YHASMIN MARTINS DE OLIVEIRA

Novas tecnologias de defesa cibernética na proteção da propriedade intelectual sob uma visão jurídica.

Brasília-DF
2023

YHASMIN MARTINS DE OLIVEIRA

Novas tecnologias de defesa cibernética na proteção da propriedade intelectual sob uma visão jurídica.

Trabalho de Conclusão de Curso apresentado como requisito parcial para defesa e obtenção do título de Mestre em Propriedade Intelectual e Transferência de Tecnologia para Inovação, do Programa de Pós-Graduação em Propriedade Intelectual e Transferência de Tecnologia para Inovação (PROFNIT) – Ponto Focal Universidade de Brasília.

Orientadora: Drª. Leila Bijos

Brasília-DF
2023

YHASMIN MARTINS DE OLIVEIRA

Uma visão jurídica sobre a defesa cibernética na defesa da propriedade intelectual.

Trabalho de Conclusão de Curso apresentado como requisito parcial para defesa e obtenção do título de Mestre em Propriedade Intelectual e Transferência de Tecnologia para Inovação, do Programa de Pós-Graduação em Propriedade Intelectual e Transferência de Tecnologia para Inovação (PROFNIT) – Ponto Focal Universidade de Brasília.

Aprovada em:

BANCA EXAMINADORA

_____
Profª. Drª. Leila Bijos

_____
Profª. Drª. Maria Hosana Conceição

_____
Profª. Drª. Alecsandra Oliveira de Souza

_____
Prof. Dr. Danilo Porfírio de Castro Vieira

FICHA CATALOGRÁFICA

Oliveira, Yhasmin Martins de,
Uma visão jurídica sobre a defesa cibernética na defesa da propriedade intelectual
Yhasmin Martins de Oliveira
Orientadora:
Leila Bijos – Brasília, 2023.
70 p.
Trabalho de Conclusão de Curso.
PROFNIT Universidade de Brasília.
Curso de Mestrado em Propriedade Intelectual e Transferência de Tecnologia para a Inovação.

1. Cibersegurança; Ameaça; Propriedade Intelectual

AGRADECIMENTOS

A todos que à sua maneira contribuíram nesta jornada.

RESUMO

O ciberespaço apresenta-se como uma plataforma sem fronteiras que permite a livre interação entre pessoas para os mais diversos fins. Por outro lado, desta abertura surgem possíveis ataques de matriz tecnológica que colocam em risco pessoas físicas, instituições e suas respectivas produções intelectuais. Deste modo, para que se possa continuar a usufruir os benefícios que este espaço proporciona, impõe-se a necessidade de criar estruturas nacionais e internacionais, públicas e privadas, de monitorização e de prevenção de práticas que ameacem os direitos. Este trabalho, portanto, teve como objetivo analisar as condições de cibersegurança no Brasil a partir dos cenários econômico, social, político e tecnológico da segurança cibernética, identificando as medidas normativas que têm sido tomadas e as eventuais lacunas por elas deixadas para então propor um modelo, a partir de um manual, visando a conscientização e o aprimoramento do ambiente cibernético. Para a realização da pesquisa foi utilizado o método dedutivo, de procedimento qualitativo e meio de informação bibliográfica com consultas ao Google Acadêmico, Periódicos CAPES, Dialnet, portais governamentais e similares. Assim, reforçou-se a relevância do trabalho como estratégia para a promoção de um ambiente de inovação mais seguro e confiável. Como produto tecnológico foi elaborado um Manual de Boas Práticas em Segurança Cibernética com o objetivo de garantir a integridade da propriedade intelectual nos meios digitais.

Palavras-Chave: Cibersegurança; Ameaça; Propriedade Intelectual.

ABSTRACT

Cyberspace presents itself as a platform without borders that allows free interaction between people for the most diverse purposes. Through this opening arise possible attacks of technological matrix that put at risk individuals, institutions, and their respective intellectual productions. Thus, in order to continue to enjoy the benefits that this space provides, it is necessary to create national and international structures, public and private, for monitoring and preventing practices that threaten rights. This work, therefore, aimed to analyse the conditions of cybersecurity in Brazil from the economic, social, political, and technological scenarios of cybersecurity, identifying the normative measures that have been taken and the possible gaps left by them to then propose a model, from a manual, aiming at the awareness and improvement of the cyber environment. To carry out the research, the deductive method, qualitative procedure and means of bibliographic information were used with queries to Google Academic, CAPES Journals, Dialnet, government portals and the like. Thus, the relevance of the work was reinforced as a strategy for the promotion of a safer and more reliable innovation environment. As a technological product, a Manual of Good Practices in Cybersecurity was prepared with the objective of ensuring the integrity of intellectual property in digital media.

Keywords: Cybersecurity; Threat; Intellectual Property

SUMÁRIO

1. APRESENTAÇÃO

Ao longo das últimas décadas, a tecnologia vem atravessando o cotidiano das pessoas e tornando-se uma ferramenta indispensável se fazendo presente de forma ativa no mundo. Contudo, junto às facilidades trazidas por esse recurso, vieram também ameaças. No sentido de identificar e melhor tutelar as necessidades daqueles que diariamente fazem uso deste mecanismo, foi preciso construir pontes e estabelecer diálogos entre os mais variados campos do saber para, então, compreender, ou aproximar-se de, a magnitude do alcance da tecnologia e seus riscos.

É sob esta influência e utilizando-se mais uma vez da multidisciplinaridade, da integração entre os campos do saber e da experiência multifacetada promovida pelo ambiente do PROFNIT, que este trabalho busca integrar o campo do Direito ao estudo da tecnologia para abordar de forma integrada e dinâmica as ameaças cibernéticas que fazem parte da atual realidade conectada.

Dentro desse contexto, o ano de 2020 trouxe consigo uma mudança brutal no cotidiano das pessoas. A quarentena em virtude da pandemia da Covid-19 acelerou o processo de transformação do mercado de trabalho que até então era predominantemente presencial, para o modelo remoto.

Nesse contexto, empresas e órgãos públicos viram seus custos com gastos triviais como luz, água, alimentação e afins diminuírem, mas por outro lado, em virtude do teletrabalho, esses mesmos agentes tiveram seus sistemas expostos a riscos em razão da falta de treinamento dos empregados e servidores para atuarem na modalidade remota, e também pela falta de estrutura das próprias empresas, órgãos e afins, para comportar a transmissão segura de dados para dispositivos externos.

Com o alto tráfego fora de uma rede programada de proteção, os ataques cibernéticos ganharam ainda mais espaço e começaram a se tornar recorrentes no cotidiano de empresas, órgãos e afins. Apesar disso, identifica-se no mercado a propensão pela adoção de um modelo híbrido de trabalho e, para algumas funções, até mesmo integralmente em modalidade remota.

Dessa forma, de acordo com pesquisa realizada pela Marsh com foco na América Latina, embora 31% das empresas tenham percebido o aumento de ataques cibernéticos desde o início da pandemia da Covid-19, apenas 24% investiram em segurança cibernética, preferindo realocar os lucros obtidos a partir da economia com

infraestrutura e suporte físico em outras áreas (CRYPTOID, 2021). O *Federal Bureau of Investigation* (FBI) ou Departamento Federal de Investigação dos Estados Unidos, também reportou um aumento de 400% nas denúncias relacionadas à segurança cibernética e, entre fevereiro e maio de 2020, mais de meio milhão de usuários de plataforma de videoconferência tiveram seus dados pessoais roubados e comercializados na *dark web* (CRYPTOID, 2021).

Empresas internacionalmente reconhecidas e consolidadas no mercado como Hyundai, Google, Sony, Credicard, entre outras, também tiveram que lidar com ataques de ordem cibernética (CORTEZ; KUBOTA, 2013), e no Brasil, mais recentemente foi possível acompanhar o ataque por *ransomware* à rede de lojas Renner.

Mas os atentados à segurança cibernética atingiram não só empresas do setor privado, como também agentes e estruturas integrantes dos poderes do Estado, à exemplo do ataque sofrido pelo Superior Tribunal de Justiça em 4 de novembro de 2020 (STJ, 2020), ocasião em que ministros e servidores ficaram sem acesso a seus próprios arquivos e *e-mails*; e poucos meses depois, em maio de 2021, a invasão aos arquivos do Supremo Tribunal Federal que fez com que o site da Corte ficasse indisponível por dias para usuários externos como forma de evitar o vazamento de dados (AGÊNCIA BRASIL, 2021).

Percebe-se, portanto, que a problemática da segurança cibernética atravessa todas as camadas da sociedade, seja pública, seja privada. Assim, nada mais lógico que Estado e iniciativa privada trabalharem juntos na identificação de gargalos e na busca por soluções, cabendo ao Estado, no desempenho das suas funções, incentivar a adoção de medidas protetivas, apoiar a capacitação de mão-de-obra e proteger o ambiente virtual e a integridade das informações nele compartilhadas.

Nesse caminho, a implementação de políticas públicas que visem concretizar esse diálogo entre os diversos setores da sociedade assume papel fundamental na proteção das empresas e, reflexamente, de toda a comunidade. Para isso, a propagação de informações a empreendedores e o incentivo através de investimentos, leis, manuais de boas práticas e demais instrumentos norteadores, tende a impactar positivamente o cenário.

Neste momento em que o debate se abre e a visibilidade do assunto cresce, é fundamental que aqueles à frente do ambiente de inovação se debrucem sobre o

assunto para encontrar soluções que harmonizem o avanço tecnológico com as garantias de que gozam indivíduos, empresas e órgãos públicos.

2. INTRODUÇÃO

A presente pesquisa se dedicou a traçar um referencial teórico da cibersegurança e da sua interrelação com a propriedade intelectual. Para tanto, o ponto de partida foi o próprio conceito do que é o ciberespaço.

A partir deste ponto, foram abordadas as principais modalidades de ataques cibernéticos praticados nos dias atuais, afim não apenas de acompanhar uma sequência lógica da própria pesquisa, mas também de informar o leitor a respeito dos riscos inseridos no cotidiano *on-line*.

Com esta base de conhecimento formada, passou-se então ao apanhado legislativo do Brasil e demais países, isto é, quais respostas o desafio da segurança cibernética tem gerado por parte de nações. A análise deste arcabouço jurídico permitiu acompanhar a evolução do assunto e a sua inserção nas agendas políticas dos países, além de auxiliar na identificação de qual caminho se está a percorrer e quais os próximos passos devem ser dados rumo a uma tutela cada vez mais eficiente e adaptada à realidade contemporânea.

Neste ponto, tornou-se inevitável abordar as questões éticas envolvidas na cibersegurança, uma vez que são múltiplos atores e consequentemente interesses, concorrendo no mesmo ambiente. Como construir uma cultura de cibersegurança que não viole nenhum direito nem torne excessivamente vulnerável uma das partes?

Partiu-se, então, para a análise da interseção entre o universo da cibersegurança com o universo da propriedade intelectual e como essa relação impacta diretamente a economia e o próprio estímulo à inovação, posto tratar-se de campo onde o sigilo é um grande aliado.

Por fim, abordou-se a questão da responsabilidade civil pelas violações que atingem diretamente a tutela da propriedade intelectual, isto é, as vias de reparação às quais o lesado pode recorrer caso seja vítima de um crime cibernético.

3. JUSTIFICATIVA

3.1 LACUNA A SER PREENCHIDA PELO TCC

Estima-se que em 2021, os danos causados pelo cibercrime alcançaram a alarmante quantia de seis trilhões de dólares (CYBERSECURITY VENTURES, 2020), montante que o aproxima de economias como a dos Estados Unidos da América e da China.

Com a revolução tecnológica e cibernética, o mundo foi presenteado com uma plataforma extremamente eficiente que permitiu a conexão entre países, povos, culturas e informações, o ciberespaço (onde se encontra assentada a internet, responsável pelo maior volume de transmissão de informações). A partir daí, nasceu uma relação de interdependência entre essa matriz que se sustenta através de dados (matriz aqui compreendida como a representação desses dados) e as pessoas, públicas e privadas, que fornecem os dados para que este universo siga se aprimorando e facilitando suas atividades.

Contudo, o nível de vulnerabilidade que acompanha essa facilitação representa uma ameaça constante à segurança dos dados que diariamente são disponibilizados de forma voluntária por quem os possui. Assim, práticas corriqueiras como utilizar o banco *on-line*, mandar um documento por *e-mail*, acessar a *intranet* da empresa entre outras, tornam-se alvo do cibercrime e podem causar prejuízos que vão desde a perda e restauração de dados armazenados, até “sequestros” de informações, desfalques, interrupção de prestação de serviços, danos à reputação, espionagem industrial e roubos de propriedade intelectual, área em que se concentrará o presente trabalho.

Assim, faz-se mister notar a importância da criação e implementação prática de uma cultura de cibersegurança não só pelos indivíduos em seus dispositivos pessoais, mas também por corporações que pretendem (e precisam) atuar no ambiente informatizado para se comunicarem, crescerem e permanecerem no mercado.

Para auxiliar o alcance de tal finalidade e, ativamente, contribuir para o fechamento da lacuna promovida pelos crimes cibernéticos, para além deste TCC, será entregue também um manual de boas práticas em cibersegurança, voltado para pessoas físicas e jurídicas.

