único de seu artigo 69, conceitua "forma de comunicação" sem confundi-la com a informação propriamente dita, como se pode verificar a seguir (BRASIL, 1997):

> Forma de telecomunicação é o modo específico de transmitir informação, decorrente de características particulares de transdução, de transmissão, de apresentação da informação ou de combinação destas, considerando-se formas de telecomunicação, entre outras, a telefonia, a telegrafia, a comunicação de dados e a transmissão de imagens.

A medida em que o conceito supracitado é difundido, tal qual o prestígio da informação torna-se mais nítido, máxime pela desmaterialização da riqueza e valorização dos bens incorpóreos, podemos denotar a delinear de um recurso promissor e apto ao reconhecimento, no que tange à sua natureza, enquanto bem jurídico. Nessas sendas, atina-se à possibilidade de extensão dos recursos provenientes do direito de propriedade à informação, o que acarretaria em seu derradeiro enaltecimento enquanto bem a ser tutelado e, por consequência, na preocupação com sua defesa através de instrumentos normativos mais claros, rigorosos e eficazes.

Retroagindo ao assentamento de conceitos recorrentes na esfera digital, deparamo-nos com aquele atribuído à "informação pessoal" no artigo 4º, IV da Lei de Acesso à Informação (Lei 12.527/2011), a saber, "aquela relacionada à pessoa natural identificada ou identificável" (BRASIL, 2011), qual confunde-se, essencialmente, com aquele conferido ao "dado pessoal" pelo art 5º, I da Lei Geral de Proteção de Dados (Lei 13.709/2018), que o define como "informação relacionada à pessoa natural identificada ou identificável" (BRASIL, 2018). Com o intuito de sanar essa ambiguidade, façamos uso do conceito de "dado" como algo "mais primitivo e fragmentado", como firmado por Doneda (2020), uma "informação em estado potencial"; "uma espécie de 'pré-informação', anterior à interpretação e a um processo de elaboração".

Ainda sobre o conceito de informação pessoal, o Conselho da Europa, na Convenção 108, de 1981, fez sua contribuição, propondo que compreende "qualquer informação relativa a um indivíduo identificado ou identificável", dando a entender que trata-se do instrumento através do qual é viável determinar uma informação como pessoal: o fato de estar vinculada a uma pessoa, revelando ou podendo revelar algum aspecto objetivo desta. Isso, todavia, não exclui a possibilidade da incidência de dado anônimo, ou seja, dado desvinculado da pessoa a qual se refere, método utilizado por algumas leis de proteção para mitigar os riscos presentes no seu tratamento.

A emergência de novos fatos e valores pessoais e institucionais relacionados à informação na sociedade contemporânea, tem exigido do Direito a adequação e/ou reconstrução de categorias jurídicas. Há pelo menos 30 anos intensifica-se a discussão e a produção legislativa sobre a tutela individual e coletiva da informação. Inicialmente, toda a atenção se voltava ao conceito de privacidade e à proteção do indivíduo, passando mais recentemente à noção mais completa de "proteção de dados" que extrapola a tutela individual. Observa-se um tipo de reconfiguração da garantia legal da inviolabilidade da pessoa e do próprio corpo, para uma dimensão virtual de proteção ao corpo eletrônico, como um direito de liberdade negativa, de não ter seus dados em arquivos eletrônicos e, ao mesmo tempo, de liberdade positiva, de controlar seus dados nestes registros. Assim, passa-se a admitir de forma relativamente independente a proteção à privacidade e aos dados pessoais eletrônicos.

A produção e circulação de informações envolvem direitos e interesses privados e públicos e podem interferir ou influir nas relações e ações sociais e políticas. Na vida política, o direito ao acesso à informação pública é considerado imprescindível à ampla participação e controle social e à responsabilização da Administração Pública. No âmbito social, há uma crescente exigência de informações sobre os mais diversos aspectos da vida, para a tomada de decisões públicas ou privadas que possam afetar a segurança das pessoas ou aquelas que fixem o limite entre a proteção pública, as escolhas individuais de prevenção ou de defesa, e as convenções sociais. Como exemplo, a expectativa de que o acesso à informação em saúde, permita uma melhor qualidade de vida e redução de riscos ao adoecimento, tem legitimado a coleta de dados pessoais, seu uso na identificação de modos de vida, hábitos e outros aspectos da vida privada e intimidade como um dos deveres estatal. A equação constitucional é clara e aplicável a qualquer tipo de informação: o detentor da informação deve o máximo respeito à privacidade dos indivíduos e a máxima transparência dos atos que envolvam interesses públicos.

2.1. DADOS E INFORMAÇÕES PESSOAIS: ATIVOS A SEREM TUTELADOS

A monetarização dos dados pessoais foi uma tendência amplamente antecipada e que hoje é vital para uma parcela bastante representativa de novos serviços e produtos. Em uma declaração que se tornou bastante popular, a Comissária Europeia do consumo, Meglena Kuneva (2009), deixou claro que "os dados pessoais são o novo óleo da Internet e a nova moeda do mundo digital", tornando claro o advento de um novo terreno adentrado pelas relações de consumo, no qual o consumidor passava a ser, em si, a fonte de um ativo que são as suas informações pessoais,

suscitando a necessidade de adequação das normas que regulam o consumo para que levem em conta esta nova situação (DONEDA, 2010).

A importância capital da proteção de dados na Sociedade da Informação reflete-se, por exemplo, no status de direito fundamental que lhe conferiu a Carta de Direitos Fundamentais da União Europeia, referindo-a expressamente em seu Art. 8º.[ii]

A informação pessoal é definida comumente como a informação referente a uma pessoa determinada ou determinável,[iii] apresentando uma ligação concreta com a pessoa. Esta modalidade de informação vem se tornando constantemente mais disponível para uma miríade de utilizações, basicamente por conta da facilidade e do baixo custo de sua coleta e armazenamento com os meios digitais hoje disponíveis. O vínculo da informação pessoal com o seu titular deve ser de tal natureza a revelar diretamente algo concreto sobre esta pessoa.

Assim, a informação pessoal refere-se às suas características ou ações, atribuíveis à pessoa em conformidade com a lei, como no caso do nome civil ou do domicílio, ou então informações diretamente provenientes de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações, como opiniões que manifesta, e tantas outras. É importante estabelecer este vínculo concreto e direto, pois ele afasta outras categorias de informações que, embora também possam ter alguma relação com uma pessoa, não seriam propriamente informações pessoais: as opiniões alheias sobre uma pessoa, por ex., não possuem este vínculo concreto e direto; do mesmo modo que a produção intelectual de uma pessoa, em si considerada, não é per se informação pessoal (embora o fato de sua autoria o seja) (DONEDA, 2010).

Pierre Catala (1983, p. 20) identifica uma informação pessoal quando o objeto da informação é a própria pessoa:

> Ainda que a pessoa em questão não seja a 'autora' da informação, no sentido de tê-la concebido voluntariamente, ela é a titular legítima de seus elementos. O seu vínculo com o indivíduo é por demais estreito para que fosse de outra forma. Quando o objeto da informação é um sujeito de direito, a informação é um atributo da personalidade (tradução livre).

Doneda (2010) destaca que a informação, em si, está ligada a uma série de fenômenos que cresceram em importância e complexidade de forma marcante nas últimas décadas. O que hoje a destaca de seu significado histórico é uma maior desenvoltura na sua manipulação, desde a coleta e tratamento até a comunicação da informação. Aumentando-se a capacidade de armazenamento e comunicação de informações, cresce também a variedade de formas pelas quais ela pode ser apropriada ou utilizada. Sendo maior sua maleabilidade e utilidade, mais e mais ela se torna um elemento fundamental de um crescente número de relações e aumenta sua possibilidade de influir

em nosso cotidiano, em um crescendo que tem como pano de fundo a evolução tecnológica e, especificamente, a utilização de computadores para o tratamento de dados pessoais - conforme notou Stefano Rodotà ainda em 1973, "(...) a novidade fundamental introduzida pelos computadores é a transformação de informação dispersa em informação organizada".

O desenvolvimento acelerado das tecnologias da informação suscitou a elaboração de instrumentos que garantam, (i) proporcionar aos interessados a tutela de suas próprias informações; (ii) proporcionar acesso a informações de qualidade e relevância para ambas as necessidades, o que deve se dar com base na chamada "segurança da informação" que, de acordo com a norma ISO 27001, consiste em uma abordagem abrangente, independente do meio em que são armazenados ou transmitidos os dados, dizendo respeito à preservação da confidencialidade, integridade e disponibilidade das informações no Espaço Cibernético (PECK, 2021).

No entanto, como ocorre em situações nas quais o Direito é chamado a regular um cenário moldado por uma tecnologia de ponta cujos contornos ainda não se encontram bem definidos, a própria compreensão deste cenário, bem como a avaliação dos métodos de maior eficácia, costumam ser tormentosos. Por isso, torna-se necessário, igualmente, que o ordenamento jurídico facilite e garanta a utilização das novas tecnologias da informação, ao mesmo tempo que estabeleça meios de garantia e proteção contra utilizações indesejáveis destas mesmas tecnologias (DONEDA, 2010).

3. CRIMES CIBERNÉTICOS: OS RISCOS DA SOCIEDADE DA INFORMAÇÃO

Da Silveira (2017, p. 15) aduz que na seara dos dados e da informação:

> As sociedades informacionais são sociedades pós-industriais que tem a economia fortemente baseada em tecnologias que tratam informações como seu principal produto. Portanto, os grandes valores gerados nessa economia não se originam principalmente na indústria de bens materiais, mas na produção de bens imateriais, aqueles que podem ser transferidos por redes digitais. Também é possível constatar que as sociedades informacionais se estruturam a partir de tecnologias cibernéticas, ou seja, tecnologias de informação e de controle, as quais apresentam consequências sociais bem distintas das tecnologias analógicas, tipicamente industriais.