3.2 ADERÊNCIA AO PROFNIT

O presente trabalho procurou alinhar, portanto, os conceitos e práticas de cibersegurança à proteção da propriedade intelectual, de modo a estabelecer

parâmetros de atuação para que a integridade das criações intelectuais seja mantida e o setor possa usufruir dos impactos positivos de um alto grau de confiabilidade.

3.3 IMPACTO

De acordo com o Confederação Nacional da Indústria (CNI, 2016), a criação de padrões de cibersegurança está entre os desafios a serem enfrentados pelas indústrias. O pouco investimento que ainda existe por parte de empresas gera um ambiente exposto e propício à ataques e, embora haja um reconhecimento por parte de empresários e gestores da necessidade de investimentos no campo, a concretização desse planejamento ainda não atingiu níveis satisfatórios.

Para lidar com esses desafios e transpor essas barreiras, é indispensável que seja estimulada a conscientização e criados padrões de cibersegurança através de legislação, regulamentos e regras de governança de tecnologia e informação para que se estabeleça uma conduta uniforme e equânime que vise não apenas punir o ato, mas principalmente evitá-lo.

Para isso, a atuação multissetorial mostra-se de grande valia e vem sendo aplicada por diversas organizações, à exemplo do Departamento de Segurança da Informação e Comunicações (DSIC) em nível nacional, e da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que em nível internacional emprega esforços para estabelecer políticas de segurança cibernética em seus países membros a partir da ação conjunta de cinco atores: o setor público, o setor privado, o terceiro setor, as instituições de ensino superior e a sociedade (OPPERMANN, 2014).

Foi com o intuito de contribuir com a construção dessa estrutura de apoio que este trabalho foi construído.

3.4 APLICABILIDADE

A aplicabilidade da produção técnica que se realizou guarda escopo em três momentos: abrangência realizada, abrangência potencial e replicabilidade.

No que tange a abrangência realizada, o manual foi o produto final da dissertação aplicada no PROFNIT/UnB.

Por sua vez, na abrangência potencial, a produção técnica aqui retratada detém capacidade de entregar um material capaz de, de forma acessível e direta, educar e direcionar as ações dos atores envolvidos na produção de propriedade intelectual para

práticas mais alinhadas com os parâmetros de segurança adotados atualmente, levando em consideração diretrizes internas e externas.

Em nível de replicabilidade, acredita-se tratar-se de produção de fácil disseminação e acesso.

3.5 INOVAÇÃO

O grau de inovação do presente trabalho caracteriza-se como produção de médio teor inovativo, posto que combina conhecimentos pré-estabelecidos, a saber: o panorama contemporâneo de segurança cibernética; no que consistem o ciberespaço e a cibersegurança; o impacto e as modalidades desses ataques sobre os ativos de propriedade intelectual; os instrumentos disponíveis para combate e repressão à tais práticas, tanto em nível interno (Política Nacional de Inteligência, Lei Geral de Proteção de Dados, Estratégia Nacional de Segurança Cibernética), quanto em nível externo (Acordo de Budapeste, Diretiva Sobre Segurança das Redes e da Informação, nova estratégia da União Europeia para a cibersegurança) para, a partir desta curadoria, elaborar um manual capaz de fornecer orientação para boas práticas de segurança cibernética.

3.6 COMPLEXIDADE

No tocante à complexidade, a elaboração do referido trabalho classifica-se como uma produção de baixa complexidade, uma vez que resulta de desenvolvimento baseado em adaptação de conhecimento já existente e estabelecido sem, necessariamente, a participação ativa de diferentes atores, embora a eles dirigido.

4. OBJETIVOS

4.1 OBJETIVO GERAL

A partir do cenário atual e da busca em bases de dados, analisar as condições da segurança cibernética no Brasil para, posteriormente, por meio da criação de um manual, contribuir para a divulgação e promoção de um ambiente cibernético mais seguro.

4.2 OBJETIVOS ESPECÍFICOS

4.2.1 Objetivo específico 1

Avaliar os dados da segurança cibernética no Brasil e o impacto econômico, social, político e tecnológico do cibercrime para contextualizar o assunto;

4.2.2 Objetivo específico 2

Identificar as medidas regulatórias que têm sido adotadas no combate e repressão ao cibercrime e suas lacunas para assim detectar o que pode ser melhorado;

4.2.3 Objetivo específico 3

Propor um modelo, a partir de um manual, inspirado nas medidas para segurança cibernética, para aprimoramento, adaptação e desenvolvimento de mecanismos para a promoção de um ambiente cibernético mais seguro.

5. REFERENCIAL TEÓRICO

5.1 O CIBERESPAÇO

O termo “*cyberspace*” (em português, “ciberespaço”), palco das preocupações que serão abordadas no presente trabalho, nasceu em 1982, no conto ficcional de William Gibson, “*Burning Chrome*” (GIBSON, 1982), sendo em seguida cunhado na obra “*Neuromancer*” (GIBSON, 1984), publicada em 1984, e designava uma rede de computadores, roteadores, chaves e pessoas em constante mutação (SILVA, 2014). Ao ser transposto para o mundo real, conforme mostra Francisco Rodrigues (2016, p. 7), o termo passou a ilustrar “[...]um conjunto de aplicações, das quais se destacam a rede global de comunicações, o media global e o espaço de interacção social e a grande biblioteca digital.” Logo, hoje, como afirma Marcelo Aparício (2017, p. 33), entende-se o ciberespaço como “uma evolução, melhoria e em alguns casos substituição, no que diz respeito ao processo comunicacional em geral e à transmissão de informação, em particular”.

Em virtude, então, da multiplicidade de operações processadas nesse ecossistema incorpóreo, surge a necessidade de desenvolver ferramentas que garantam a segurança dos procedimentos realizados nesse ambiente. Seguindo essa direção, de acordo com Jorge Gouveia (2021, p. 59), nasce o conceito (embora não definitivo, tampouco fechado em si mesmo) de cibersegurança como “[...]a proteção que se realiza no ciberespaço contra as ameaças a valores ou direitos da comunidade política, assim perpetrados neste novo ambiente digital”.

Para que se concretize, é necessária então a adoção de medidas por parte dos mais variados setores da sociedade em nível nacional e internacional. A esse movimento de adequação comportamental, normativa e organizacional à uma política de segurança cibernética, dá-se o nome de “cultura de cibersegurança”.

Para a implementação eficiente dessa cultura de cibersegurança, os setores público e privado devem caminhar juntos e atentos não só às situações que se desenham no Brasil, como aquelas que se desenham no exterior, posto tratar-se de uma questão transnacional que requer união de esforços para o combate.

Na esfera privada, esse tipo de ação pode resultar em diversas violações, à exemplo da violação de livre concorrência, regida pelo Princípio da Livre Concorrência que conforme ressalta Fortes e Bassoli (2010, p. 240), “parte da ideia de liberdade de competição no mercado a partir da igualdade de condições entre os agentes econômicos”, gerando sérios impactos econômicos e sociais, uma vez que o

desenvolvimento social suscitado por aquela atividade também é afetado.

Esses motivos que por si só já bastariam para justificar o interesse do Estado em investir na segurança, são reforçados quando adicionado à equação o valor agregado à tecnologia e ao conhecimento. Nesse sentido, discorre Ronaldo Bach da Graça (2015, p. 10):

> Para que se possa mensurar de forma mais precisa o prejuízo de um furto de tecnologia de ponta, pode-se constatar que se estão analisando hipóteses de tecnologias por vezes caríssimas, mas que perdem valor de forma intensa quando são difundidas ou ao menos deixam de ser segredo. O tempo também pode desvalorizar tecnologias dominadas, porém este processo tende a se acelerar em virtude da espionagem cibernética.

Conhecimento neste ponto, sendo compreendido como a matéria-prima que viabilizará, através de aperfeiçoamentos, recombinações e demais interações possíveis, a implementação de tecnologias que, quando aplicadas ao mundo concreto, poderão resultar em processos de inovação que impulsionam o crescimento não só de quem os implementam, como da sociedade que deles desfruta.

O impacto econômico dessas violações, portanto, é um dos fatores que mais chama atenção e pode ser mensurado a partir da análise de suas consequências, concluindo ser a cibersegurança uma das principais categorias de risco econômico e empresarial. Neste sentido, o Relatório Cibersegurança em Portugal Economia elenca possíveis soluções (2022, p. 16)

> Para limitar os impactos dessas barreiras ao investimento podem ser adotadas diferentes medidas regulatórias: i) A regulação da segurança ex ante e a responsabilização ex post; ii) A divulgação de informação para reduzir assimetrias; iii) A generalização da adoção de seguros contra riscos cibernéticos; iv) A responsabilização indireta do intermediário; e, inclusivamente v) A promoção de medidas de reconhecimento de boas práticas e protocolos de cibersegurança, nomeadamente, de certificação.

É difícil encontrar um processo industrial, comercial, financeiro ou administrativo que não se utilize de instrumentos TICs em algum momento. Assim, o mau funcionamento desses instrumentos impacta diretamente sobre a economia e o mercado.

Mas através de que meios esses ataques cibernéticos que afetam tão diretamente dados estratégicos, propriedade intelectual e economia, se concretizam?

5.2 PRINCIPAIS MODALIDADES DE CIBERCRIMES

A modalidade de ataque mais usada por cibercriminosos ainda é o *phishing* por *e-mail*, técnica de engenharia social que conforme explicita Patricia Peck Pinheiro

(2021, p. 16), consiste em “[...] uma simulação, na qual a vítima é atraída ou enganada para que, pensando se tratar de um conteúdo legítimo, clique em um *link* falso, acesse uma página falsa ou execute algum arquivo para que haja furto de dados, ou acesso e elevação de privilégios”.

Outra modalidade de ataque é o *malware*, popularmente conhecido como “vírus de computador”, e de acordo com a autora “Nos dias atuais, os *malwares* normalmente visam à subtração de informações, ao controle da máquina e da infraestrutura de rede, à disseminação local ou remota, a ser um vetor de ataques e à extorsão por sequestro dos dados ou vazamento de informações, podendo ter um ou mais desses propósitos como funcionalidade” (2021, p. 16).

E a modalidade que mais tem ganhado repercussão na mídia, em grande parte pela habilidade que requer e pela capacidade de gerar prejuízos vultuosos, o *ransomware,* que de acordo com a autora (2021, p. 18), possui duas formas de atuação, podendo ser simultâneas ou não:

> Na primeira modalidade, é infectada a máquina e os dados do dispositivo são criptografados, sendo gerado um arquivo acessível, geralmente na área de trabalho ou apresentado em um navegador web em que o criminoso pede um resgate – geralmente a ser pago em criptomoedas – prometendo o envio de um código que possibilite que os dados sejam decriptografados, o que muitas vezes não acontece, ainda que seja efetivado o pagamento do “resgate”.
>
> Na segunda modalidade, ocorre o mesmo processo supracitado, porém, o criminoso envia os dados da vítima – e da empresa inteira em algumas oportunidades – para servidores remotos, podendo ou não os criptografar, exigindo o resgate para não revelar informações sigilosas que a empresa possua.
>
> Em ambos os casos, a “negociação” é feita habitualmente por *e-mail*, sendo que no segundo caso, muitas vezes é o criminoso quem procura a empresa, demonstrando estar de posse dos dados.

Menos conhecidos do público geral por suas denominações, mas também fonte de preocupação são os ataques por *botnets* e *Distributed Denial of Service* (DDoS).

Botnets são redes de computadores que foram invadidas e infectadas para permitirem o acesso remoto. Já os ataques DDoS visam gerar a indisponibilidade dos servidores, fazendo com que o acesso fique fora do ar.

De acordo com relatório emitido pela IBM no ano de 2022 referente ao ano de 2021 a respeito do cenário de segurança cibernética (2002, p. 4), os *ransomwares* representaram o principal tipo de ataque, embora tenham tido uma redução de 2% em comparação ao ano anterior. Em segundo lugar, está o *phishing*, com 41% dos incidentes.

Para além disso, há ainda a preocupação com a corrupção dos próprios

funcionários, servidores ou terceirizados do local, que podem agir no fornecimento de dados e informações à concorrência, comprometimento de servidores e bancos de armazenamento, entre outros atos prejudiciais.

Quais instrumentos então já existem para combater e reprimir essas práticas?

5.3 A LEGISLAÇÃO DE CIBERSEGURANÇA NO BRASIL

Quando se pensa em legislações na área de tecnologia e inovação, é importante destacar a importância e tendência de uma abordagem menos dura, no sentido de dar preferência a normas que não engessem e intimidem o avanço tecnológico e que, ao mesmo tempo, tenham capacidade de atender as demandas sem cair na obsolescência. Todavia, seguindo a tradição pátria, o Brasil tem adotado uma postura mais positivista, optando pela formulação de instrumentos formalmente legislativos.

Até 2014, ano marcado pelo advento do Marco Civil da Internet, Lei 12.965/2014 (BRASIL, 2014), o Brasil não possuía uma normatização voltada para a *internet* e, embora não inclua medidas de cibersegurança propriamente falando, foi um passo importante na direção de começar a pensar e reconhecer a relevância do tema.