Ao lidar com a utilização de recursos ainda não explorados para a produção de riqueza, como os dados e demais bens digitais, a sociedade da informação assume custos sociais como contrapeso às benesses do desenvolvimento, fenômeno comum no percurso dos avanços tecnológicos – como, por ex., se assumiu o risco da poluição ao se ingressar nas atividades industriais – e característico da intitulada "Sociedade de Risco", de Ulrick Beck (2011).

Nesse contexto, os delitos informáticos que violam os dados e informações correspondem ao preço advindo da exploração dos bens proporcionados pela revolução digital. Aqui, no entanto, a criminalidade surge mais complexa, sem limites territoriais ou fronteiras, com anonimato facilitado, riscos físicos dos criminosos reduzido a zero, assim como os esforços durante a ação, óbices quando da investigação e responsabilização dos agentes maliciosos (BRITO, 2013).

Decerto, uma vez que um bem possui relevância econômica, deve possuir, de mesmo modo, relevância jurídica, ensejando sua tutela por parte do Direito, especialmente no âmbito penal. Esse, preocupado com os riscos advindos do uso dessas novas matérias primas, acaba por se debruçar sobre as condutas que as violam, isto é, os intitulados crimes "cibernéticos", "informáticos" ou "virtuais", que, para Tarcísio Teixeira (2018), compreendem práticas ilícitas através de meios informáticos, assim como aquelas cujo objetivo são os próprios sistemas e meios tecnológicos.

No mesmo sentido, Ivette Senise Ferreira (2005) afirma que os crimes cibernéticos podem ser entendidos como toda ação típica, antijurídica e culpável realizada através ou contra processamento automático e/ou eletrônico de dados ou sua transmissão, o que demonstra a generalidade do termo "crime virtual", que acaba por abranger uma vasta gama de possibilidades, haja vista que, sumariamente, consiste em qualquer violação de direitos juridicamente tutelados desde que seja sucedida no ambiente cibernético.

De forma mais específica, os crimes cibernéticos podem ser analisados sob dois aspectos, a saber: impróprios e próprios. Essa primeira categoria compreende os delitos onde o computador ou dispositivo digital é utilizado para a execução do crime como mero instrumento, sem que haja a violação de dados ou informações. No rol de condutas incluídas nesse tipo estão aquelas já tipificadas pela legislação, mas que, com a revolução digital, passam a ocorrer no meio-ambiente cibernético, como por exemplo, crimes contra a honra (calúnias, injúria e difamação), racismo, homofobia e pornografia infantil.

Já os crimes cibernéticos próprios, dizem respeito àqueles onde "a informática é o bem jurídico agredido" (DE JESUS, 2016), de modo que os dados e informações encontram-se entre as riquezas alcançadas pela conduta delitiva, encaixando-os como os principais objetos da presente pesquisa. São exemplos de crimes digitais próprios: a invasão de dispositivo informático, interferência em sistemas, furto de dados ou vazamento de informações, entre outros.

Por sua vez, o Relatório Final da Comissão Parlamentar de Inquérito dos Crimes Cibernéticos (maio de 2016)[iv] apresentou as espécies de crimes informáticos do modo a seguir:

> a) Os crimes virtuais puros englobam toda e qualquer conduta ilícita cujo objetivo seja a violação da integridade física ou lógica do sistema computacional, isto é, tem como finalidade atacar o software (programa), hardware (componente físico do computador, tais como: CPU, monitor, teclado, circuito), dados, sistemas e meios de armazenamentos, etc;
> b) Os crimes virtuais mistos são as condutas em que a utilização de meios computacionais é condição necessária para a efetivação da conduta, embora o bem jurídico lesado seja diverso do informático, tais como a transferência ilícita de valores em uma "homebanking" ou a prática de "salemislacing" (retirada diárias de pequenas quantias em milhares de contas, também conhecida como retirada de saldo).
> c) Os crimes virtuais comuns são aqueles em que os dispositivos computacionais são utilizados apenas como instrumento para a realização de um delito já tipificado pela lei penal, constituindo-se em apenas mais um meio de execução desses delitos, tal como ocorre nos seguintes crimes, já tipificados pela lei penal: o estelionato (art. 171 do CP), a ameaça (art. 147 do CP - Código Penal), os crimes contra a honra (arts. 138 a 140 do CP), a veiculação de pornográfica infantil (art. 241-A do Estatuto da Criança e do Adolescente – Lei nº 8.069/90), o crime de violação ao direito autoral (art. 184 do CP), entre outros.

O ataque cibernético ao Hospital Sírio-Libanês, ocorrido na madrugada do dia 6 de junho de 2020, encontra-se entre os inúmeros exemplares fatídicos destas conjunturas socialmente desagradáveis advindas da relação homem-tecnologia, que afrontam os próprios bens informáticos. Segundo UOL (2018), em artigo veiculado naquele dia, hackers tentaram violar o sistema da instituição fazendo que o Portal do site e aplicativo fossem retirados do ar. Não se sabe a motivação do ataque, mas especula-se que tenha relação com a vastidão de informações sensíveis sob posse do hospital que já tratou a saúde de personalidades relevantes, como artistas e ex-presidentes. O relatório da Norton Cyber Security, destac que os delitos informáticos ocorridos no Brasil, incidiram em um prejuízo de US$ 22 bilhões e impactaram aproximadamente 62 milhões de pessoas em 2017, colocando o país entre as lideranças do rol de países com o maior número de casos de crimes virtuais, onde passa a figurar na 2ª colocação, ficando atrás somente da China que, em 2017, teve um prejuízo de US$ 66,3 bilhões (UOL, 2018).

Segundo o Relatório de Crimes Cibernéticos Norton, que entrevistou cerca de 7 mil pessoas, "ao menos 65% da população adulta mundial já foi uma vítima em potencial. Entre os países com os índices mais altos destacam-se China (83%), Brasil (76%), Índia (76%) e Estados Unidos (73%)" (GABRIELA PORTO ALEGRE, 2019). A pesquisa verificou que os meios de invasão mais comuns são os vírus e ataques de malware, afetando aproximadamente 51% da população, enquanto, na sequência, encontram-se golpes on-line, ataques de phishing, roubo de perfis de redes sociais, fraudes de cartão de crédito e assédio sexual. Ao serem questionados, 79% dos entrevistados afirmaram que não tinham expectativas de que os delinquentes fossem levados à justiça, o que escancara a sensação de insegurança jurídica promovida pela vulnerabilidade inerente ao meio

ambiente cibernético.

Segundo a Coordenação-Geral de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CGCTIR), no ano de 2019 foram registrados 10.732 incidentes envolvendo a segurança dos sistemas de computação ou das redes de computadores, dos quais 2.404 dos casos correspondiam à categoria "vazamento de informação", que figura em 2º lugar no gráfico, um total bastante diferente daquele levantando em 2011, com apenas 20 ocorrências de vazamento.

Essa crescente se dá, entre outros fatores, pela popularização dos smartphones, que alcançaram a marca de 230 milhões no país de acordo com a Pesquisa Anual de Administração e Uso de Tecnologia da Informação nas Empresas, desenvolvida pela Fundação Getúlio Vargas de São Paulo (FGV-SP), e pela difusão do acesso à internet que, conforme indica o IBGE, em 2018, passou a abranger 79,1% dos domicílios brasileiros, 4,2% a mais que no ano anterior. Aliás, a internet compreende um *fato social* imprescindível para a edificação do cenário suso mencionado, uma vez que é responsável pela construção da Sociedade da Informação enquanto elemento fulcral para a hiperconectividade.

O Instituto Brasileiro de Governança Corporativa (IBGC) publicou em 2019, o guia "Papeis e responsabilidade do Conselho na gestão de riscos cibernéticos" para orientar e apoiar as instituições na atualização das melhores práticas de governança corporativa relacionadas justamente à questão do risco cibernético. Há várias definições para esse risco. Aqui, utilizaremos a dada pela International Organization of Securities Commissions (IOSCO, 2016), que é ampla: "Risco cibernético refere-se aos potenciais resultados negativos associados a ataques cibernéticos. Por sua vez, ataques cibernéticos podem ser definidos como tentativas de comprometer a confidencialidade, integridade, disponibilidade de dados ou sistemas computacionais." Reforçando, "Ataques cibernéticos são ofensivos aos sistemas, infraestrutura e dados (operacionais e pessoais) de uma organização e que visam destruir, expor, modificar, roubar ou ter acesso a um ativo ou de usá-lo sem autorização".

Nota-se, por essa definição, que o risco cibernético é vasto e pode incluir dados em qualquer tipo de dispositivo ou serviço, como a computação em nuvem e a internet das coisas. Esse risco está ligado à digitalização dos negócios e à ultra conexão de pessoas e ativos dentro e fora da organização – e daí vem a preocupação com a segurança da informação, ou com um conjunto de práticas que visam a confidencialidade, integridade e disponibilidade da informação. Essa preocupação é crescente, dado que o uso de tecnologias digitais também se expande exponencialmente e que novas modalidades de trabalho, como o teletrabalho, podem abrir novas portas e vulnerabilidades para ataques e que também requerem atenção e conscientização, segundo

o Guia do IBGC.