Mais alinhado às noções de segurança e privacidade no ambiente digital, em 2016, o Brasil editou o Decreto nº 8.793/2016 (BRASIL, 2016), estabelecendo a Política Nacional de Inteligência e consolidando alguns conceitos fundamentais, a ver

> **6.1 Espionagem** É a ação que visa à obtenção de conhecimentos ou dados sensíveis para beneficiar Estados, grupos de países, organizações, facções, grupos de interesse, empresas ou indivíduos.
>
> Ações de espionagem podem afetar o desenvolvimento socioeconômico e comprometer a soberania nacional. Há instituições e empresas brasileiras vulneráveis à espionagem, notadamente aquelas que atuam nas áreas econômico-financeira e científico-tecnológica. O acesso indevido a dados e conhecimentos sensíveis em desenvolvimento, bem como a interceptação ilegal de comunicações entre organizações para a obtenção de informações estratégicas, têm sido recorrentes e causado significativa evasão de divisas.
>
> **6.5 Ataques cibernéticos** Referem-se a ações deliberadas com o emprego de recursos da tecnologia da informação e comunicações que visem a interromper, penetrar, adulterar ou destruir redes utilizadas por setores públicos e privados essenciais à sociedade e ao Estado, a exemplo daqueles pertencentes à infraestrutura crítica nacional.
>
> Os prejuízos das ações no espaço cibernético não advêm apenas do comprometimento de recursos da tecnologia da informação e comunicações. Decorrem, também, da manipulação de opiniões, mediante ações de

> propaganda ou de desinformação. [grifos do autor] (BRASIL, 2016)

Dentre as diretrizes, o decreto traz ainda

> **8.8 Fortalecer a cultura de proteção de conhecimentos** O acesso não autorizado a técnicas, processos de inovação, pesquisas, planos e estratégias, bem como ao patrimônio genético e a conhecimentos tradicionais a ele associados, pode comprometer a consecução de objetivos nacionais e resultar em prejuízos expressivos no campo socioeconômico.[...] Os importantes resultados advindos de pesquisas científicas e tecnológicas requerem contínuo aperfeiçoamento de mecanismos de proteção nos meios acadêmicos e empresariais.
>
> Torna-se, portanto, imprescindível e urgente fortalecer, no âmbito da sociedade, a cultura de proteção, visando ao estabelecimento de práticas para a salvaguarda de conhecimentos por parte daqueles que os detenham. A Inteligência deve concorrer para a disseminação dessa cultura como forma de evitar ou minimizar prejuízos ao País. [grifos do autor] (BRASIL, 2016)

No campo da proteção de dados pessoais, em 2018, o Brasil ganhou a Lei Geral de Proteção de Dados, Lei 13.709/2018 (BRASIL, 2018), e com ela cinco eixos em torno dos quais a proteção se articula, conforme esquematizam Danilo Doneda e Laura Mendes (2018, p. 312) “[...] i) unidade e generalidade da aplicação da Lei; ii) legitimação para o tratamento de dados (hipóteses autorizativas); iii) princípios e direitos do titular; iv) obrigações dos agentes de tratamento de dados; v) responsabilização dos agentes.”

Mas o grande salto ocorreu em 2020, ano em que foi aprovada a Estratégia Nacional de Segurança Cibernética (E-Ciber), através do Decreto nº 10.222, de 5 de fevereiro de 2020 (BRASIL, 2020), com validade para o quadriênio 2020-2023.

O referido Decreto estabelece, de início, dez ações estratégicas a serem adotadas pelos setores públicos e privados. São elas (BRASIL, 2021): i) Fortalecer as ações de governança cibernética; ii)Estabelecer um modelo centralizado de governança no âmbito nacional; iii) Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade; iv) Elevar o nível de proteção do Governo; v) Elevar o nível de proteção das Infraestruturas Críticas Nacionais; vi) Aprimorar o arcabouço legal sobre segurança cibernética; vii) Incentivar a concepção de soluções inovadoras em segurança cibernética; viii) Ampliar a cooperação internacional do Brasil em Segurança cibernética; ix) Ampliar a parceria, em segurança cibernética, entre setor público, privado, academia e sociedade e; x) Elevar o nível de maturidade da sociedade em segurança cibernética.

Contudo, considerando se tratar de uma questão transfronteiriça, como já apontado, não basta olhar apenas para o Brasil. É preciso trabalhar sob o manto da

internacionalização do direito e da cooperação internacional para alcançar uma postura comum na repressão e combate das questões de segurança. Reforçando essa visão, aduzem Rafaela Favera e Rosane Silva (2016, p. 8) que “tanto o direito internacional quanto a comunidade internacional estariam legitimados a influenciar, reforçar e dar suporte aos Estados para a elaboração de suas leis e delineamento de políticas internas nacionais”.

Assim, cumpre observar também o caminho regulatório que tem sido feito no cenário internacional.

5.4 A LEGISLAÇÃO DE CIBERSEGURANÇA EM OUTROS PAÍSES

O traço transfronteiriço do ciberespaço somado ao mau uso das Tecnologias de Informação e Comunicação (TICs) estimulou os Estados a, cooperativamente, dirigirem seus esforços para definir princípios e regras comuns em matéria de cibersegurança, conforme transparece o Relatório Cibersegurança em Portugal: Ética e Direito (2020, p.41)

> A primeira iniciativa deste tipo foi avançada no quadro da OCDE, em 1996, e consistiu numa proposta da França de adoção de uma Carta para a Cooperação Internacional na Internet, largamente decalcada das regras existentes de Direito Internacional do Mar (Mačák, 2016: 130). A proposta não foi acolhida, tal como não viria a ser acolhida a proposta de adoção de um tratado para proibir o uso de armas informáticas, avançada pela Rússia no quadro da ONU, em 1998. A proposta russa teve, em todo o caso, o efeito de colocar a regulação do ciberespaço na agenda da ONU, ao motivar a primeira resolução da Assembleia Geral sobre os “desenvolvimentos no setor da informação e telecomunicações no contexto da segurança internacional” (A/RES/53/70) e a subsequente constituição de um Grupo de Peritos Governamentais para estudar as ameaças oriundas do ciberespaço e as possíveis soluções jurídicas para as enfrentar (Eggenschwiler, 2019: 3). No seu relatório de 2013, o Grupo de Peritos concluiu que as normas de Direito Internacional já existentes – desde logo, a Carta da ONU – se aplicam ao ciberespaço (UN Doc A/68/98), uma pronúncia que, sem ser inteiramente esclarecedora quanto à substância e ao modo daquela aplicação, parece ter condenado quaisquer planos de adoção de um tratado internacional de âmbito mundial sobre cibersegurança num futuro próximo (Mačák, 2016: 128-130).

O que fica nítido dos esforços conjuntos destes Estados (e também da iniciativa privada) é que não há interesse em utilizar ferramentas jurídicas rígidas demais que possam, futuramente, ser um empecilho à correspondência entre realidade fática (sempre em veloz avanço) e proteção jurídica, de modo que há uma preferência por adoção de recomendações e compromissos políticos firmados entre as partes.

Como parte deste processo, os Estados se viram abrindo mão de parte do seu poder normativo em prol da autorregulação por parte das empresas de tecnologia.

Contudo, muito embora a presença de múltiplos atores seja interessante do ponto de vista de enriquecimento do debate, por outro lado, contribui para a fragmentação da norma, resultando em vários paradigmas sobre responsabilidade no ciberespaço e respectivas normas aplicáveis, o que, na contramão do pretendido, pode transparecer falta de consenso entre a comunidade, afetando, consequentemente, a credibilidade.

Contudo, isto é apenas uma tendência, de modo que não obsta a formulação de instrumentos mais duros, como o Acordo de Budapeste, sancionado pelo Conselho da Europa em 2001, que recomenda aos países signatários a adoção de medidas legislativas para tipificar crimes cibernéticos, dividindo as orientações em basicamente três categorias: a parte penal, focada na punição de condutas que surgiram com o advento da *internet*; a parte processual, focada nas provas e nos meios para sua obtenção e; a parte de cooperação internacional, voltada para mecanismos de assistência mútua entre os países partes (AZZOLIN, 2018).

Duas décadas após a assinatura e entrada em vigor, no ano de 2020, com validade de três anos, o Brasil recebeu o convite para aderir ao Acordo, cumprindo com a orientação de cooperação internacional e possibilitando uma efetividade maior na persecução penal dos crimes cibernéticos. No ano de 2021, através do Decreto Legislativo 37/21 (BRASIL, 2021), o Brasil promulgou o referido Acordo.

No bloco da União Europeia, a discussão encontra-se em constante avanço, ocupando espaço relevante na agenda política desde a adoção pela Comissão Europeia do Plano de Ação para a Sociedade da Informação em 1994. A partir de então, seguiu-se uma série de instrumentos legislativos para regular a segurança no ciberespaço.

Em 2004, dando continuidade a esse movimento, foi criada a Agência Europeia para a Segurança das Redes e da Informação (ENISA), com a missão de exercer um papel ativo junto aos Estados Membros e aos agentes privados, desenvolvendo uma cultura de segurança das informações em rede.

De uma proposta legislativa anexa à primeira Estratégia da União Europeia para a Cibersegurança, resultou a Diretiva sobre Segurança das Redes e da Informação (SRI), que entrou em vigor no ano de 2016, voltada a reforçar a cooperação entre os Estados-Membros no que concerne a cibersegurança e estabelecer

> [...] obrigações de segurança a cumprir pelos operadores que prestam

> serviços essenciais (em setores críticos como a energia, os transportes, a saúde e as finanças) e pelos prestadores de serviços digitais (mercados em linha, motores de pesquisa e serviços de computação em nuvem). Será também exigido a cada país da UE que designe uma ou mais autoridades nacionais e defina uma estratégia para lidar com as ameaças cibernéticas. (CONSELHO EUROPEU, 2016)

Dando continuidade às estratégias e instrumentos legislativos no âmbito da União Europeia, em 2017 foi lançado um pacote de cibersegurança contendo como proposta a criação de uma certificação de cibersegurança a nível da União Europeia, concretizado posteriormente em 2019 com o Regulamento 2019/881. Em 2020, foi apresentada a Estraégia de Cibersegurança da União Europeia para a década digital.

No final de 2020, a Comissão Europeia e o Serviço Europeu para a Ação Externa (SEAE) apresentaram uma nova proposta de estratégia da União Europeia (UE) para a cibersegurança com o objetivo de “reforçar a resiliência da Europa contra as ciberameaças e garantir que todos os cidadãos e empresas possam se beneficiar plenamente de serviços e ferramentas digitais fiáveis e credíveis. A nova estratégia contém propostas concretas para a utilização de instrumentos regulamentares, de investimento e de ação” (CONSELHO EUROPEU, 2021).

Em Portugal, grande expoente desta discussão, contando com larga produção acadêmica voltada para segurança no ambiente digital, como não poderia deixar de ser, a legislação voltada à cibersegurança acompanha os compromissos assumidos e os parâmetros determinados pela União Europeia, como demonstra o Relatório Cibersegurança em Portugal Economia (2022, p. 49)

> A Lei do Cibercrime, aprovada pela Lei n.º 109/2009, de 15 de setembro, transpôs a Decisão-Quadro 2005/222/JAI, do Conselho da União Europeia, relativa a ataques contra sistemas de informação, e adaptou a ordem jurídica nacional à Convenção de Budapeste. A Lei n.º 46/2018, de 13 de agosto, transpôs a Diretiva SRI, estabelecendo o regime jurídico da segurança do ciberespaço. A Lei n.º 58/2019, de 8 de agosto, veio assegurar a execução, na ordem jurídica portuguesa, do Regulamento Geral sobre a Proteção de Dados, etc. No plano institucional, as matérias da cibersegurança caem sob a alçada de diferentes entidades [...]
> [...]
> A primeira Estratégia Nacional de Segurança do Ciberespaço foi adotada em 2015, com o propósito de estabelecer, em sintonia com as linhas gerais da Estratégia da UE para a Cibersegurança, “objetivos e linhas de ação com vista a uma eficaz gestão de crises, a uma coordenação da resposta operacional a ciberataques, a um desenvolvimento das sinergias nacionais e a uma intensificação da cooperação nacional, europeia e internacional neste domínio”.
> [...]
> A Estratégia Nacional aprovada em 2019, para o período 2019-2023, continua a alicerçar-se nos princípios de subsidiariedade, complementaridade e proporcionalidade, assumindo agora como objetivos estratégicos maximizar a resiliência, promover a inovação e gerar e garantir recursos.

Nos Estados Unidos da América (EUA), por sua vez, esforços mais veementes voltados à cibersegurança foram percebidos a partir do governo Obama, notadamente com a criação, em 2009, do *Cyberspace Policy Review,* responsável por moldar o cenário de cibersegurança no país. A partir de então, outros instrumentos foram criados. Em 2011, surgiu a Estratégia Internacional para o Ciberespaço, com o propósito de situar os EUA no centro das discussões sobre o tema, direcionando, também, a atuação do país. Em 2016, foram criados o Plano Nacional de Ação de Cibersegurança e o Comando Cibernético dos Estados Unidos (USCYBERCOM), voltados a criar mais integração entre os campos da sociedade e, consequentemente, promover respostas mais rápidas às ameaças (BURSSED, 2021).

Verifica-se, então, que medidas têm sido adotadas para coibir esses tipos de ataque e resguardar o que é produzido em seara de propriedade intelectual. Contudo, a velocidade do avanço da tecnologia e a expertise de seus operadores são um desafio para a regulação do tema.

Desta forma, como esse processo de adequação pode ser simplificado e difundido entre os setores ameaçados?

5.5 DIMENSÃO ÉTICA DA CIBERSEGURANÇA

A dependência da tecnologia na qual a sociedade mergulhou aparenta ser irreversível. O uso alargado das TICs, que seduzem no cotidiano, igualmente representam uma ameaça que, para a maioria dos usuários, passa despercebida. Ou pior, não alarmam o bastante frente às inúmeras facilidades que trazem. Esse grau de dependência aliado à insegurança de um universo tão amplo e com múltiplos atores é fator decisivo no movimento em direção à construção de estratégias e mecanismos de cibersegurança. Cotino e Sánchez (2021, p. 8)

> Com o advento da pandemia de COVID-19, o processo de digitalização global se acelerou consideravelmente, trazendo consigo mudanças importantes na forma de viver, trabalhar e comunicar-se. A digitalização aumentou nas empresas, residências e serviços públicos.
> [...] a dependência das TICs para gerir e monitorar sistemas essenciais que sustentam áreas primordiais como segurança, água, energia, mobilidade e rastreamento de ocorrências catastróficas relacionadas à mudança do clima aumenta os níveis de risco de ataques cibernéticos.

Somado a isso, observou-se crescer também a presença das empresas no mundo digital. O domínio em cibersegurança a partir de então, mostra-se fator decisivo para gerar nos cidadãos confiança nas instituições e na prestação estatal,

uma vez que o Estado tem por papel fundamental garantir a segurança e a integridade não só aos indivíduos, como às instituições públicas e privadas. Sobre esses riscos, discorre Nunes (2012, p. 125)

> O ciberespaço não é limitado pela esfera pública ou privada, interna ou externa. As ameaças podem surgir de qualquer local e ter efeitos assimétricos e fortemente disruptivos. Métodos de ataque semelhantes podem ser utilizados para atingir indivíduos, empresas ou Estados. O inegável valor associado à livre utilização da internet pode assim ser seriamente comprometido por uma vaga crescente de ciberataques, minando a confiança na segurança global do ciberespaço.

Mas qual seria o limite entre a tutela eficaz e a intrusão do Estado nos direitos e liberdades que ele mesmo se propõe a proteger? Uma proteção mais contundente pode representar um maior controle das redes e dados. Neste sentido, Oppermann (2014, p. 148) “[...] o ciberespaço não deveria ser utilizado incorretameente como um instrumento de guerra, espionagem ou sabotagem [...]”.

Este tipo de dilema ilustra o caráter ético que permeia a cibersegurança, de modo que uma atuação meramente técnica não se mostra suficiente para suprir as demandas do tema, uma vez que a onipresença da rede na sociedade moderna impõe que governos, empresas, organizações e indivíduos, respeitem as fronteiras uns dos outros.

Soma-se a isso o fenômeno da redistribuição de poder, visto que em uma sociedade acoplada ao mundo digital, quem possui dados (sensíveis ou não) é rei. Acquisti, Taylor e Wagman (2016, p. 445) “Se é verdade que informação é poder, então o controle sobre informações pessoais pode afetar o equilíbrio do poder econômico entre as partes”.

A partir de então, surge a preocupação com o armazenamento de dados pessoais por parte de entidades públicas e privadas e com a conscientização da sociedade como um todo dos riscos aos quais está exposta e da responsabilidade que o gozo de tantos benefícios exige. Tene e Polonetsky (2011, p. 63)

> Os dados tornaram-se a matéria-prima da produção, uma nova fonte de imenso valor econômico e social. Os avanços na mineração e análise de dados e o aumento maciço do poder de computação e da capacidade de armazenamento de dados expandiram, por ordem de magnitude, o escopo de informações disponíveis para empresas, governo e indivíduos. Além disso, o crescente número de pessoas, dispositivos e sensores que agora estão conectados por redes digitais revolucionou a capacidade de gerar, comunicar, compartilhar e acessar dados. Os dados criam um enorme valor para a economia global, impulsionando a inovação, a produtividade, a eficiência e o crescimento. [tradução nossa]

Trata-se, portanto, de uma nova dimensão da cidadania o estímulo à adoção de

comportamentos eticamente adequados frente à avalanche de informação que as redes trazem, como aponta Gonçalves (2019, p. 16)

> O aumento da consciência relativamente à cibersegurança e à segurança da informação irá fazer com que os colaboradores reduzam a prática de comportamentos que colocam a cibersegurança em causa, isto se for bem utilizada, aplicada e interpretada.

O grande desafio, portanto, que se coloca quando o assunto é cibersegurança, é o de estabelecer quão cerceadores os instrumentos e recursos utilizados devem ser, de modo a garantir a segurança, integridade e eficácia das redes, sem para tanto ferir os direitos fundamentais que pretensamente se pretende resguardar. Daí a necessidade de uma discussão madura sobre ética.

O Direito e a Ética, embora intimamente ligados, não podem ser confundidos. Isso ganha contornos mais definidos quando se cai na armadilha de que aos aplicadores do Direito bastaria agir tecnicamente para o cumprimento da legislação sem se atentar à realidade do cenário que resultou naquela violação, a respeito dessa relação, Di Rezende Bernardes (2012, p. 36)

> [...] é possível observar a Ética, em interface com o Direito, acata a definição de conduta amparada na aplicação de regras morais no meio de convívio social, ou seja, a caracterização do homem enquanto ser racional. É essa face normativa da Ética que a relaciona intimamente com o Direito. Nesse sentido, a contínua discussão da Étiuca dentro do Direito encontra respaldo no fato de ser uma área das Ciências Humanas que busca a consolidação e a manutenção da justiça e da moralidade social.

O Direito representa a moldura da atuação nas questões relacionadas à segurança na rede, mas é dever de seus aplicadores dar um passo além e observar o quadro como um todo.

A velocidade com a qual a tecnologia avança claramente provoca um descompasso com o mundo jurídico, uma vez que facilmente leis e afins tornam-se obsoletas. Por esse motivo, *soft laws* mostram-se mais interessantes, dando preferência, então, a instrumentos normativos mais flexíveis e menos burocráticos para atualização, como códigos de conduta, conforme ensina Serrano (2022, p. 29)

> O Soft Power, evita as ferramentas tradicionais de política externa procurando obter influência através da construção de redes, comunicando por meio de narrativas convincentes, estabelecendo regras internacionais e aproveitando os recursos que tornam um país naturalmente atraente para o mundo.
> [...]
> É possível afirmar que o “Ciber”- Soft Power, funciona como uma extensão do Soft Power e respetivas ferramentas no Ciberespaço e deste modo, a noção de Soft Power aliada ao prefixo “ciber”, surge como a capacidade de influenciar, de controlar ou dominar os recursos existentes no Ciberespaço com uma finalidade que não se limita apenas ao Estado e ao seu interesse

> nacional/internacional, mas também a outros atores civis ou não .

O controle das ferramentas cibernéticas tem potencial para representar um risco à dignidade da pessoa humana, isto porque trata-se de tema que atinge diretamente diversos pontos dos direitos fundamentais, como a privacidade, a liberdade, a propriedade, a saúde e demais aspectos do foro íntimo de cada um, tão caros à Carta Magna brasileira, conforme demonstra Lima (2020, p. 17)

> Ao invés de uma promoção de direitos fundamentais concretizados pelo contexto atual da cidadania, as novas tecnologias os reduziram. Estes riscos, segundo Pérez Luño (2003), podem ser classificados como jurídicos, sociais e políticos. Os riscos políticos seriam de uma verticalização da política, uma mercantilização da esfera pública e a apatia política. Os riscos morais apontam para uma carência da realidade e os riscos jurídicos para uma degradação do processo legislativo, um aumento da criminalidade informática e uma invasão da intimidade.

A compatibilização, portanto, de um sistema firme o bastante para combater questões de tamanha complexidade, mas ao mesmo tempo suficientemente sensíveis para não agredir valores tão caros, é um desafio.

O mundo inteiro viu seu sentido de privacidade ser seriamente abalado após os ataques do 11 de setembro, onde a proteção da informação, fosse pública ou privada, tornou-se prioridade número um. O resultado foi uma vigilância intensa sobre os cidadãos e seu modo de agir e tomar decisões, ou seja, instaurou-se um estado de hipervigilância muito similar às práticas de cibersegurança que, sob o fundamento de proteção, colocam em xeque a liberdade e autonomia em prol de segurança. Sobre esta influência, dispara Lemos *et al*. (2011, p. 43)

> A sociedade contemporânea pós 11 de setembro alia, ao mesmo tempo, formas de vigilância disciplinar, panóptica (Foucault) e formas de controle, digitais, em movimento, típico das sociedades de controle (Deleuze). Câmaras de vigilância, rastreamento de dados na internet, formação de perfis digitais com mineração de dados em redes sociais [...] As formas de controle, monitoramento e vigilância estão por toda parte e passam a integrar o *modo operandis* da sociedade da informação neste começo de século XXI. [...] A sociedade contemporânea expandiu, como nenhuma outra, as formas de controle, monitoramento e vigilância, tanto de maneira forçada [...] como de forma espontânea [...]

Esses níveis de exposição ultrapassam a esfera privada e atingem também empresas e governos.

5.6 A PROPRIEDADE INTELECTUAL E A CIBERSEGURANÇA

Os principais esforços para a tutela da propriedade intelectual a nível internacional aconteceram antes da chegada dos anos 2000, marco da ampliação do

uso da internet em todo o mundo (Convenção de Paris em 1883; Convenção de Berna em 1886; Convenção de Roma em 1961; Convenção de Bruxelas em 1974).

Por esta razão, temas como a exploração digital das obras, prestações e produções protegidas por direito de autor e direitos conexos e confidencialidade de informações comerciais e industriais diretamente relacionadas à concorrência leal no ambiente empresarial, estão intimamente conectadas aos conflitos de cibersegurança.

Sobre o impacto da cibersegurança na propriedade intelectual, Delloitte, empresa de auditoria e consultoria empresarial presente em mais de 150 países, reforça (2016, p. 27)

> A perda da Propriedade Intelectual é um custo intangível associado com a perda do controle exclusivo sobre segredos de marca, *copyrights*, planos de investimentos, e outras propriedades e informações confidenciais, que podem levar a uma perda da vantagem competitiva, perda de receita, e prejuízo duradouro e irreparável para a companhia. Propriedades Intelectuais como, mas não limitadas a, patentes, designer, *copyrights*, marcas, e segredos industriais. [tradução nossa]

Em uma sociedade massivamente informatizada, as bases de dados armazenadas digitalmente são o principal repositório das empresas. Este fator agrava a questão da segurança, uma vez que frequentemente essas bases são armazenadas em nuvens pertencentes a locais físicos subordinados a gerência distinta da gerência dos dados. O advento da pandemia do COVID-19 dobrou esse risco, uma vez que com o teletrabalho houve a realocação das redes empresariais para as redes domésticas, escalonando a ameaça para os segredos de negócio. Sobre a relevância da pandemia na aceleração do processo de informatização dos dados, afirmam Tereso e Pratas (2021, p. 127)

> A ligeireza com que as empresas passaram a sua atividade presencial para o regime online, não permitiu que questões importantes como as boas práticas de cibersegurança fossem pensadas, na maioria dos casos, atempadamente. Este tema, levanta-nos grandes questões: será que as empresas possuem os mecanismos de acesso aos seus sistemas a partir do exterior implementados e configurados de forma segura? Será que as empresas possuem políticas de segurança ajustadas à sua realidade de trabalho? Será que as empresas dispõem de um serviço de vigilância sobre os sistemas de informação seguros? Será que os colaboradores fazem um uso seguro da internet nas suas casas, cumprindo com as boas práticas de segurança e não expondo os seus dados, quando acedem remotamente aos sistemas de informação da empresa?

Agravando o quadro, de acordo com o estudo dos resultados de segurança de 2021 pela Cisco (Cisco, 2021), as empresas brasileiras tem sucesso de apenas 47% em gerenciar os principais riscos, bem como em criar uma cultura de cibersegurança,

dado alarmante, considerando que em 2019, pesquisa realizada com 200 empresas brasileiras (Cyber Review, 2019) concluiu que 55,4% eram totalmente dependentes do uso de tecnologia para a concretização de suas atividades e 35% delas poderiam sofrer paralizações causadas por problemas tecnológicos. Esta mesma pesquisa ainda ressaltou que para 80% um incidente cibernético causaria um impacto operacional com reflexos em toda a empresa; 34% relataram já terem sido vítimas de ataques cibernéticos entre os anos 2018 e 2019; 29% relataram ter sido vítimas de ataques que atingiram o campo operacional da empresa; 27,8% tiveram altos custos de reconstrução sistêmica e 4% tiveram sua reputação no mercado prejudicada.

Nesta medida, a tutela da confidencialidade dos ativos de propriedade intelectual representa, em grande medida, a tutela também da cibersegurança dos locais onde esses dados serão armazenados e processados. Deste modo, dentro da sua esfera de ação, mostra-se razoável que a atuação do legislador ou a ele equiparado, se centre na elaboração de medidas voltadas à obtenção, preservação e conservação desses dados.