Dessa forma, o risco cibernético vem galgando degraus no ranking de riscos mais prováveis a que as empresas estão sujeitas. O roubo e a fraude relacionada a dados ocupou o quarto lugar como o risco mais provável nos próximos dez anos, e os ataques cibernéticos capazes de causar interrupção das operações ou infraestrutura ficaram em quinto lugar em pesquisa realizada pelo Fórum Econômico Mundial (2019). Em 2021, além de apontar "iminência de pandemia cibernética",[v] conforme especialistas do Centro de Segurança Cibernética do Fórum Econômico Mundial, "Em 2025, as tecnologias de próxima geração como conectividade onipresente, inteligência artificial, computação quântica ou novas abordagens de gerenciamento de identidade e acesso podem liquidar as defesas e dar início a uma pandemia cibernética global. Acrescentando que:

> [...] as tecnologias da próxima geração representam novos riscos para o mundo, e seu impacto não é totalmente compreensível neste estágio. Há uma necessidade urgente de ação coletiva, intervenção política e maior responsabilização por organizações governamentais e empresas privadas. Sem esta intervenção, será difícil manter a confiança nas novas tecnologias, das quais depende o futuro desenvolvimento do mundo.

Recentemente, o Relatório de Risco Global 2022 (Global Risks Report 2022),[vi] elaborado e divulgado no Fórum Econômico Mundial de Davos, confirmou o que os especialistas em cibersegurança já previam: "a falha de segurança cibernética apareceu entre os 10 principais riscos que mais pioraram desde o início da crise do COVID-19". De fato, o cenário pandêmico proveniente do COVID-19, provocou um recolhimento social a nível global. Essas circunstâncias se vinculam ao aumento da criminalidade virtual em decorrência do êxodo de atividades para o ambiente cibernético através do *home office* e de outras medidas como a implementação do sistema de estudo a distância/remoto pelas instituições de ensino. Como mencionado por Martha Imenes (2020), em matéria publicada aos 06 de setembro de 2020, essas conjunturas são propícias para os criminosos virtuais, que "ficam à espreita para praticar os mais diversos cibercrimes, como roubo de senhas, de dados, compras via clonagem de cartão", entre outros.

Na ocasião, a jornalista ainda faz menção aos dados alarmantes, relativos ao ano de 2020, provenientes da Fortinet Threat Intelligence Insider Latin America, "ferramenta que coleta e analisa incidentes de segurança cibernética em todo o mundo, aponta que no Brasil já ocorreram mais de 2,6 bilhões de ataques cibernéticos de janeiro a junho, de um total de 15 bilhões em toda a América Latina e Caribe" (IMENES, 2020).

No tangente a 2021, pesquisa da empresa de segurança cibernética Kaspersky aponta, no Brasil, o aumento de 23% nas incidências de crimes virtuais entre janeiro e agosto, em relação ao mesmo período do ano anterior. Segundo a análise, "golpistas brasileiros são responsáveis por 481 milhões de tentativas de infecção dos 20 malwares mais populares - o que equivale a 1.395 tentativas por minuto" (LOURENÇO, 2021).

O Relatório de Risco Global 2022 do Fórum Econômico Mundial reforça, "A crescente dependência da tecnologia, combinada à democratização das criptomoedas, tem criado o ambiente ideal para os invasores motivados financeiramente". Segundo o relatório, somente de 2019 para 2020, o valor de criptomoedas recebido por ataques do tipo ransomware[vii] aumentaram de US$93 milhões para US$406 milhões, um crescimento gigantesco". No Brasil, o ano de 2022 será ainda mais desafiador, que segundo Capella (2022):

> [...] avançamos na jornada de adoção da nuvem, do open finance e evoluímos no acesso ao 5G. O país ainda passará por eleições presidenciais, momento que propicia a ampliação da exposição a ataques. Para minimizar o risco, empresas e governos devem adotar estratégias de 'confiança zero' ou Zero Trust, estando preparados para mapear e gerenciar corretamente o seu ambiente de tecnologia da informação, incluindo possíveis vulnerabilidades, gerenciamento de identidades e acessos digitais, e melhora das práticas de desenvolvimento seguro.

Para tanto, indica urgência máxima com atenção e cooperação dos setores público e privado para minimizar riscos, evitando a exposição de milhares de dados e, o impacto nos negócios das corporações e governos.

Embora certos ataques cibernéticos se concentrem em organizações específicas, a maioria visa o maior número possível de usuários da Internet. Tais ataques geralmente são relativamente fáceis de serem realizados pelos cibercriminosos e podem causar sérios danos. O impacto da atividade maliciosa indiscriminada online pode ser significativo e acarretou um preço global estimado de US$6 trilhões em 2021. Portanto, "A segurança cibernética está se tornando uma questão de segurança pública" (Amy Jordan, líder da plataforma para moldar o futuro da segurança cibernética e do Digital Trust do Fórum Econômico Mundial, 2020).[viii]

Razão disso, o Centro do Fórum Econômico Mundial para Segurança Cibernética (2020)[ix] reuniu um grupo de Provedores de serviços de Internet (ISPs) compostos por líderes e organizações multilaterais, para desenvolver novas maneiras (princípios-chaves) de proteger e impedir que esses ataques cheguem aos consumidores. A iniciativa de "convocar os *stakeholders* do setor público e privado para compartilhar e implementar as melhores práticas do setor, (...) ajudam não apenas as organizações envolvidas, mas também os usuários da Internet em geral" (Kevin Brown, Diretor da

BT Security).[x] Vejamos os princípios dos ISPs:

> **1.** Proteja os consumidores por padrão de ataques cibernéticos generalizados e aja coletivamente com os colegas para identificar e responder a ameaças conhecidas.
> **2.** Agir para aumentar a conscientização e a compreensão das ameaças e apoiar os consumidores na proteção de si mesmos e de suas redes.
> **3.** Trabalhe mais de perto com fabricantes e fornecedores de hardware, software e infraestrutura para aumentar os níveis mínimos de segurança.
> **4.** Tome medidas para reforçar a segurança de roteamento e sinalização para reforçar a defesa eficaz contra ataques. [xi]

Conforme os indicadores citados aumentam – o que é inevitável – resta nítida a necessidade de esforços por parte de vários ramos do Direito, mormente o penal, a fim de minimizar os danos provenientes desse novo contexto sócio-econômico, propiciando o desenvolvimento da sociedade da informação e da indústria 4.0, ao passo em que garanta instrumentos eficazes de segurança jurídica aos cidadãos.

O ponto de discussão gira em torno do campo da previsibilidade e controle de riscos e violação de direitos fundamentais, preocupações sobre segurança física, por ex., caso falhe o código de um robô, ou as decorrentes de potenciais consequências da avaria do sistema ou de ataques informáticos a sistemas robóticos interligados, numa altura em que são desenvolvidas e utilizadas cada vez mais aplicações autônomas, sejam estas destinadas a carros e a aeronaves pilotadas à distância (*drones*), a robôs que prestam assistência ou a robôs utilizados para a manutenção de ordem pública e do policiamento.

A informática proporciona uma fácil interação entre as pessoas e, caso não seja utilizada de forma correta, acaba por ser um meio eficaz na prática de delitos, o que "torna necessária a atuação do Estado no sentido de coibir esse tipo de conduta, sendo necessária a criação de tipos penais ainda não previstos na legislação e que envolvam o mundo virtual, uma vez que não é permitido, em Direito Penal, utilizar analogia em relação às tipificações já existentes" (POLEGATTI; KAZMIERCZAK, 2012, p. 1, 2, 8).

Na mesma direção, há quem defenda que o direito penal tradicional se tornou insuficiente para resolver os problemas surgidos pelas problemáticas da pós-modernidade e da globalização ligadas à ideia da "sociedade de risco" estudada pelo sociólogo Ulrich Beck (*in* BOSCO, 2010, p. 1).[xii] Tal como aduz Smanio (2000, p. 27): "A sociedade de massa trouxe fenômenos sociais e jurídicos que não poderiam ser adequadamente resolvidos dentro da legislação então vigente, fundamentada na proteção individual". Conforme salientado por Figueiredo (2007, p. 134) "esta ideia suscita ao direito penal problemas novos, ao pôr em evidência uma transformação radical da sociedade em que vivemos e que seguramente se acentuará no futuro":

> Ela anuncia o fim de uma sociedade industrial em que os riscos para a existência, individual e comunitária, ou provinham de acontecimentos naturais (para a tutela dos quais o direito penal é incompetente), ou derivavam de acções humanas próximas e definidas, para contenção das quais era bastante a tutela dispensada a clássicos bens jurídicos como a vida, o corpo, a saúde, a propriedade, o património, em suma, o catálogo próprio de um direito penal liberal e extremamente *antropocêntrico*. Anuncia o fim desta sociedade e a sua substituição por uma sociedade exasperadamente tecnológica, massificada e global, onde a acção humana, as mais das vezes anónima, se revela susceptível de produzir riscos globais ou tendendo para tal, susceptíveis de serem produzidos em tempo e em lugar largamente distanciados da acção que os originou ou para eles contribuiu e de poderem ter como consequência, pura e simplesmente, a extinção da vida.
> Ora, diz-se, para tutela destes riscos não está preparado o Direito penal de vertente liberal. [...] A adequação do direito penal à "sociedade do risco" implica por isso uma nova **política criminal**, que abandone a função minimalista de tutela de bens jurídicos e aceite uma função promocional e propulsora de valores orientadores da acção humana na vida comunitária.

Assim como a ampliação do uso da inteligência artificial e da robótica avançada, novas irrupções ocorrerão fatalmente, e o Direito não pode ser o algoz do desenvolvimento. Como revelado pelas tecnologias de reprodução assistida, genética e nanotecnologia, as tecnologias emergentes trazem avanços científicos, mas também desafios sociais e de regulamentação jurídica.

4. CIBERSEGURANÇA: PROTEÇÃO INFORMACIONAL

Como apresentado acima, diariamente nos deparamos com conjunturas desagradáveis provenientes da relação entre pessoas e o universo virtual, algumas dessas situações são aparentemente inofensivas, ao passo em que outras apresentam reais ameaças ao indivíduo, empresa ou governo, haja vista que todos esses sujeitos encontram-se vinculados através das redes e, por consequências, suscetíveis à violações que podem afetar não só o bem-estar dos cidadãos ou clientes, como também gerar prejuízos milionários.

Nesse contexto, surge a necessidade e preocupação para com a segurança cibernética, que, em síntese, corresponde àquela referente às informações que se encontram nos meios digitais, segundo as definições presentes na ISO 27032 de 06/2015,[xiii] cuja efetividade encontra-se condicionada à participação e empenho dos muitos participantes dessa cadeia vinculada pela transmissão de dados.

Em suma, a cibersegurança requer a atenção de empresas e de governos para com a segurança da informação[xiv] através de investimentos em sistemas de proteção, a fim de atenuar os riscos e os efeitos dos crimes virtuais, mas também o cuidado pessoal de cada cidadão para com

suas informações particulares, sejam elas utilizadas no âmbito de trabalho ou nas redes sociais.

Com o intuito de auxiliar na promoção de medidas de cibersegurança no Brasil, bem como na educação da população para lidar com as adversidades da internet, faz-se mister, não só a criação de leis coerentes com a realidade experimentada pela sociedade, mas também o fomento de instituições que prestem suporte aos usuários da rede mundial de computadores, como o CERT.br (Centro De Estudos, Resposta e Tratamento De Incidentes de Segurança no Brasil) e o CERT internacional (Computer Emergency Response Team).

No âmbito empresarial e governamental, o treinamento de profissionais e o investimento massivo no desenvolvimento de bloqueios aos ataques e saneamento de vulnerabilidades se mostram fundamentais, devendo contar, sobretudo, com a assistência de figuras especializadas, intituladas *white hats* ou *hackers* éticos, correspondem à força antagônica aos *crackers,*[xv] ou seja, a parcela de hackers que se submete à lei e tem a proteção de computadores, software, redes e infraestruturas de TI como norte de suas ações. "In a dichotomic world, they are the good guys" (JAQUET-CHEFFELE; LOI, 2020, p. 182).

Costumeiramente, essas figuras surgem no cenário institucional como componentes de Times de Respostas a Incidentes de Segurança, a saber, organizações encarregadas de tratar de "qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores" (CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL, 2017) ao qual a entidade sob tutela, seja empresarial, governamental ou acadêmica, encontra-se submetida.

Nesse contexto, com o fito de promover a tutela que lhe cabe, o *ethical hacking*[xvi] emprega a defesa cibernética que, comumente, é concebida em duas perspectivas: a ativa, caracterizada pela ação direta contra as ameaças virtuais com o propósito de aniquilá-las ou reduzir seus efeitos, e a passiva que encerra quaisquer formatos de proteção, desde que indiretos, que visam a minimização dos resultados dos ataques cibernéticos (DENNING; STRAWSER, 2017).

Essa última abrange métodos de prevenção a ataques cibernéticos como testes de segurança que buscam por vulnerabilidades no sistema da entidade, colocando à prova o êxito das defesas dos sistemas com o intuito de sanar qualquer fragilidade detectada.

Já a defesa ativa, corresponde aos chamados *counterstrikes,* requer uma análise mais atenta uma vez que faz uso dos mesmos meios que o agente malicioso durante o processo de tutela dos bens e direitos da vítima.

Para fins de esclarecimento, vale pontuar que prática da defesa ativa pelo *hacker* ético consubstancia-se no *hacking back*, isto é, literalmente, contra atacar o remetente do ataque

cibernético com a finalidade de obter sua localização ou até mesmo causar danos aos seus sistemas informáticos como forma de garantir a segurança do alvo ameaçado. Nesse sentido, Dorothy Denning define a modalidade supracitada como sendo (2008, p. 422):

> [...] uma forma de resposta ativa que usa hackers para combater um ataque cibernético. Existem duas formas principais. A primeira envolve o uso de rastreamentos invasivos para localizar a origem de um ataque. A segunda envolve contra-atacar uma máquina atacante para desligá-la ou pelo menos fazer com que ela pare de atacar.[xvii]

Em apertada síntese, a defesa ativa pode ser caracterizada como esforços ofensivos cujo objetivo é a neutralização de uma ameaça imediata através de sua detecção, rastreio e, por fim, interrupção, respondendo ativamente a um ataque em desenvolvimento para mitigar os danos ao sistema. Logo, em que pese a importância da segurança passiva e os testes com o propósito de aprimorá-la, a defesa ativa assume um caráter de maior eficiência e relevância no confronto à criminalidade virtual.

Na esfera estatal, por exemplo, as ameaças digitais surgem com um aspecto mais crítico do que "simples" *script kiddies,* uma vez que seu alvo pode representar conteúdo com grau de segurança nacional, o que exige algo além que a pura defesa passiva. Aqui, identificar a fonte dos ciberataques, que pode ou não ser estrangeira, é de suma importância para resguardar os bens imateriais do Estado, como informações restritas, que podem possuir as mais diversas materias, como questões comerciais ou até mesmo bélicas, a fim de extinguir ou, ao menos, minimizar os prejuízos causados pelo incidente, assim como identificar o delinquente para que seja devidamente penalizado como demanda o art. 154-A, § 5º, do Código Penal.

No âmbito corporativo, a importância da cibersegurança não é menor. Para empresas é de grande pertinência que seu patrimônio informacional encontre-se protegido, dada sua relevância no cenário da sociedade hodierna onde, cada vez mais, os dados e informações assumem caráter de riqueza. Todavia, o campo privado não dispõe de proteção estatal permanente, mas nem por isso deixa de ser ameaçado pela delinquência eletrônica, o que demonstra a necessidade de grupos destinados à prática do *ethical hacking* em seu quadro organizacional, visando o monitoramento constante das redes e sistemas para que, quando imprescindível, possa responder adequadamente, e sem tardar, à quaisquer violações.

4.1. A LEGISLAÇÃO BRASILEIRA E A PROTEÇÃO CONTRA A CIBERCRIMINALIDADE

O ordenamento jurídico brasileiro não possui regulamentações abrangentes que contemplem, explicitamente, a segurança cibernética. A despeito dos esforços para se construir uma estrutura legislativa eficaz que tenha como escopo a cibersegurança, o arcabouço legislativo sobre a temática vem sendo desenvolvido paulatinamente, satisfazendo, assim, as necessidades momentâneas através da elaboração de leis esparsas.

Entre as tentativas brasileiras de tratar legislativamente dos crimes cibernéticos, verifica-se o Projeto de Lei n. 84/99, que almejava tipificar crimes cometidos na área de informática, mormente aqueles intitulados "informáticos próprios", determinando suas penalidades, através de modificações em trechos do Código Penal e do Código Penal Militar. Todavia, somente em 2012 foi promulgada a Lei 12.737, também conhecida como "Lei Carolina Dieckmann", em razão das circunstâncias que aceleraram sua tramitação, com objetivo de tipificar a "invasão de dispositivo informático" e "interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública", sendo, até a atualidade, a mais significativa inovação legislativa no sentido de lidar com crimes cibernéticos e a cibersegurança.

Alterada pela Lei 14.155, de 2021 que, entre outras, modificou a redação do caput do art. 154 do Código Penal, aumentando a incidência do tipo penal, ao excluir o trecho "mediante violação indevida de mecanismo de segurança", de modo a deixar de exigir violação ativa de medidas de proteção. Além disso, majorou a pena do crime do art. 154-A, que tipifica a invasão de dispositivo informático alheio, cuja pena foi alterada de 3 (três) meses a 1 (um) ano, e multa, para 1 (um) a 4 (quatro) anos de reclusão. O limite da causa de aumento de pena de seu §2º também mudou, de um sexto a um terço da pena, para 1/3 (um terço) a 2/3 (dois terços), ao passo em que a qualificadora do §3º teve sua pena majorada de 6 (seis) meses a 2 (dois) anos, e multa, para 2 (dois) a 5 (cinco) anos, e multa. Também o art. 155 do Código Penal, recebeu a qualificadora de furto mediante fraude cometido por meio de dispositivo eletrônico ou informático.

Outro insigne instrumento normativo na alçada ora analisada, é Lei 12.965/2014, intitulada de Marco Civil da Internet que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, ratificando elementos que fundamentam a tratativa da cibersegurança no país, como o registro de dados, protocolo de internet e sobre a requisição judicial de registros, entre outros.

Também no sentido de corroborar com a construção de diretrizes que versem sobre a proteção de dados e a segurança da informação, de modo especial a empresas e às organizações do Estado, a Lei nº 13.709/2018 ou Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em agosto de 2020, se destaca ao contribuir com a consolidação de boas práticas de segurança, sobretudo por chamar a atenção para a cibersegurança, elencada, em seu art. 6º, como ponto nevrálgico no tratamento de dados pessoais, assim como por exigir a implementação de medidas técnicas e administrativas para proporcionar segurança ao tratamento dos dados pessoais contra incidentes, haja vista seu art. 46 que dispõe:

> Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

É notável o empenho governamental na tentativa de enfrentar as adversidades da sociedade da informação, especialmente na década de 2010, um período marcado pela inclusão de documentos basilares para auxiliar e nortear a atuação estratégica do Brasil na esfera cibernética, como por exemplo a Política Cibernética de Defesa e a Doutrina Militar de Defesa Cibernética, que, veiculados pelo Ministério da Defesa, demonstram progresso, ainda que vagaroso, no sentido de se valorizar a segurança da informação no Brasil.