Desta forma, e mais uma vez tomando como ponto de partida da discussão o caráter transfronteiriço da cibersegurança, a preocupação quando se fala em propriedade intelectual e cibersegurança pode ser ramificada em três: a compatibilidade dos sistemas internacionais; a criação de medidas para evitar, investigar e provar de maneira eficiente violações e a criação de mecanismos internacionais com força de aplicação.

5.7 A RESPONSABILIDADE PELA VIOLAÇÃO PELA PROPRIEDADE INTELECTUAL

Contudo, por nem sempre serem as violações à segurança cibernética evitadas, deve ser garantido aquele que teve seu direito violado uma reparação pelo prejuízo sofrido. É neste contexto que se insere a análise da responsabilidade pela violação da propriedade intelectual tanto pela ótica externa, quanto interna, uma vez que se trata de tema transnacional.

5.7.1 A responsabilidade internacional pela violação da propriedade intelectual

Ao Direito Internacional cabe a regulação da coletividade de nacionais constituída em territórios e governada por Estados dotados de soberania e politicamente organizados.

Também cabe a este ramo autônomo do Direito a cooperação com organismos e organizações com o fim de manter o equilíbrio da sociedade global.

Assim como no Direito interno, uma vez invadida a esfera jurídica de um terceiro em âmbito internacional, nasce um conflito que requer o sopesamento entre a responsabilidade internacional de garantir a preservação do equilíbrio e a autonomia dos Estados soberanos, sem deixar de lado seus papéis como sujeitos de direito e, consequentemente, de deveres.

Desta forma, não fogem os Estados à responsabilização pelos atos por si mesmos cometidos ou viabilizados por sua invigilância. Assim, conta também a comunidade internacional com um marco de responsabilidade que visa abordar a violação dos direitos dos Estados-nações e das comunidades que os compõem.

Para assentar os contornos normativos da responsabilidade internacional dos Estados, foi elaborado pelas Nações Unidas (2005) o *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (ARSIWA). Em breve análise, seu artigo 2º estabelece os casos em que incidirá a responsabilidade civil de um Estado.

> Artigo 2º Elementos de um ato internacionalmente ilícito de um Estado
> Há um ato internacionalmente ilícito de um Estado quando a conduta consiste em uma ação ou omissão que:
> (a) é atribuível ao Estado de acordo com o direito internacional; e
> (b) constitui uma violação de uma obrigação internacional do Estado. (Nações Unidas, 2005) [tradução nossa]

Infere-se que apesar dos esforços, o ARSIWA se posicionou de maneira tímida ao estabelecer as situações em que incidiria a responsabilidade do Estado e, quando o fez, o fez de forma favorável a ele, responsabilizando-o apenas nas situações em que figurar como partícipe de alguma forma. O artigo 8º confirma tal posicionamento

> Artigo 8 Conduta dirigida ou controlada por um Estados-nação
> A conduta de uma pessoa ou um grupo de pessoas deve ser considerada ato de um Estado sob a lei internacional se a pessoa ou grupo de pessoas está de fato agindo sob sua instrução, ou sob o direcionamento ou controle desse Estado na realização da conduta. (Nações Unidas, 2005) [tradução nossa]

Logo, a promoção de um ambiente vulnerável ou a falta de previsão de punição adequada pelo Estado, de acordo com o referido documento, não invoca para ele nenhuma responsabilidade.

Com isso, outro problema surge a partir desse posicionamento que é a desproporcionalidade em relação ao inimigo: o ataque cibernético.

Quando pensado na esfera de um ataque privado, isto é, de uma invasão ao computador de uma pessoa física, por exemplo, tal raciocínio pode parecer distante.

Contudo, quando desenhado um cenário de acesso não autorizado a dados armazenados em bancos de dados de órgãos públicos, por exemplo, seja esse ataque de origem nacional ou internacional, tal visão passa a fazer sentido.

Assim, identificar as ações de órgãos estatais e de particulares no ambiente cibernético, por mais desafiador que seja, é elementar no combate a ilícitos dessa ordem. Desta forma, um Estado que raramente assume alguma responsabilidade e que se mostra lento no avanço de adoção de políticas públicas preventivas e repressivas voltadas as esferas pública e privada, coloca a sociedade global em situação de vulnerabilidade e pode ensejar, inclusive, a revitimização das vítimas de ataques, uma vez que, a título de exemplo, vazados os dados dos clientes de um escritório no Brasil, este escritório pode ser responsabilizado por *culpa in vigilando* (caracterizada pela falta de cuidado e fiscalização por parte do proprietário ou responsável pelo bem) e *culpa in custodiendo* (caracterizada pela ausência de atenção e cuidado com respeito a alguma coisa) se não forem adotados critérios de segurança.

Depreende-se, portanto, que a responsabilização pela prática do ilícito no ambiente cibernético e pelos danos por ele gerados pode alcançar não apenas a esfera privada, como a pública, posto que é possível tanto a figura do ofendido singular, quanto a figura de uma coletividade de indivíduos ofendia.

Entretanto, o atual posicionamento internacional, conforme Gabriela de Lima (2017, p. 214) aponta, opta por

> [...] mitigar a atribuição de responsabilidade internacional pelos ataques cibernéticos cometidos em detrimento da sociedade planetária, represando o direito dos usuários da rede a terem garantida a segurança necessária para o seu amplo e não vitimado acesso.

Nesse cenário, então, dificultada a perseguição dos direitos devidos em âmbito internacional, resta ao indivíduo a opção de buscar a reparação de prejuízos sofridos na esfera interna, isto é, a partir do arcabouço de direitos garantidos pela legislação brasileira.

5.7.2 A responsabilidade pela violação da propriedade intelectual no Brasil

Então, para além do previsto em esfera internacional, como o Brasil repara eventuais prejuízos causados por essas violações? Destaca-se que as violações decorrentes de ataques cibernéticos podem ser punidas em duas esferas: a penal e a cível, como assevera Cardoso (2008, p. 52)

> O desrespeito às normas e princípios relativos ao assunto produz em princípio, a responsabilidade civil de seu infrator. Além disso, essa violação pode também importar um ilícito penal, e seu autor sofrer a persecução penal por parte do Estado.

Ao voltar o olhar para a seara cível, se destaca a responsabilidade civil, que surge como uma reparação ou compensação patrimonial pelo prejuízo sofrido, prejuízo este que pode extrapolar a esfera da receita de uma empresa, por exemplo, e impactar diretamente a atratividade de investimentos no país, visto que a principal forma de retribuição pelos investimentos feitos em pesquisa e desenvolvimento é o lucro auferido com a entrada desses produtos no mercado.

Logo, o desrespeito aos direitos de propriedade intelectual tem o potencial de desestimular os investimentos por parte de terceiros sob o argumento de que o risco de violação de seus direitos não vale o aporte, ainda que considerado o pagamento parcial dos direitos a que fazem jus.

Considerando a propriedade intelectual então como um dos principais estímulos à inovação tecnológica e a um possível aumento do bem-estar social e o risco ao qual todos estão expostos devido a informatização das informações, a tendência é que ao refletir sobre a tutela da segurança da propriedade intelectual no ambiente cibernético, o impulso primário seja o de proteger esses direitos a todo custo.

Contudo, como já dito em momento anterior, se esta proteção se der de maneira demasiadamente rígida, como consequência, entre outras, poderia se ter a criação de um monopólio legal que inviabilizaria, por exemplo, a livre concorrência garantida pela Constituição Federal em seu artigo 170, inciso IV

> Art. 170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios:
> IV - livre concorrência (BRASIL, 1988)

Por essa razão, faz sentido que se recorra ao que já existe na norma para tutelar esses direitos. Nesse caminho, em um momento anterior a violação cibernética que pode resultar na lesão aos direitos de propriedade intelectual, ou quaisquer outros, os contratos bilaterais se mostram uma boa opção, principalmente quando considerados a segurança e o incentivo àqueles que pretendem investir em pesquisa e desenvolvimento, atendendo aos interesses de todos os envolvidos.

Ademais, a promoção da proteção como um direito obrigacional (instrumentalizado através do contrato), possibilita que a propriedade intelectual seja

tida como um instrumento de política pública e, consequentemente, de desenvolvimento nacional.

Porém, passada esta primeira oportunidade de, preventivamente, dirimir possíveis riscos, resta lidar com a preocupação que persiste em relação às violações, de modo que se mostra relevante abordar mais detalhadamente o tema da responsabilidade civil.

Ocorre que como já citado anteriormente, a responsabilidade civil tem por meta promover a restauração do equilíbrio perdido em razão de um prejuízo sofrido pela conduta de outrem. Essa função de reparação limita-se ao dano do lesado e abrange tanto os danos emergentes (prejuízo direto), como os lucros cessantes (valor que deixou de receber). Contudo, em decorrência dessa função reparadora, não pode o ofendido obter ganho superior àquele que auferiria antes da lesão (TARTUCE, 2022, p. 385).

Uma classificação relevante para dar continuidade à análise é a separação da responsabilidade civil em objetiva (sem culpa) e subjetiva (com culpa). No Brasil, somente cabe a responsabilidade civil objetiva quando houver previsão legal específica ou quando importar em risco da atividade, conforme o artigo 927 do Código Civil de 2002.

> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
>
> Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem. (BRASIL, 2002)

Considerando que a Lei de Propriedade Industrial é silente nesse aspecto e que não se aplica o risco da atividade aos direitos referentes à propriedade industrial, resta recorrer à regra geral, isto é, a responsabilidade subjetiva (por culpa), nos termos dos artigos 186 e 927 (transcrito acima), *caput*, ambos do Código Civil de 2002. Entender essa questão é importante pois, a partir dela, é possível entender a função da responsabilidade civil.

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito. (BRASIL, 2002)

Quando se fala em responsabilidade subjetiva (por culpa), além da função reparatória, desempenham-se também as funções preventiva e punitiva. Assim, é

necessário também que a conduta danosa seja interrompida a fim de evitar mais danos e que ela carregue poder de coerção suficiente para inibir futuras violações. Desta forma, tem-se que a indenização deve não só recompor o dano, mas também todo o prejuízo suportado.

Para que se configure essa responsabilização, há que se falar em quatro pressupostos: ato ilícito, culpa, dano e nexo causal (GONÇALVES, 2002).

O ato ilícito, para a responsabilidade civil, pode ser por ação ou omissão, ou seja, em decorrência de um fazer ou de um não fazer.

A culpa, conforme já esclarecido, é subjetiva, dependendo, portanto, de dolo ou culpa do agente. Para a norma, culpa é um juízo de censura da conduta do sujeito que deveria ter agido de uma determinada forma, mas não o fez, insurgindo assim em um ato reprovado pelo ordenamento jurídico. No caso da propriedade intelectual, tal ato seria, por exemplo, a violação da exclusividade do titular da tecnologia sobre sua propriedade através de um ato malicioso praticado por meio digital.

Esta culpa pode incidir tanto sobre o ato em si, quanto sobre os prejuízos causados por este ato, e ambos são de extrema importância para determinar o *quantum* a ser indenizado.

Em relação ao dano, quatro classificações são relevantes para os direitos de propriedade intelectual, são elas: o dano em sentido real e o dano em sentido patrimonial; os danos emergentes e os lucros cessantes; os danos presentes e os danos futuros; e os danos patrimoniais e não patrimoniais. A respeito de cada um deles, ensina Luis Leitão (2018, p. 344-350)

> Em resumo, os conceitos utilizados na classificação dos danos mencionados são: a) o dano em sentido real é indenizado por meio de uma reparação natural ou a entrega de outro equivalente; o dano patrimonial consiste numa indenização arbitrada no valor da diminuição do patrimônio. No caso, a regra prioritária a ser obedecida é a da indenização pelo dano real, reconstituindo-se a situação anterior, como se dano não tivesse existido. Somente na impossibilidade, deve-se fixar a indenização pecuniária. b) Danos emergentes seria o prejuízo imediato sofrido, ou seja, a perda de uma utilidade que o lesado já usufruia, enquanto que os lucros cessantes é a perda para o futuro, com forte possibilidade, quase como uma certeza, de o ganho existiria , se não fosse a lesão; c) danos presentes são os que são imediatamente verificados e os futuros, são os ainda não se verificaram no momento da fixação do valor do dano; d) danos patrimoniais são aqueles suscetíveis de avaliação pecuniária, enquanto que os danos não patrimoniais ou morais, não são suscetíveis dessa avaliação. Deve ser verificado de acordo com o tipo de utilidade que era usufruída pelo bem.