Em fevereiro de 2020, foi publicado o Decreto 10.222, que apresentou a Estratégia Nacional de Segurança Cibernética (e-Ciber), que, como a Estratégia Brasileira para a Transformação Digital (e-Digital) de 2018, apresenta diretrizes nacionais para a tratativa do assunto, sendo o "o primeiro documento oficial que visa proporcionar um panorama sobre o papel do Brasil na segurança cibernética, bem como os objetivos e princípios norteadores para seu desenvolvimento entre os anos de 2020 e 2023" (HUREL et al., 2021).

Por fim, há de se mencionar a mais nova evolução brasileira no âmbito da proteção de dados, a saber, a constitucionalização do direito fundamental à proteção de dados (PEC nº 17/2019 – EC 115/2022, promulgada pelo Congresso brasileiro em 10 de fevereiro de 2022), inclusive no âmbito virtual, consagrando uma nova visão do direito à privacidade, atrelada à perspectiva da sociedade da informação. A Emenda a Constituição também atribui à União as competências de legislar, organizar e fiscalizar a proteção e o tratamento de dados pessoais.

Certo é, que o avanço normativo representa a adequada preocupação do poder legiferante no sentido de robustecer o arcabouço jurídico sobre o tema, tornando indiscutível a sua fundamentalidade e propiciando cenários mais benéficos para a implementação das demais leis, como a Lei Geral de Proteção de Dados Pessoais, que tem sua eficácia fortalecida.

5. PRÓXIMOS PASSOS

A diminuição da capacidade regulatória do Estado com o surgimento de novos problemas globalizados relaciona-se, paradoxalmente, com o "incremento das tarefas que se apresentam ao Estado em face dos novos desafios da sociedade mundial" (NEVES, 2009, p. 34). Nesse sentido, se leva em conta que o Estado é o foco fundamental da reprodução da nova ordem normativa mundial, contudo, não se desconhece a emergência de novos atores, sistemas, regimes ou redes globais com pretensão de tomar decisões coletivas envolvendo a produção de normas jurídicas.

Em relação à produção legislativa, é apontado um alargamento e uma desformalização dos procedimentos. Isso ocorre porque quanto maior a complexidade e o risco apresentado pelas matérias a se normatizar, a exemplo da inteligência artificial e da robótica avançada, menos os setores institucionais responsáveis manifestam-se dispostos a assumir com exclusividade a responsabilidade, passando, assim, a delegar parte dela à sociedade ou aos *stakeholders* (clientes, acionistas, colaboradores, fornecedores, bancos, reguladores), por meio de consultas públicas, audiências públicas, programas de compliance digital e criminal no seguimento de e-commerce de consumo, relatórios técnicos etc. De fato, Schepel (2005) relata que no mundo econômico, há longa data a autorregulação industrial introduz *standards* técnicos, *compliance programs*, recomendações, códigos de conduta e de responsabilidade tanto em nível nacional como regional, "e também em âmbito global" (DILLING, 2008).

Dilling (2008) aduz que o contexto da territorialidade das jurisdições nacionais e do lento progresso do direito internacional com base no princípio da soberania, representa um sério desafio, com isso, é dada atenção ao potencial da auto-regulação e governança privada por corporações multinacionais e redes econômicas transnacionais, que se diluíram cada vez mais (mas certamente não tornaram irrelevante) o papel do Estado e de seus processos formais de lei. O autor acredita claramente, que a regulamentação oficial e privada pode funcionar em conjunto, aumentando o impacto global dos objetivos regulatórios, apresentando evidências empíricas e teóricas convincentes para apoiar essa crença.

O Plano de Ação da Agenda de Túnis para a Sociedade da Informação de 2005,[xviii] sobre governança da internet, afirmou que a internet se converteu em um recurso global disponível para o público e que, por isso mesmo sua governança deveria se constituir em um elemento essencial na Agenda da Sociedade de Informação. Indicando ainda, que a gestão internacional da internet deveria ser multilateral, transparente e democrática, tedo a participação de todos os governos, do setor privado, da sociedade civil e das organizações internacionais (Documentos da Cúpula Mundial sobre a Sociedade da Informação, 2005, p. 87).

O certo é que, regulamentar o campo digital-cibernético, exigirá novas abordagens em matéria de governança responsável, antecipatória e participativa, e a avaliação da tecnologia em tempo real. Governança aqui, refere-se às ações, processos, tradições e instituições pelas quais a autoridade é exercida e as decisões são tomadas e implementadas, em especial para contribuir com a identificação, avaliação, gestão e comunicação de riscos em um contexto amplo. Deve incluir a totalidade dos atores, regras, convenções, processos e mecanismos e preocupar-se com a forma como as informações relevantes de risco são coletadas, analisadas e comunicadas e como as decisões de gestão são tomadas. Ela aplica os princípios da boa governação para o manejo de risco. A disposição e a capacidade para assumir e aceitar o risco é fundamental para alcançar o desenvolvimento econômico e a introdução de novas tecnologias.

A regulação de risco na esfera de proteção de dados pessoais implica necessariamente no conjunto dos seguintes elementos:

> (i) instrumentos de tutela coletiva e participação de entidades civis no diálogo preventivo com autoridades independentes de proteção de dados pessoais, (ii) obrigações e instrumentos de regulação ex ante atribuídas aos controladores para identificação de riscos a direitos e liberdades fundamentais, (iii) disseminação de metodologias de "gestão de risco" e calibragem entre riscos gerados pelo tratamento e uso de dados pessoais e imunidades jurídicas construídas pela discussão ética sobre os limites do progresso técnico (ZANATTA, 2017, p. 183).

Wolfgang Hoffmann-Riem (2019, p. 536) faz uma análise acerca da influência individual, privada, social e estatal na regulamentação da sociedade informacional do ordenamento jurídico alemão. No direito pátrio, há situações consonantes às explicitadas no direito alemão, pois, os fenômenos dos avanços tecnológicos, e da comunicação se dão de forma global. Para o autor, a autorregulamentação ("selbst regelung"), ou "auto-organização", é compreendida, como as "medidas individuais ou conjuntamente empreendidas para a realização de objetivos por comportamento autônomo próprio." O jurista traz como exemplo, os produtores do setor de TI, que criam regras comportamentais, compromissos morais, códigos de conduta, e etc. Já quanto à regulação ("regulierung"), diferentemente da autorregulamentação, há a preponderante intervenção estatal, "em processos sociais, que com o objetivo específico, estabelecem diretrizes gerais de comportamento, as quais criam ou mantêm estruturas funcionais para resolver problemas específicos" (HOFFMANN-RIEM, 2019, p. 532).

Rafael Zanatta (2017, p.184-5) destaca que o Regulamento Geral de Proteção de Dados europeu traz definições e critérios de diferenciação de "risco" e "risco elevado", assim como determina que o responsável pela decisão do tratamento de dados deve auferir a potencialidade e grau de risco. Isto posto, o autor se apoia em Hirsch, para apontar o fenômeno da "co-regulação",

na qual, com base no regulamento de proteção de dados, os próprios entes responsáveis pelo tratamento de dados atuam como reguladores de risco ao definir padrões, galgar certificações, elaborar práticas de condutas, e seguir determinações de diretrizes por parte do encarregado pela proteção de dados pessoais. Frazão, Oliva e Abílio (2019, p. 684-5) tratam a "co-regulação" como um sinônimo de uma "autorregulação regulada", pois, a atividade estatal, e a entidade privada, atuam de forma colaborativa, com nítida influência e troca de experiência ao tratarem dados pessoais.

Nada obstante às construções já sedimentadas pelo direito brasileiro, denota-se a necessidade de fazer ainda mais, uma vez que as tecnologias prosseguem em desenvolvimento acelerado, tal qual a criminalidade que as ameaça. À vista disso, verificamos a urgência da implementação da governança da segurança cibernética em escala nacional, isto é, a edificação de uma infraestrutura de segurança da informação, consubstanciada em "instituições, iniciativas, políticas, programas e entre outros mecanismos (formais e informais) que integram um ecossistema de competências e responsabilidades distribuídas para a segurança cibernética" (HUREL, et al. 2021).

A Estratégia e-Ciber já representa um passo significativo nessa direção, pavimentando as sendas nas quais respostas mais pungentes poderão se fundar em um futuro próximo. O próprio dispositivo faz referência ao recém cunhado termo "governança da segurança cibernética", apresentando, assim, um norte para as ações a serem desenvolvidas nos próximos anos (BRASIL, 2020).[xix]

Esse trabalho, porém, não há de ser desenvolvido, tão somente pelo Estado, pelo contrário, requer uma ampla colaboração entre diversos setores da sociedade, seja no âmbito da sociedade civil, órgãos de combate à criminalidade cibernética, como Ministério Público Federal, Polícia Federal e Delegacias Especializadas da Polícia Civil, o setor público, financeiro, a defesa nacional, a comunidade técnica e o setor privado (HUREL, et al. 2021).

Em "Uma Estratégia para a Governança da Segurança Cibernética no Brasil", publicado em Setembro de 2018 pelo Instituto Igarapé, Hurel e Lobato, informam que o estudo faz referência a um processo amplo de governança, que compreende arranjos formais e informais de cooperação entre os diferentes atores que compõem a estrutura de segurança cibernética brasileira, sob a abordagem, que, fundamentada nos processos de governança da segurança cibernética, lança luz sobre outras possibilidades de colaboração entre setores que dificilmente são vislumbrados a partir de uma estrutura mais rígida pautada em agrupamentos de competências (segurança cibernética, segurança da informação e defesa cibernética). O estudo indica que, a consolidação de uma estrutura coerente de governança de segurança cibernética facilitará a identificação e o compartilhamento de

boas práticas, bem como estimulará uma crescente coordenação entre setores, tão necessária para responder aos crescentes desafios para a segurança, estabilidade e resiliência das redes. Segundo o relatório,

> O processo de institucionalização da segurança cibernética no Brasil foi catalisado por dois eventos principais. O primeiro foi a aprovação do Marco Civil da Internet, em 2013, motivado pelo impacto político das revelações a respeito da estrutura de vigilância virtual dos Estados Unidos. O segundo foi consequência direta dos megaeventos sediados no país entre 2012 e 2016, que incluem esforços como (i) a criação do Centro de Defesa Cibernética (CDCiber); (ii) a construção de capacidades de instituições públicas nos âmbitos federal e municipal; (iii) o incremento da colaboração entre governos e setor privado; e (iv) o estabelecimento de doutrinas, políticas e diretrizes relacionadas à segurança cibernética.

Através dessa cooperação multissetorial, é possível alcançar os mais vastos grupos populacionais, engendrando conhecimento acerca da segurança da informação e, quiçá, a popularização e incentivo da prática do *ethical hacking,* passiva e ativamente, sob a supervisão das instituições governamentais de combate aos incidentes cibernéticos.

Outrossim, uma maior participação brasileira na discussão sobre a cibersegurança a nível internacional também seria de grande valia para o desenvolvimento do país, como, por ex., a adesão à Convenção de Budapeste sobre Crimes Cibernéticos de 2001 do Conselho da Europa,[xx] ou simplesmente, Convenção sobre Cibercrime ou Coonvenção de Budapeste, primeiro tratado internacional sobre a matéria, ainda não ratificada pelo Brasil,[xxi] que mostraria ao mundo a abertura do país para ocupar-se de uma problemática atual que é preocupação, sobretudo, para as maiores potências do globo. De fato, tendo em mente que delitos criminais passaram a ser praticados exponencialmente por intermédio de ferramentas computacionais e informáticas "desde o advento da internet na década de 1990 para fins civis e comerciais, incluindo práticas de ataques cibernéticos, a discussão reforçada em foros multilaterais, como no Conselho da Europa, apenas endossa a preocupação de política normativa" (POLIDO, 2021).

CONSIDERAÇÕES FINAIS

O presente estudo possibilitou uma análise abrangente da evolução brasileira no âmbito da cibersegurança, através de uma tratativa sistemática da edificação do novo cenário sócio-econômico no qual nos encontramos, bem como dos bens e riscos que com ele nasceram.

Percebe-se, no entanto, que o arcabouço jurídico sobre o assunto é esparso, estando contido em diferentes instrumentos normativos, de maneira a dificultar a unificação da linguagem e a

comunicação entre os agentes multissetoriais, o que promoveria uma abordagem mais efetiva do tema ora analisado através da edificação de uma sólida infraestrutura para a governança da segurança cibernética.

Em virtude disso, resta nítida a necessidade de uma atuação mais precisa, com um código e instituições que reúnam as atribuições e assuntos pertinentes à cibersegurança, a fim de atuar de modo mais eficaz e conciso na esteira do combate à criminalidade virtual e à proteção dos dados e informações.

Uma vez comprovada a pungência dos prejuízos advindos de tal delinquência, pode-se captar a urgência de investimentos massivos na educação em cibersegurança e no suporte às equipes de combate ao crime virtual, assim como a majoração das penas de modo a desestimular a prática delituosa.

É indiscutível que o caminho a ser percorrido pelo Brasil é longo. No entanto, também é incontestável que passos importantes já foram dados pela nação rumo à uma maior segurança jurídica no uso dos meios cibernéticos e no reconhecimento dos direitos de seus usuários.

REFERÊNCIAS

BITTAR, Eduardo C.B. A Teoria do Direito, a Era Digital e o Pós-Humano: o novo estatuto do corpo sob um regime tecnológico e a emergência do Sujeito Pós-Humano de Direito. **Rev. Direito Práx**., Rio de Janeiro, Vol. 10, n. 02, 2019, p. 933-961. Eduardo C. B. Bittar DOI: 10.1590/2179-8966/2018/33522| ISSN: 2179-8966 https://www.scielo.br/j/rdp/a/5MqNJXcvc9chdXnvPNZsjmk/?lang=pt&format=pdf. Acesso Junho de 2021.

BOBBIO, Norberto. **A era dos direitos**. Rio de Janeiro:Campus, 1992.

BOSCO, E. A Política Na Sociedade de Risco - Ulrich Beck. **Ideias**, Campinas, SP, v. 1, n. 2, p. 229–253, 2010. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/ideias/article/view/8649300. Acesso Abril de 2021.

BRASIL. CÂMARA DOS DEPUTADOS. CPI - Crimes cibernéticos: comissão parlamentar de

inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país.. Brasília, 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D%3E+RCP+10/2015. Acesso Junho de 2021.

BRASIL. Decreto n° 678, de 6 de novembro de 1992. Promulga a Convenção Americana sobre Direitos Humanos (**Pacto de São José da Costa Rica**), de 22 de novembro de 1969. Disponível em:http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso Abril de 2020.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848compilado.htm. Acesso Abril de 2020.

BRASIL. Conselho Nacional de Justiça. **Crimes digitais**: o que são, como denunciar e quais leis tipificam como crime? 2018. Disponível em: http://www.cnj.jus.br/noticias/cnj/87058-crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime. Acesso Abril de 2020.

BRASIL. Lei 12.527, de 18 de Novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm> Acesso Set. 2020.

BRASIL. Lei 12.965, de 23 de Abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso Set. 2020.

BRASIL. Lei 13.709, de 14 de Agosto de 2018. **Lei Geral de Proteção de Dados Pessoais** (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em Set. 2020.

BRASIL. IBGE. Pesquisa Nacional por Amostra de Domicílios Contínua. PNAD Contínua. 2018. **Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal 2018**. Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101705_informativo.pdf>. Acesso Março de 2021.

BRITO, A. **Direito Penal Informático**. São Paulo: Saraiva, 2013.

CANÁRIO, Pedro. Brasil precisa de lei sobre proteção de dados pessoais, diz Villas-Bôas Cueva. **Consultor Jurídico**. 15 de agosto de 2017. https://www.conjur.com.br/2017-ago-15/brasil-lei-protecao-dados-pessoais-cueva. Acesso Maio de 2022.

CAPELLA, Arthur. **Risco cibernético exige a cooperação dos setores público e privado**. 09 de Março de 2022. https://canaltech.com.br/seguranca/risco-cibernetico-exige-a-cooperacao-dos-setores-publico-e-privado/ acesso Maio de 2022.

CARVALHO, A. C. A. P. **Marco Civil da Internet no Brasil**. São Paulo: Alta Books, 2014.

CASTELLS, Manuel. **A sociedade em rede**. v.1. 5. ed. São Paulo: Paz e Terra, 2001. in A era da informação: Economia, sociedade e cultura.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Trad. Maria Luiza X. de A. Borges. Revisão Paulo Vaz. Rio de Janeiro: Zahar, 2003.

CASTELLS, M. **A Sociedade em Rede**: Economia, Sociedade e Cultura. 6. ed. São Paulo: Paz e Terra, 2013. v.1.

CATALA, Pierre. **Ebauche d'une théorie juridique de l'information**, in: Informatica e Diritto, ano IX, jan-apr. 1983.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Incidentes Reportados ao CERT.br** — Janeiro a Junho de 2020, 09 de setembro de 2020.

Disponível em: <https://www.cert.br/stats/incidentes/2020-jan-jun/total.html>. Acesso em: 20 de junho de 2020.

CENTRO DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO - CTIR GOV em Números. **Incidentes.** 11 de março de 2021. Disponível em: <https://emnumeros.ctir.gov.br/incidentes/>. Acesso em: 24 de março de 2021.

CHRISTENSEN, Clayton M. **O Dilema da Inovação:** quando as novas tecnologias levam empresas ao fracasso. São Paulo: M. Books, 1997.

CHRISTENSEN, Clayton M; RAYNOR, Michael E.; MCDONALD, Rory. **What is Disruptive Innovation?** 2015. <https://hbr.org/2015/12/what-is-disruptive-innovation>. Acesso Jul. 2018.

COE, **The Budapest Convention on Cybercrime**: benefits and impact in practic*e*. Council of Europe: Strasbourg. 2020, esp.p.5. Disponível em: <https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac>.

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

DA SILVEIRA, Sergio Amadeu. Tudo sobre tod@s: Redes digitais, privacidade e venda de dados pessoais. Edições Sesc, 2017.

DE JESUS, D. D. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

DENNING, Dorothy E. **The Ethics of Cyber Conflict**. In: HIMMA, Kenneth Einar; TAVANI, Herman T. The Handbook of Information and Computer Ethics. Hoboken, New Jersey: Wiley, 2008. Disponível em: < http://www.cems.uwe.ac.uk/~pchatter/2011/pepi/The_Handbook_of_Information_and_Computer_Ethics.pdf>. Acesso em: 03 jul. 2020.