Há que se falar ainda na presunção do dano. Gama Cerqueira, embora ainda sob a égide do Código Civil de 1916, já argumentava que tão somente o desrespeito

ao direito seria suficiente para o julgamento procedente da ação, ainda que sem a comprovação de efetivo prejuízo, cabendo ao juiz, na ausência de elementos, fixar a indenização por arbitramento, isto é, suprindo o elemento faltante com a produção de prova pericial. Tal pensamento ainda ecoa nos dias atuais sob a vigência do Código Civil de 2002

> PROPRIEDADE INDUSTRIAL. USO INDEVIDO DE MARCA. INDENIZAÇÃO POR DIREITOS MATERIAIS. COMPROVAÇÃO. DISSÍDIO JURISPRUDENCIAL CONFIGURADO. CRITÉRIO DE CÁLCULO.
> 1. A falta de prequestionamento em relação aos arts. 331, I, do CPC e 208 da Lei 9.279/96, impede o conhecimento do recurso especial.
> Incidência da súmula 211/STJ.
> **2. No caso de uso indevido de marca, com intuito de causar confusão ao consumidor, o entendimento predominante desta Corte é que a simples violação do direito implica na obrigação de ressarcir o dano. Precedentes.**
> 3. Conquanto os lucros cessantes devidos pelo uso indevido da marca sejam determinados pelo critério mais favorável ao prejudicado, conforme o art. 210, caput, da Lei 9.279/96, o critério de cálculo previsto na lei deve ser interpretado de forma restritiva, fazendo-se coincidir, nesse caso, o termo "benefícios" presente no incido II, do art. 210, com a idéia de "lucros".
> 4. Recurso especial conhecido em parte e, nesta parte, provido.
> (REsp n. 710.376/RJ, relator Ministro Luis Felipe Salomão, Quarta Turma, julgado em 15/12/2009, DJe de 2/2/2010.) (Superior Tribunal de Justiça, 2009) [grifos nossos]

Assim, o mero acesso a informações sigilosas relacionadas a patentes através de violação cibernética, por exemplo, ainda que sem aplicação no mundo real, já é capaz de configurar a responsabilidade, uma vez que representa o nexo causal (quarto pressuposto para se falar em responsabilidade civil) entre a conduta ilícita e o dano.

Frente essa possibilidade, o legislador brasileiro já inseriu na Lei da Propriedade Industrial três formas de apuração dos lucros cessantes quando da violação a direitos

> Art. 210. Os lucros cessantes serão determinados pelo critério mais favorável ao prejudicado, dentre os seguintes:
> I - os benefícios que o prejudicado teria auferido se a violação não tivesse ocorrido; ou
> II - os benefícios que foram auferidos pelo autor da violação do direito; ou
> III - a remuneração que o autor da violação teria pago ao titular do direito violado pela concessão de uma licença que lhe permitisse legalmente explorar o bem. (BRASIL, 2002)

Na hipótese do inciso I, caberá ao titular do direito demonstrar a redução dos lucros em virtude da concorrência desleal (prática industrial ou comercial desonesta), desdobramento comum quando do roubo de patentes. Contudo, tal demonstração pode se mostrar um obstáculo à prestação jurisdicional pretendida, uma vez que, conforme elucida João da Gama Cerqueira (2010, p. 1.131)

> Não se deve concluir, entretanto, só por esse fato, que a contrafação não tenha causado prejuízos, porque estes não se revelam, necessariamente, na diminuição dos lucros ou na sua estabilização em determinado nível. O que o bom-senso indica é que o dono da marca realizaria lucros ainda maiores se não sofresse a concorrência criminosa do contrafator.

A hipótese do inciso II é a mais utilizada na prática forense por permitir que a apuração dos danos seja feita a partir da demonstração da realidade do mercado afetado pela violação. Contudo, neste caso, a perícia técnica contábil depende do prévio acesso aos registros contábeis do infrator, nem sempre acessível.

Por fim, o inciso III consiste em uma compensação, embora potencialmente insuficiente, considerando que nem sempre alcançará os reais prejuízos sofridos ou, ainda, o que seria negociado a título de licenciamento. Ainda assim, aplica-se a alternativa naqueles casos em que a demonstração do impacto do dano for de difícil mensuração, conforme explica Denis Barbosa em seu artigo “Valor indenizável das violações da Propriedade Intelectual” (p. 25)

> Tecnicamente, trata-se de uma forma de compensação do enriquecimento sem causa, essencial sempre que não se possam produzir provas de que a infração do direito beneficiou ao infrator. Apesar de bastante discutida na doutrina comparada, seja pela ideia de seria uma forma não adequada (pois que insuficiente e, por se equivaler a um preço para livremente infringir, ou seja, ...não punitiva....) de composição patrimonial, essa fórmula é sempre útil e por vezes vantajosa.

Retomando a opção mais recorrente na prática forense brasileira, qual seja, o inciso II, é interessante manter em vista que a realização da perícia contábil dependerá da chamada “massa contrafeita”, compreendida como a delimitação do objeto alvo de indenização. No caso de uma patente, o delimitado pelas reivindicações. Essa forma de valoração passa, portanto, pela fase objetiva (elementos) e pela fase temporal (duração da violação), deixando bem determinado qual elemento do mercado foi de fato atingido. Novamente no artigo “Valor indenizável das violações da Propriedade Intelectual”, Denis Barbosa esclarece o ponto (p. 29)

> O elemento ao qual a violação da exclusiva ou a deslealdade afeta pode ser igual, maior ou menor em extensão do que o produto ou serviço em questão. Será igual, se o produto ou serviço, por inteiro, for o afetado pela violação. Será menor, se apenas parte do produto ou serviço o for (por exemplo, do carro, apenas o design da calota tiver sido contrafeito). Será maior, quando a contrafação implicar em ganho para o infrator, ou perda para o lesado, de outras oportunidades de mercado que necessária e incondicionalmente acompanhassem a operação econômica praticada (por exemplo, quando a contrafação do design de uma xícara frustrasse a venda pelo titular do design do respectivo pires). Determinada a massa contrafeita, passar-se-á a fixar qual o ingresso líquido atribuível àquela massa.

Desta forma, embora a doutrina defenda a ideia de que a “massa contrafeita” poderá chegar a ser mais abrangente do que a reivindicação da tecnologia, principalmente quando não for possível a sua exploração de forma isolada, a lei e os Tribunais dão tratamento diferente à matéria, conforme demonstra o artigo 44, § 3º da Lei de Propriedade Industrial e julgados

> Art. 44 § 3º O direito de obter indenização por exploração indevida, inclusive com relação ao período anterior à concessão da patente, está limitado ao conteúdo do seu objeto, na forma do art. 41. (BRASIL, 1996)

> AGRAVO DE INSTRUMENTO. PROPRIEDADE INDUSTRIAL E INTELECTUAL. DISPOSITIVO DA SENTENÇA DÚBIO QUANTO À EXTENSÃO DA CONDENAÇÃO.
>
> Determinação de pagamento da contrafação proporcional a cada máquina ou mecanismo em separado que tenham sido vendidos com o uso do componente patenteado. **Descabimento da inclusão no cálculo da indenização do valor integral das máquinas plantadeiras ou semeadoras em que o mecanismo contrafeito foi implantado. Indenização desproporcional ao prejuízo efetivo causado. Enriquecimento sem causa. O valor da indenização deve ser calculado com base no valor do conjunto compactador e não com base no valor das semeadoras para plantios. O valor agregado da semeadora é muito superior ao valor do conjunto compactador**. Inteligência do art. 44, § 3º da Lei n. 9.279/96. Agravo de instrumento provido, por maioria. (Agravo de Instrumento Nº 70079819439, Sexta Câmara Cível, Tribunal de Justiça do RS, Relator: Luís Augusto Coelho Braga, Julgado em 28/03/2019).
>
> (TJ-RS - AI: 70079819439 RS, Relator: Luís Augusto Coelho Braga, Data de Julgamento: 28/03/2019, Sexta Câmara Cível, Data de Publicação: Diário da Justiça do dia 03/04/2019) (Tribunal de Justiça do Rio Grande do Sul, 2019) [grifos nossos]

> EMBARGOS DE DECLARAÇÃO – OMISSÃO E CONTRADIÇÃO – CRITÉRIO DE APURAÇÃO DA MULTA PELO DESCUMPRIMENTO DA ANTECIPAÇÃO DE TUTELA CONCEDIDA EM PRIMEIRO GRAU.
>
> Determinação para que a multa incida por evento, independentemente das perdas e danos a serem apuradas em liquidação de sentença - **Quantum indenizatório que deve ser apurado somente sobre o valor do soquete objeto da patente de invenção PI 9505263-1, e não sobre o valor do farol como um todo** - Acolhimento dos embargos declaratórios da Magneti Marelli, rejeitados os da empresa Indústrias Arteb S/A.
>
> (TJ-SP - EMBDECCV: 91310773820078260000 SP 9131077-38.2007.8.26.0000, Relator: Silvério Ribeiro, Data de Julgamento: 02/06/2010, 5ª Câmara de Direito Privado) 9Tribunal de Justiça de São Paulo, 2007) [grifos nossos]

Isso mostra que apesar de se contar com a “massa contrafeita” para auxiliar na determinação do montante a ser indenizado, deve haver um equilíbrio entre esta e a expectativa do titular da tecnologia, apesar das contrariedades que uma violação dessa espécie possa causar.

Dando continuidade a apuração do montante a ser pago a título de indenização, dispõem os artigos 208 e 209 da Lei da Propriedade Industrial (Lei nº. 9.279/1996), além do já abordado artigo 210 da mesma lei

> Art. 208. A indenização será determinada pelos benefícios que o prejudicado teria auferido se a violação não tivesse ocorrido.
> Art. 209. Fica ressalvado ao prejudicado o direito de haver perdas e danos em ressarcimento de prejuízos causados por atos de violação de direitos de propriedade industrial e atos de concorrência desleal não previstos nesta Lei, tendentes a prejudicar a reputação ou os negócios alheios, a criar confusão entre estabelecimentos comerciais, industriais ou prestadores de serviço, ou entre os produtos e serviços postos no comércio.
> § 1º Poderá o juiz, nos autos da própria ação, para evitar dano irreparável ou de difícil reparação, determinar liminarmente a sustação da violação ou de ato que a enseje, antes da citação do réu, mediante, caso julgue necessário, caução em dinheiro ou garantia fidejussória.
> § 2º Nos casos de reprodução ou de imitação flagrante de marca registrada, o juiz poderá determinar a apreensão de todas as mercadorias, produtos, objetos, embalagens, etiquetas e outros que contenham a marca falsificada ou imitada. (Brasil, 1996)

Isso mostra que apesar de contar com o recurso da “massa contrafeita” para auxiliar na determinação do montante a ser indenizado, deve haver, sobretudo, um equilíbrio entre esta e a expectativa do titular da tecnologia, a despeito das contrariedades que uma violação possa causar.

A partir do exposto, observa-se que o prejudicado conta com um amparo da legislação pátria, embora, por vezes, a extensão do ataque cibernético seja extraterritorial. Conhecer a extensão dos direitos que podem ser reivindicados é primordial não só no foro pessoal, como no público, tendo em vista que a propriedade intelectual exerce um papel decisivo no crescimento econômico em razão de sua relação próxima com a pesquisa, o desenvolvimento e a inovação.

6. METODOLOGIA

6.1 LISTA DAS ETAPAS METODOLÓGICAS

Etapas	Descrição	Tempo
Levantamento dos dados sobre o estado de coisas da cibersegurança e seus principais conceitos	A partir da adoção de meios de informação bibliográficos, com fontes de dados primárias e secundárias.	De 1º/2021 a 2º/2022
Organização dos dados obtidos na primeira etapa	Curadoria e catalogação das principais ameaças à segurança cibernética e dos principais meios adotados para combatê-la.	1º/2022 a 1º/2023
Qualificação do Projeto	Formalização da proposta de pesquisa e produto tecnológico ao PROFNIT Nacional.	1º/2022
Análise dos dados	Por tratar-se de uma pesquisa qualitativa quanto à abordagem, a análise dos dados se dará a partir da interpretação e observações da pesquisa, de modo a viabilizar a produção de um manual de boas práticas a partir da coleta de dados realizada nas etapas anteriores.	1º/2022 a 1º/2023

6.2 DESCRIÇÃO DETALHADA DE CADA ETAPA METODOLÓGICA

A partir da relação existente entre sociedade, direito e tecnologia, e impulsionado pelo papel de aceleração que a pandemia da Covid-19 desempenhou na prática do compartilhamento de dados através de nuvens e demais ferramentas, o presente trabalho pretende encontrar uma alternativa que corresponda a necessidade de uniformizar e atualizar as medidas de segurança cibernética para que a proteção à propriedade intelectual, bem como de dados e demais ativos armazenados no ciberespaço de empresas e demais setores da sociedade, se torne mais eficiente.

Para obter os resultados e respostas acerca da problematização apresentada neste trabalho, decidiu-se pelo método dedutivo. Sobre ele, aduz Matias-Pereira (2016, p. 49) que “O raciocínio dedutivo [...] Por intermédio de uma cadeia de raciocínio em ordem descendente, de análise do geral para o particular, chega a uma conclusão”.

Assim, pelo método dedutivo, a pesquisa se destinou, em um primeiro momento, a abordar o fenômeno da segurança cibernética e sua importância no

avanço da tecnologia para, a partir deste panorama, ser observado, na realidade do Brasil, os níveis de correspondência entre as medidas adequadas para se evitar esses tipos de ataque e seus desdobramentos na propriedade intelectual e como aperfeiçoar essa proteção.

Como método procedimental, optou-se pelo qualitativo. A esse respeito, Lakatos e Markoni (2017, p. 302) entendem que “desenvolve-se numa situação natural, oferecendo riqueza de dados descritivos, bem como focalizando a realidade de forma complexa e contextualizada”. Desta forma, os dados trabalhados na pesquisa foram oriundos de interpretações e observações viabilizadas pela pesquisa.