DENNING, Dorothy E.; STRAWSER, Bradley J. **Active cyber defence**: applying air defence to the cyber domain. Carnegie Endowment for International Peace, 2017. Disponível em: <https://carnegieendowment.org/2017/10/16/active-cyber-defence-applying-air-defence-to-cyber-domain-pub-73416>. Acesso em: 20 jul. 2020.

DILLING, O. **Proactive Compliance?** Repercussions of National Regulation in Standards of Transnational Business Networks. In Dilling, O; Herberg, M; Winter, G. (eds.). Responsible Business. Self-Governance and Law in Transnational Economic Transactions, Oxford, Hart Publishing, 2008, p. 96-98.

DOCUMENTOS DA CÚPULA MUNDIAL SOBRE A SOCIEDADE DA INFORMAÇÃO [livro eletrônico]: Genebra 2003 e Túnis 2005 /International Telecommunication Union ;[traduzido por Marcelo Amorim Guimarães]. --São Paulo: Comitê Gestor da Internet no Brasil, 2014.1,42 Mb ; PDF Título original: World Summit on the Information Society, Geneva 2003-Tunis 2005ISBN 978-85-60062-88-1. https://www.cgi.br/media/docs/publicacoes/1/CadernosCGIbr_DocumentosCMSI.pdf. Acesso Junho 2022.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Revista dos Tribunais, 2020.

DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia / Escola Nacional de Defesa do Consumidor; elaboração Danilo Doneda. – Brasília: SDE/DPDC, 2010. Disponível em https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf, acesso Março 2021.

EUROPEAN PARLIAMENT 2014-2019. DRAFT REPORT with recommendations to the Commission on **Civil Law Rules on Robotics** (2015/2103 (INL). Committee on Legal Affairs. 31.5.2016. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-582.443+01+DOC+PDF+V0//EN&language=EN. Acesso Jul. 2018.

FERRAZ JÚNIOR, T. S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista Da Faculdade De Direito, Universidade de São Paulo**, 88, 439-459, 1993. Recuperado de https://www.revistas.usp.br/rfdusp/article/view/67231. Acesso Junho 2022.

FERREIRA, Ivette Senise. A criminalidade informática. In: Newton De Lucca; Adalberto Simão Filho (Coord.). **Direito e Internet** - aspectos juridicos relevantes. 2ª ed. São Paulo, Quartier Latin, 2005.

FIGUEIREDO, Jorge Dias. **Direito Penal: Parte Geral:** Tomo I: questões fundamentais: a doutrina geral do crime**.** 1ª ed. São Paulo: Editora Revista dos Tribunais, 2007.

FRAZÃO, Ana, OLIVA, Milena D. e ABÍLIO, Vivianne da S. Compliance de dados pessoais in **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Revista dos Tribunais, 2019.

FULLER, Greice Patrícia; SOARES, Roger da Silva Moreira. A tutela penal dos dados empresariais na sociedade da informação do ordenamento jurídico brasileiro. **Revista Jurídica da Presidência** [recurso eletrônico]. Brasília, v.20, n.121, jun./set. 2018.

HOFFMANN-RIEM, Wolfgang. Autorregulação, Autorregulamentação e Autorregulamentação Regulamentada no contexto digital. **Revista da AJURIS**. Porto Alegre, v. 46, n. 146, Junho, 2019. http://ajuris.kinghost.net/OJS2/index.php/REVAJURIS/article/view/1048. Acesso Out. 2020.

HOFFMANN-RIEM, Wolfgang. Controle do comportamento por meio de algoritmos: um desafio para o Direito. **Direito Público**, [S.l.], v. 16, dez. 2019. https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3647. Acesso Out. 2020.

HOSTERT, Ana Cláudia et al. **Proteção de dados pessoais na internet:** a necessidade de lei específica no ordenamento jurídico brasileiro. 2018. Dissertação de Mestrado. Florianópolis, SC.

HUREL, Louise Marie. **Cibernética no Brasil: uma análise da estratégia nacional.** INSTITUTO IGARAPÉ. Abril de 2021. https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf. Acesso Maio de 2022.

HUREL, Louise Marie; LOBATO, Luisa Cruz. **Uma Estratégia para a Governança da Segurança Cibernética no Brasil.** INSTITUTO IGARAPÉ. Setembro de 2018. https://igarape.org.br/wp-content/uploads/2018/09/Uma-estrate%CC%81gia-para-a-governanc%CC%A7a-da-seguranc%CC%A7a-ciberne%CC%81tica-no-Brasil.pdf. Acesso Maio de 2022.

IMINES, Martha. **País tem aumento de crimes virtuais durante a pandemia**. O Dia, 06 de setembro de 2020. Disponível em: <https://odia.ig.com.br/economia/2020/09/5982325-alerta-de-crimes-ciberneticos.html>. Acesso em: 10 de outubro de 2020.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. IBGC. **Papéis e responsabilidades do Conselho na gestão de riscos cibernéticos**. Instituto Brasileiro de Governança Corporativa. - São Paulo, SP: IBGC Orienta, 2019.

INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS. **Cyber Security in Securities Markets** – An International Perspective Report on IOSCO's cyber risk coordination efforts, 2016.

JAQUET-CHIFFELLE, DO., LOI, M. Hacking ético e antiético. In: Christen, M., Gordijn, B., Loi, M. (eds) A Ética da Cibersegurança. A Biblioteca Internacional de Ética, Direito e Tecnologia, vol 21, 2020. Springer, Cham. https://doi.org/10.1007/978-3-030-29053-5_9. AcessoJunho 2022.

KADOW, André; CAMARGO, Carlos. Internet das Coisas: Vulnerabilidade, Privacidade e Pontos de Segurança. **Revista Competência**, v. 9, n. 1, p. 153-161, 2016.

KUNEVA, Meglena**. Personal data is the new oil of the Internet and the new currency of the digital world.** Discurso proferido na mesa redonda sobre coleta de dados, direcionamento e perfilação. Bruxelas, 31 de março de 2009.

LOURENÇO, Gabriel D. **Cibercrimes no Brasil crescem em 23% em 2021, aponta pesquisa**. Olhar Digital, 31 de agosto de 2021. Disponível em: <https://olhardigital.com.br/2021/08/31/seguranca/cibercrime-brasil-2021/>. Acesso Out. 2021.

MOLINARO, Carlos Alberto; SARLET, Ingo Wolfgang. Direito à informação e direito de acesso à informação como direitos fundamentais na constituição brasileira. Revista da AGU Brasília-DF, ano XIII, n. 42, p. 09-38, out./dez., 2014.

NEVES, Marcelo. **Transconstitucionalismo**. São Paulo: Martins Fontes, 2009.

PINHEIRO, P. Peck. **Direito digital**. 6. ed. São Paulo:Saraiva, 2015.

PINHEIRO, P. Peck. **Direito Digital Aplicado 4.0**. Revista dos Tribunais, 2021.

POLEGATTI, B. C.; KAZMIERCZAK, L. F. **Crimes Cibernéticos:** O Desafio do Direito Penal na Era Digital. Ourinhos, 2012.

POLIDO, Fabricio Bertini Pasquot. Por que o Brasil deve urgentemente aderir à Convenção de Budapeste. **Consultor Jurídico**. 5 de julho de 2021. https://www.conjur.com.br/2021-jul-05/polido-brasil-urgentemente-aderir-convencao-budapeste.

PORTAL DE NOTÍCIAS UOL. Brasil é o segundo país no mundo com maior número de crimes cibernéticos. 15 de fevereiro de 2018. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm#:~:text=Brasil%20%C3%A9%20o%20segundo%20pa%C3%ADs%20no%20mundo%20com%20maior%20n%C3%BAmero%20de%20crimes%20cibern%C3%A9ticos,-Pesquisa%20indica%20que&text=De%20acordo%20com%20um%20relat%C3%B3rio,preju%C3%ADzo%20de%20US%24%2022%20bilh%C3%B5es.>. Acesso em: 24 de março de 2021.

PORTO ALEGRE, Gabriela. **Ocorrências crescem 110% de 2017 para 2018**. Jornal do Comércio, 15 de outubro de 2019. Disponível em: <https://www.jornaldocomercio.com/_conteudo/cadernos/jornal_da_lei/2019/10/706706-ocorrencias-crescem-110-de-2017-para-2018.html>. Acesso Out. 2020.

RODOTÀ, Stefano. **Tecnologie e Diritti**. Bolonha: Il Mulino, 1995.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. *In:* MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 21-60.

SARLET, Ingo Wolfgang . Precisamos da previsão de um direito fundamental à proteção de dados no texto da CF? **Consultor Jurídico**. 2020. Disponível em: https://www.conjur.com.br/2020-set-04/direitos-fundamentais-precisamos-previsao-direito-fundamental-protecao-dados-cf. Acesso Maio de 2022.

SCHEPEL, H. The Constitution of Private Governance. Product Standards of Integrating Markets, Oxford, Hart Publishing, 101-176, 2005.

SCHWAB, Klaus. The Fourth Industrial Revolution: What It Means and How to Respond. *Foreign Affairs***,** Dez. 2015. <https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution>. Acesso Jul. 2018.

SCHWAB, Klaus. **A Quarta revolução industrial**. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SHIRLEY, Robert Weaver. **Antropologia Jurídica**. São Paulo: Saraiva, 1987.

SMANIO, Gianpaolo Poggio. **Tutela Penal dos Interesses Difusos**. São Paulo: Atlas, 2000.

SMITH, Brad; SHUM, Harry. **The Future Computed**: Artificial Intelligence and its role in society, 17, Janeiro 2018.

SYDOW, S. T. COL. **Saberes monográficos**: crimes informáticos e suas vítimas. 2. ed. São Paulo, Saraiva, 2015.

TAYLOR, C. **A Secular Age**. Harvard University Press, 2007.

TEIXEIRA, T. **Curso de direito e processo eletrônico**. 4. ed. São Paulo, Saraiva, 2018.

WORLD ECONOMIC FORUM. **The Global Risks Report 2019**. Disponível em: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf. Acesso Março 2021.

WORLD ECONOMIC FORUM. **The Global Risks Report 2020.** Disponível em https://www.weforum.org/reports/the-global-risks-report-2020/ Acesso Junho 2022.

WORLD ECONOMIC FORUM. **The Global Risks Report 2021.** Disponível em https://www.weforum.org/reports/the-global-risks-report-2021/ Acesso Maio 2022.

WORLD ECONOMIC FORUM. **The Global Risks Report 2022** 17th Edition. Disponível em https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf. Acesso Maio 2022.

XAVIER, M. **Crimes digitais**. São Paulo, Saraiva, 2011.

ZANATTA, RAFAEL. **Proteção de dados pessoais como regulação de risco:** uma nova moldura teórica? in: I Encontro da Rede de Pesquisa e Governança da Internet. Rio de Janeiro, 14 de novembro de 2017.

http://www.redegovernanca.net.br/public/conferences/1/anais/ZANATTA,%20Rafael_2017.pdf. Acesso em Set. 2020.

[i] https://www.nossosaopaulo.com.br/Reg_SP/Barra_Escolha/ONU_SociedadeDaInformacao.htm. Acesso em Maio de 2022.

[ii] Protecção de dados pessoais. 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

[iii] Esta é a base da definição presente tanto no Art. 2 da Convenção n. 108 do Conselho da Europa para a proteção dos indivíduos em relação ao processamento automatizado de dados pessoais, como no Art. 1 das Linhas-Guia da OCDE sobre proteção da privacidade e fluxos transfronteiriços de dados pessoais ("personal data" means any information relating to an identified or identifiable individual ('data subject')"). Esta base foi assimilada pela Diretiva Europeia 95/46/CE em seu Art. 2º, que define como "'Dados pessoais "qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); (...)". Tal disposição encontra-se incorporada nas várias normativas europeias sobre o tema, por exemplo no Art. 3º da Lei da Proteção de dados (Lei nº 67/98) de Portugal ou no § 3 (1) da Lei Federal de Proteção de Dados da Alemanha.

[iv]https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/noticias/conheca-as-propostas-do-relatorio-final-da-cpiciber

[v] https://www.weforum.org/reports/global-risks-report-2022/in-full/chapter-3-digital-dependencies-and-cyber-vulnerabilities#chapter-3-digital-dependencies-and-cyber-vulnerabilities; https://blog.idwall.co/ameacas-ciberneticas-riscos-globais/ acesso em Maio de 2022.

[vi] https://www.weforum.org/reports/global-risks-report-2022/in-full/chapter-3-digital-dependencies-and-cyber-vulnerabilities#chapter-3-digital-dependencies-and-cyber-vulnerabilities;
https://www.weforum.org/reports/global-risks-report-2022. Acesso Maio de 2022.

[vii] ataque com vírus malware aumentou 358% em 2020, enquanto o ransomware subiu para 435% no mesmo ano. Com o advento do vírus malware, uma das tendências nos crimes cibernéticos é o Ransomware como serviço (Ransomware as a service, em inglês). Essa modalidade visa comercializar o ransomware para ter acesso à rede, sistema ou plataforma da empresa, roubando ou bloqueando o acesso aos dados e, depois, solicita um valor em criptomoedas para que tudo seja devolvido ou liberado.

[viii]https://inforchannel.com.br/2020/01/24/novos-principios-de-seguranca-da-internet-desenvolvidos-com-o-forum-economico-mundial/ acesso Maio de 2022.

[ix]https://inforchannel.com.br/2020/01/24/novos-principios-de-seguranca-da-internet-desenvolvidos-com-o-forum-economico-mundial/ acesso Maio de 2022.

[x]https://inforchannel.com.br/2020/01/24/novos-principios-de-seguranca-da-internet-desenvolvidos-com-o-forum-economico-mundial/ acesso Maio de 2022.

[xi]https://inforchannel.com.br/2020/01/24/novos-principios-de-seguranca-da-internet-desenvolvidos-com-o-forum-economico-mundial/ acesso Maio de 2022.

[xii] Segundo Ulrich Beck, "a sociedade de risco designa uma época em que os aspectos negativos do progresso determinam cada vez mais a natureza das controvérsias que animam a sociedade".

[xiii] Esta Norma fornece diretrizes para melhorar o estado de Segurança Cibernética, traçando os aspectos típicos desta atividade e suas ramificações em outros domínios de segurança.

[xiv] Segurança da Informação, de acordo com a norma ISO 27001, relaciona-se à uma abordagem abrangente, independente do meio em que são armazenados ou transmitidos os dados, dizendo respeito à preservação da confidencialidade, integridade e disponibilidade das informações no Espaço Cibernético (PINHEIRO, 2021).

[xv] Crackers, sejam eles black hats ou grey hats, representam os hackers responsáveis pelas invasões maliciosas e quebra de sistemas, isto é, são considerados os reais criminosos do meio-ambiente virtual (CRESPO, 2011).

[xvi] Também conhecidos como hackers éticos, os Ethical Hackers são especialistas em segurança e em estratégias de hacking, mas com a missão de defender as organizações.

[xvii] No inglês: "[...] a form of active response that uses hacking to counter a cyber attack. There are two principal forms. The first involves using invasive tracebacks in order to locate the source of an attack. The second involves striking back at an attacking machine in order to shut it down or at least cause it to stop attacking".

[xviii] https://www.cgi.br/media/docs/publicacoes/1/CadernosCGIbr_DocumentosCMSI.pdf. Acesso Maio de 2022.

[xix] A governança na área cibernética está relacionada às ações, aos mecanismos e às medidas a serem adotados

com o fim de simplificar e modernizar a gestão dos recursos humanos, financeiros e materiais, e acompanhar o desempenho e avaliar os resultados dos esforços empreendidos nesse campo. Essa governança visa incorporar elevados padrões de conduta em segurança cibernética, e orientar as ações de agentes públicos e de agentes privados, ao considerar o papel que exercem em suas organizações, conforme a finalidade e a natureza de seu negócio. Inclui, ainda, o planejamento voltado à execução de programas, de projetos e de processos, e o estabelecimento de diretrizes que irão nortear a gestão de riscos. Nesse contexto, orienta pessoas e organizações quanto à observância das normas, dos requisitos e dos procedimentos existentes em segurança cibernética.

[xx] Tratado internacional sobre direito penal e processual penalque objetiva promover a cooperação entre os países no combate aos crimes praticados por meio da Internet e com o uso de computadores. A Convenção de Budapeste é complementada por um Protocolo sobre Xenofobia e Racismo cometidos por meio de sistemas de computador.

[xxi] "Hoje, 92 membros das Nações já contam com regras vigentes e consistentes com os artigos 16 a 21 da Convenção de Budapeste, que estabelecem poderes processuais às autoridades de aplicação das leis para preservação e proteção das provas digitais (*e-evidences*)" (POLIDO, 2021). Polido aduz em conformidade com o Relatório COE (jul 2020), do Escritório do Programa de Crimes Cibernéticos do Conselho da Europa, que "Alguns indicadores são relevantes em temas de cooperação para acesso transfronteiriço a dados. Em fevereiro de 2020, cerca de 177 países (92%) estavam em processo de reformar suas legislações internas, ou o fizeram nos últimos anos em matéria penal para se ajustar às demandas digitais e novas tecnologias. As partes não apenas se basearam na Convenção de Budapeste quando reformaram suas legislações internas, mas também cerca de 153 (79%) dos membros da Organização das Nações Unidas se utilizaram dos dispositivos do tratado como guia ou uma fonte de inspiração para basear suas reformas legislativas domésticas. Por fim, cerca de 106 (55%) países da ONU já tem adotado normas, em seus direitos internos, equivalentes aos dispositivos da Convenção de Budapeste. Um terço de países adotou, ao menos, algumas regras específicas de Direito Penal segundo a convenção, incrementando seus sistemas jurídicos domésticos." (COE, 2020). Veja ainda https://www.conjur.com.br/2021-jul-05/polido-brasil-urgentemente-aderir-convencao-budapeste.

Sobre os autore:

Loreci Gottschalk Nolasco
Doutora em Biotecnologia e Biodiversidade (2016) pela Universidade Federal de Goiás. Mestre em Direito pela Universidade de Brasília (2002). Docente do Programa de Pós Graduação lato sensu em Direitos Difusos e Coletivos e da Graduação em Direito da Universidade Estadual de Mato Grosso do Sul. Coordenadora do Projeto de Pesquisa: O DIREITO NA SOCIEDADE DIGITAL – estudos sobre "disrupção tecnológica" e "interrupção regulatória". Coordenadora Pedagógica do Projeto de Extensão Empresa Júnior do Curso de Direito da UEMS.
Lattes: http://lattes.cnpq.br/8817250711332244 ORCID: https://orcid.org/0000-0002-5867-6412
E-mail: lorecign@gmail.com

Bruno Dutra Maciel Silva
Pesquisador no Programa de Iniciação Científica da Universidade Estadual de Mato Grosso do Sul.
Estudante do Curso de Direito da Universidade Estadual de Mato Grosso do Sul.
Lattes: http://lattes.cnpq.br/7511216231962585
E-mail: bruno16dutra@gmail.com

Os autores contribuíram igualmente para a redação do artigo.