Para a obtenção de dados, optou-se pelas fontes primária e secundária, isto é, fontes de conteúdo original como artigos e dissertações e fontes consistentes em análises e avaliações daquelas, como livros e manuais; como meio de informação foi usada a modalidade bibliográfica com base em materiais já publicados, o que permitiu a construção de uma pesquisa, quanto aos objetivos, descritiva, posto levantar as boas práticas no Brasil e quais movimentos têm sido feitos em direção a maiores níveis de segurança cibernética, e explicativa, uma vez que visou esclarecer e demonstrar quais medidas podem contribuir para o sucesso na área.

Quanto à finalidade, produziu-se uma pesquisa aplicada no sentido de gerar conhecimentos para aplicação prática de medidas que promovam um ambiente cibernético mais seguro.

Quanto à abordagem, a pesquisa foi do tipo quantitativa, visando explicar através da investigação sistêmica do tema segurança cibernética, os impactos causados pela sua violação e as medidas a serem adotadas para evitá-los, culminando na tradução quantificada desses dados para classificá-los e assim, permitir uma análise mais precisa do quadro.

E por fim, considerando que foi desenvolvido um estudo sistematizado a partir de material publicado em livros e demais meios de maior acessibilidade como sites do governo, a pesquisa foi bibliográfica quanto aos procedimentos.

Contudo, considerando a escala constante de evolução que reveste o universo da tecnologia, cumpre destacar que em decorrência do avanço natural, os conceitos, estados da arte, teorias, definições e demais pensamentos aqui expressos, correm o risco de tornarem-se ultrapassados em momento futuro.

De forma sucinta, fica assim estabelecido:

1. Consulta aos dados bibliográficos encontrados em bases de dados

indexadas (Google Acadêmico; Periódicos Capes; Connected Papers; Academia.edu e Dialnet) e a informações públicas disponíveis nos sites oficiais das instituições;

2. Curadoria de conceitos básicos ao tema e das principais leis, normas e recomendações no combate às ameaças à segurança cibernética;

3. Verificação da compatibilidade e eficiência desses mecanismos na proteção da propriedade intelectual;

4. Utilização dos *softwares* Microsoft Excel® e Microsoft Word® para elaboração de planilhas, gráficos e tabelas;

5. Criação de um manual de boas práticas para salvaguardar os dados de propriedade intelectual no ambiente virtual.

6.3 RELAÇÃO ENTRE OBJETIVOS ESPECÍFICOS, METODOLOGIA E RESULTADOS

O levantamento dos dados da segurança cibernética no Brasil e o impacto econômico, social, político e tecnológico do cibercrime se deu a partir de uma pesquisa bibliográfica com o objetivo de contextualização do assunto, realizada através de buscas nas plataformas Google Acadêmico; Periódicos Capes, através do acesso CAFe, pelo login vinculado a Universidade de Brasília; Connected Papers ; Academia.edu; Dialnet e Planalto, site do governo federal que comporta todas as legislações atualizadas. A pesquisa foi feita a partir dos termos “cybersecurity+”, “Brasil+” e “ataques+” no campo de palavras-chave do título ou descrição. Utilizou-se o caractere de truncagem “+” para obtenção de variações das palavras e o operador booleano “AND” para obtenção de resultados cruzados entre os termos, isto é, entre as palavras-chave. Por fim, buscou-se dar preferência para resultados recentes, englobando o período de 2015 a 2022.

A identificação das medidas regulatórias que têm sido adotadas no combate e repressão ao cibercrime para identificar as lacunas existentes, foi realizada através de consulta a fontes primárias e secundárias de pesquisa, notadamente sites do governo federal e plataformas correlatas, como Planalto. Já para a detecção do que pode ser melhorado, foram aplicados meios de informação bibliográficos, contando para isto com o uso das plataformas acima citadas, quais sejam, Google Acadêmico; Periódicos Capes, através do acesso CAFe, pelo login vinculado a Universidade de Brasília; Connected Papers; Academia.edu e Dialnet, através dos termos “cibersegurança+”, “Brasil+” e “proteção+” no campo de palavras-chave ou descrição.

Utilizou-se o caractere de truncagem “+” para obtenção de variações das palavras e o operador booleano “AND” para obtenção de resultados cruzados entre os termos, isto é, entre as palavras-chave. Por fim, buscou-se dar preferência para resultados recentes, novamente englobando o período de 2015 a 2022.

Para a concepção de um manual explorando o aprimoramento, adaptação e desenvolvimento de mecanismos para a promoção de um ambiente cibernético mais seguro, foi utilizado o método dedutivo, de procedimento qualitativo e finalidade aplicada.

7. RESULTADOS ESPERADOS

O que se pretendeu com este trabalho foi contribuir, através da construção de um manual de boas práticas, para a orientação e promoção de um ambiente cibernético mais favorável e seguro para o avanço de tecnologias a partir de aplicações voltadas a cibersegurança que garantam a integridade da propriedade intelectual, para que assim o processo de inovação e seus colaboradores não restem prejudicados.

A partir de uma análise, portanto, do estado de coisas relacionado à segurança cibernética; do ambiente em que ela se situa, qual seja, o ciberespaço; e em como a questão tem sido abordada, foi possível construir um arcabouço teórico capaz de apontar as alternativas passíveis de serem adotadas para mitigar os riscos da presença *on-line*.

Como apresentado, o número de violações à segurança cibernética aumentou consideravelmente com o advento da pandemia da Covid-19, considerando principalmente o aumento das atividades *on-line* em decorrência das limitações sanitárias, incluindo a adoção da modalidade de trabalho remoto.

Assim, além do ambiente privado, o ambiente de trabalho, já sob constante ameaçã, tornou-se ainda mais vulnerável a essas ameaças, com vazamentos desde dados financeiros a segredos comerciais e propriedade intelectuais estratégicas para as empresas.

A partir de então, percebeu-se que um simples programa antivírus instalado na máquina não seria o suficiente para conter as invasões operacionalizadas através de *ransomwares*, *phishing*, *malwares*, entre outros, de modo que, a tempo, seria necessário instaurar uma verdadeira cultura de cibersegurança para ensinar aos operadores das esferas pública e privada como lidar com a manipulação de informações nesse ambiente.

Para a concretização dessa medida, passou-se a abordar o tema com a roupagem de política pública, inserindo-se na pauta normativa de diversos países, entre eles o Brasil, a questão da segurança cibernética.

Sem perder de vista a norma, o trabalho abordou também a dimensão ética da cibersegurança, dada a sua relevância por constar na base da determinação dos limites a serem impostos pela norma para garantir a segurança, a integridade e a eficácia das redes, sem deixar de lado os fatores inerentes às interações humanas e os direitos fundamentais dos indivíduos que cotidianamente a rede.

Foi verificado também que o impacto econômico que uma violação dessa natureza pode ter sobre uma empresa, principalmente quando essa empresa se posiciona no mercado através da tecnologia e inovação, é considerável, tendo em vista que é agregado um valor que gera riqueza não só para o ente privado, como para o Estado, que por sua vez passa a gozar do *status* de ambiente seguro ao desenvolvimento e á inovação.

Por essa razão, foi abordada também a responsabilidade civil pela violação da propriedade intelectual, uma vez que não só a prevenção “conta pontos” para a fixação desse *status*, mas também a certeza de contar com um aparato eficiente para lidar com qualquer infortúnio durante o processo.

Verificou-se, então, que ao ofendido cabe a recomposição do prejuízo sofrido, composto tanto pelo lucro perdido, quanto por aquele que ele deixou de auferir, na proporcionalidade cabível.

Foi a partir desse conjunto de informações e com o fito de disponibilizar à sociedade um material acessível sobre o assunto que o Manual de Boas Práticas em Cibersegurança foi elaborado.

8. DISCUSSÃO

A partir do referencial teórico levantado, foi possível detectar que a falta de um instrumento de disseminação de informação é o principal fator que contribui para o retardamento da adoção de uma cultura de cibersegurança no país.

A situação fática existe, mas o despreparo de organizações e pessoas físicas para lidar com os ataques posterga o avanço necessário e urgente no assunto.

O que se tem nos dias atuais equivale a um esforço conjunto em garantir um ponto de partida quando se discute segurança cibernética, contudo, pela própria natureza transmutacional do tema, esse esforço ainda se traduz em leis e medidas vagas e temorosas de caírem na obsolescência.

Ademais, a falta de familiaridade para com os institutos ligados à propriedade intelectual e sua relevância no avanço dos setores privado e público também representa uma barreira a ser ultrapassada para que a cibersegurança possa ser vista como um instrumento de proteção e prevenção voltado também à propriedade intelectual, e não apenas como um instrumento de contra-ataque.

A ausência de debate sobre os pontos que interceptam os dois assuntos (propriedade industrial e cibersegurança) também se mostra prejudicial a sua tutela, afinal, o conhecimento é o ponto de partida para um combate efetivo. Além disso, a construção da conduta ideal deve ser pautada por diretrizes adequadss à realidade dos interessados, que só pode ser conhecida através do diálogo.

É a fim de promover essa interação e conscientização que esse trabalho se destina, funcionando em um primeiro momento, como um compilado de como o Brasil e demais países estão lidando com a questão da segurança cibernética e, em um segundo momento, representado pelo manual de boas práticas e diretrizes para a proteção da propriedade intelectual de ameaças cibernéticas, como uma versão acessível à sociedade de medidas preventivas que podem ser adotadas.

9. IMPACTOS

De acordo com a Confederação Nacional da Indústria (CNI, 2016), a criação de padrões de cibersegurança está entre os desafios a serem enfrentados pelas indústrias. O pouco investimento que ainda existe por parte de empresas gera um ambiente exposto e propício à ataques e, embora haja um reconhecimento por parte de empresários e gestores da necessidade de investimentos no campo, a concretização desse planejamento ainda não atingiu níveis satisfatórios.

Para lidar com esses desafios e transpor essas barreiras, é indispensável que seja estimulada a conscientização e criados padrões de cibersegurança através de legislação, regulamentos e regras de governança de tecnologia e informação para que se estabeleça uma conduta uniforme e equânime que vise não apenas punir o ato, mas principalmente evitá-lo.

Para isso, a atuação multissetorial mostra-se de grande valia e vem sendo aplicada por diversas organizações, à exemplo do Departamento de Segurança da Informação e Comunicações (DSIC) em nível nacional, e da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que em nível internacional emprega esforços para estabelecer políticas de segurança cibernética em seus países membros a partir da ação conjunta de cinco atores: o setor público, o setor privado, o terceiro setor, as instituições de ensino superior e a sociedade (OPPERMANN, 2014).

Foi no intuito de contribuir com a construção dessa estrutura de apoio que este trabalho foi construído.

10. ENTREGÁVEIS DE ACORDO COM OS PRODUTOS DO TCC

Para a conclusão do referido mestrado profissional e obtenção do título de Mestre em Propriedade Intelectual e Transferência de Tecnologia para a Inovação, foram entregues o Trabalho de Conclusão de Curso (TCC) e um manual contendo boas práticas e diretrizes para a proteção da propriedade intelectual de ameaças cibernéticas.

11. CONCLUSÃO

Embora já familiar, a cibersegurança ainda necessita ser entendida e explorada com mais profundidade, tanto pelas organizações de direito privado, como pelas organizações de direito público. Por representar uma problemática que a cada dia se torna mais evidente a partir de sua relevância, abrangência e aspectos legais que invoca, torna-se urgente o investimento de recursos para tornar a segurança dos sistemas digitais satisfatória e efetiva.

A apresentação dos principais tópicos sobre segurança cibernética, incluindo os atributos legais, expõem o potencial de alcance dos danos que uma violação dessa natureza possui, podendo paralisar desde serviços essenciais à propriedades sutis, porém estratégicas, como os ativos de propriedade intelectual.

O sucesso em garantir a proteção de informações e dados contra ataques hostis passa necessariamente pela educação no mundo digital e pela adoção de boas práticas por parte daqueles que lidam com as informações. Para a concretização desse quadro, é necessário que a cibersegurança integre a agenda política de governo e seja de fato acolhida como uma prioridade para, então, ser difundida como uma cultura.

É na construção dessa realidade que a difusão de conhecimento se torna protagonista e que, pouco a pouco, se vai garantindo um ambiente seguro e estável para a propagação da propriedade intelectual e desenvolvimento da inovação.

12. PERSPECTIVAS FUTURAS

O cenário da cibersegurança no Brasil e no exterior mostra-se promissor, buscando, na medida do possível, acompanhar a realidade dos fatos. Contudo, a demora em aprovar medidas normativas (principalmente no Brasil) mostra-se prejudicial à tutela do interesse, uma vez que se trata de campo extremamente dinâmico.

Para além disto, verifica-se que cada vez mais tem se buscado integrar todos os países nos direcionamentos de boas práticas, postura absolutamente acertada dado o caráter transfronteiriço do ciberespaço.

A implementação de uma cultura em cibersegurança ainda tem como maior obstáculo as pessoas físicas e as empresas de menor porte, uma vez que esses atores acreditam (erroneamente) que por serem indivíduos simples e empresas de menor porte, não enfrentam risco de se tornarem alvos.

O consumo de conhecimento a respeito da segurança cibernética, infelizmente, ainda é mais comum após ser alvo de um ataque, motivo pelo qual o produto tecnológico produzido em decorrência desta pesquisa, qual seja, um Manual de Boas Práticas em Cibersegurança, visa, a partir de uma linguagem simplificada, alertar sobre os riscos e orientar os meios de evitá-los para, assim, contribuir com a evolução do cenário da segurança cibernética no país.

REFERÊNCIAS

ACQUISTI, Alessandro; TAYLOR, Curtis; WAGMAN, Liad. The economics of privacy. **Journal os economic literature**, v. 54, n. 2, p. 442-492, 2016.

AGÊNCIA BRASIL. **STF apura suspeita de ataque hacker e tira site oficial do ar**. 2021. Disponível em: https://agenciabrasil.ebc.com.br/justica/noticia/2021-05/STF-apura-suspeita-de-ataque-hacker-e-tira-site-oficial-do-ar. Acesso em: 12 out. 2021.

APARÍCIO, Marcelo. **O ciberespaço como dimensão de segurança**. 2017. 123 f. Dissertação (Mestrado em Aeronáutica Militar), Academia da Força Aérea, Sintra, Portugal, 2017.

AZZOLIN, Horácio. **O Marco Legal para os crimes cibernéticos**. Governança e Regulações da Internet na América Latina. 2018. Disponível em: https://www.gobernanzainternet.org/livro_portugues/gobernanza_y_regulaciones_de_internet_en_america_latina_pt.pdf. Acesso em: 16 set. 2021.

BARBOSA, Denis Borges. Valor indenizável das violações da Propriedade Intelectual. Disponível em: https://www.dbba.com.br/wp-content/uploads/valor_indenizavel.pdf. Acesso em: 22 dez. 2022.

BRASIL. Decreto nº 8.793/2016 de 29 de junho de 2016. Política Nacional de Inteligência. **Diário Oficial da União**, Brasília, DF, 30 de junho de 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm. Acesso em: 15 set. 2021.

BRASIL. Decreto nº 10.222/2020 de 5 de fevereiro de 2020. Estratégia Nacional de Segurança Cibernética. **Diário Oficial da União**, Brasília, DF, 6 de fevereiro de 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm. Acesso em: 12 ago. 2022.

BRASIL. Lei nº 9.279/1996 de 14 de maio de 1996. Lei de Propriedade Industrial. Diário Oficial da União, Brasília, DF, 15 de maio de 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9279.htm. Acesso em: 19 de dezembro de 2022.

BRASIL. Lei nº 10.406/2002 de 10 de janeiro de 2002. Código Civil. **Diário Oficial da União**, Brasília, DF, 11 de janeiro de 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 20 de dezembro de 2022.

BRASIL. Lei nº 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados. **Diário Oficial da União**, Brasília, DF, 15 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 out. 2021.

BRASIL. Lei nº 12.965 de 23 de abril de 2014. Marco Civil da Internet. **Diário Oficial da União**, 24 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 13 out. 2021.

BRASIL. Superior Tribunal de Justiça. **Recurso especial** n. 710.376/RJ. Relator: Ministro Luis Felipe Salomão. Quarta Turma. Julgado em: 15 dez. 2009. Dje, 02 fev. 2010.

BRASIL. Tribunal de Justiça de São Paulo**. Embargos de declaração** n. 994.07.017571-0/50000. Relator: Silvério Ribeiro. Quinta Câmara de Direito Privado. Julgado em: 02 jun. 2010. DJe, 14 jun. 2010.

BRASIL. Tribunal de Justiça do Rio Grande do Sul. **Agravo de instrumento** n. 70079819439. Relator: Luís Augusto Coelho Braga. Sexta Câmara Cível. Julgado em: 28 mar. 2019. Dje, 03 abr. 2019.

BURSSED, Ana Luiza de Campos. **As semelhanças e as diferenças nas abordagens das administrações Obama (2009-2016) e Trump (2017-2020) nas políticas de cibersegurança dos Estados Unidos**. 2021. 72 fls. Trabalho de Conclusão de Curso (Graduação em Relações Internacionais), Faculdade de Filosofia e Ciências de Marília, Universidade Estadual Paulista, São Paulo, 2021.

CARDOSO, Oscar Valente. A competência da Justiça Federal na Tutela dos Direitos da Propriedade Intelectual. **Revista CEJ**, Brasília, ano XII, p. 51-56, out/dez, 2008.

CERQUEIRA, João da Gama. **Tratado de Propriedade Industrial** – Volume II, Tomo I. São Paulo: Editora Revista dos Tribunais, 2ª edição, 1982.

CISCO. Security – Outcomes.

CNI. **Desafios para indústria 4.0 no Brasil.** Confederação Nacional da Indústria. Conselho Temático Permanente de Política Industrial e Desenvolvimento Tecnológico – COPIN. Brasília: CNI, 2016. 34 p. Disponível em: https://static.portaldaindustria.com.br/media/filer_public/d6/cb/d6cbfbba-4d7e-43a0-9784-86365061a366/desafios_para_industria_40_no_brasil.pdf. Acesso em: 16 set. 2021.

CONSELHO EUROPEU. Disponível em: https://www.consilium.europa.eu/pt/press/press-releases/2016/05/17/wide-cybersecurity-rule-adopted/. Acesso em: 17 set. 2021.

CORTEZ, Igor Siqueira; KUBOTA, Luis Claudio. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. **Revista de Administração (São Paulo)**, v. 48, p. 757-769, 2013.

COTINO, Lorenzo; SÁNCHEZ, Marco. **Guia de cibersegurança para cidades inteligentes**. Tradutor: Marsel de Souza. Washington: BID, dezembro de 2021, 107 págs.

CRIPTOID. **Cibersegurança no novo normal: como a Covid-19 mudou a segurança digital para sempre.** 2021. Disponível em: https://cryptoid.com.br/seguranca-da-informacao-identidade-digital/ciberseguranca-no-novo-normal-como-a-covid-19-mudou-a-seguranca-digital-para-sempre/. Acesso

em: 11 set. 2021.

CYBERCRIME MEGAZINE. **Cybercrime To Cost The World $10.5 Trillion Annually By 2025**. 2020. Disponível em: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/?utm_source=angellist Acesso em: 11 set, 2021.

CYBER REVIEW 2019. JLT BRASIL. Disponível em: <http://www.brasil.jlt.com/midia/noticias-e-releases/2019/04/nova-edicao-cyber-view-2019>. Acesso em 12 de ago. 2022.

DA GRAÇA, Ronaldo Bach. Enfoque Jurídico da Defesa Cibernética Aplicada às Sociedades Empresárias. **Revista Brasileira de Direito Empresarial**, v. 1, n. 1, p. 231-254, 2015.

DA SILVA, Júlio Cezar Barreto Leite. Guerra cibernética: a guerra no quinto domínio, conceituação e princípios. **Revista da Escola de Guerra Naval**, v. 20, n. 1, p. 193-211, 2014.

DALLA FAVERA, Rafaela Bolson; DA SILVA, Rosane Leal. Cibersegurança na União Europeia e no Mercosul: Big Data e Surveillance Versus Privacidade e Proteção de Dados na Internet. **Revista de Direito, Governança e Novas Tecnologias**, v. 2, n. 2, p. 112-134, 2016.

DI REZENDE BERNARDES, Marcelo. Os princípios éticos e sua aplicação no Direito. **Revista Eletrônica do Ministério Público do Estado de Goiás**, n. 2, p. 29-42, 2012.

DONEDA, Danilo; MENDES, Laura Schertel. Um perfil da nova Lei Geral de Proteção de Dados brasileira. **Governança e Regulações da Internet na América Latina**. 2018. E-book. 558 p. Disponível em: https://www.gobernanzainternet.org/livro_portugues/gobernanza_y_regulaciones_de_internet_en_america_latina_pt.pdf. Acesso em: 16 set. 2021.

GIBSON, William. **Burning Chrome**. Ed. Harper Voyager. Londres, Inglaterra. 1982.
_____. **Neuromancer**. São Paulo: Editora Aleph, 1984.

GOMES, Rita de Cássia Medeiros. O direito e a propriedade intelectual: constitucionalização, campo de atuação e responsabilidade a violação do direito. **PIDCC – Revista de Propriedade Industrial-Direito Contemporâneo e Constituição**, Aracajú, ano IX, v.1, n. 01, p. 60-82, 2020.

GONÇALVES, Carlos R. Direito Civil Brasileiro – Volume 4. São Paulo: Editora Saraiva, 2022. E-book. ISBN 9786555596144. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555596144/. Acesso em: 20 dez. 2022.

GONÇALVES, Rita Santos. **O fator humano da cibersegurança nas organizações**. 2019. 62f. Dissertação (Mestrado em Gestão de Sistemas de Informação), Universidade de Lisboa, Lisboa, 2019.

GOUVEIA, Jorge Bacelar. Direito do Ciberespaço e Segurança Cibernética. **Revista Jurídica Portucalense**, n. 29, p. 59-77, 2021.

KEMPFER BASSOLI, Marlene; FORTES, Fellipe Cianca. Análise econômica do direito tributário: livre iniciativa, livre concorrência e neutralidade fiscal. **Scientia iuris**, v. 14, p. 235-253, 2010.

LAKATOS, Eva Maria; MARCONI, Maria de Andrade. **Metodologia Científica, 7ª edição**. São Paulo: Grupo GEN, 2017.

LEITÃO, Luis Manuel Teles Menezes. **Direito das Obrigações** – Volume I. São Paulo: Editora Almedina, 15ª edição, 2018.

LEMOS, André et al. Câmeras de vigilância e cultura da insegurança: percepções sobre as câmeras de vigilância da UFBA. **ALCEU**, v. 12, n. 23, p. 143-153, 2011.

LIMA, Gabriela Eulalio de. Ciberataques: uma reflexão sobre a responsabilidade internacional dos Estados. **Caderno de Relações Internacionais**, v. 8, n. 15, p. 201-221, 2017.

LIMA, William Custodio. **O tratamento de dados pessoais em perspectiva comparada entre União Europeia e Brasil: o papel da autoridade nacional de proteção de dados como instrumento para a tutela de direitos fundamentais**. 2020. 108 f. Dissertação (Mestrado em Direito), Centro de Ciências Sociais e Humanas, Universidade Federal de Santa Maria, Rio Grande do Sul, 2020.

MATIAS-PEREIRA. **Manual de Metodologia da Pesquisa Científica, 4ª edição**. São Paulo: Grupo GEN, 2016.

MATOS, Pedro Carvalhais de Abreu. **Cibersegurança: políticas públicas para uma cultura de cibersegurança nas empresas**. 2018. 117 f. Dissertação (Mestrado em Economia e Políticas Públicas), Escola de Ciências Sociais e Humanas, Instituto Universitário de Lisboa, Lisboa, 2018.

NUNES, Paulo. A definição de uma estratégia nacional de cibersegurança. **Nação e defesa**, v. 133, n. 5, p. 113-127, 2012.

OBSERVATÓRIO DE CIBERSEGURANÇA. **Relatório de cibersegurança em Portugal:** ética e Direito. Portugal: CNCS, 2020
_____. **Relatório Cibersegurança em Portugal Economia**. Portugal: CNCS, 2022.

OPPERMANN, Daniel. Governança da internet e segurança cibernética no Brasil. **Monções: Revista de Relações Internacionais da UFGD**, v. 2, n. 4, p. 259-283, 2014.
_____. O cenário de cibersegurança depois de Snowden e consequências no Brasil. **JANUS 2014-Metamorfoses da violência (1914-2014)**, p. 148-149, 2014.

PINHEIRO, Patricia. Peck. **Segurança Digital - Proteção de Dados nas**

Empresas. São Paulo: Grupo GEN, 2020.

PROFNIT. **Cartilha PROFNIT de produtos Técnico-tecnológicos e Bibliográficos**. 2019.

RODRIGUES, Francisco José Lucas. Principais ameaças no contexto da cibersegurança. **Centro de Investigação & Desenvolvimento sobre Direito e Sociedade**, v. , n. 48, 2016.

SERRANO, Inês Isabel Balão. Cibersegurança na União Europeia: a ciberdiplomacia como ferramenta política de gestão e prevenção de conflitos. 2022. 98 f. Dissertação (Mestrado em Rerlações Internacionais e Estudos Europeus), Escola de Ciências Sociais, Universidade de Évora, Évora, 2022.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Em razão de ataque cibernético, STJ funcionará em regime de plantão até o dia 9**. 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04112020-Em-razao-de-ataque-cibernetico--STJ-funcionara-em-regime-de-plantao-ate-o-dia-9.aspx. Acesso em: 12 out. 2021.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial** n. 710.376/RJ, relator Ministro Luis Felipe Salomão, Quarta Turma, julgado em 15/12/2009. Dje, 02 fev. 2010.

TARTUCE, Flávio. **Responsabilidade Civil**. São Paulo: Grupo GEN, 2022. E-book. ISBN 9786559645251. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559645251/. Acesso em: 20 dez. 2022.

TENE, Omer; POLONETSKY, Jules. **Privacy in the age of big data:** a time for big decisions. Stan. L. Ver. Online, 2011, vol. 64, p.63.

TERESO, Marco; PRATAS, Antônio. Cibersegurança e teletrabalho: um mundo de oportunidades de risco. **Atas do VII Encontro Científico da UI&D (ecUI&D)**, p. 126-136, 2021.

APÊNDICE A – Matriz FOFA (SWOT)

APÊNDICE B – Modelo de Negócio CANVAS

<table>
<tr>
<td rowspan="2">Parcerias Chave

Orientadora e professores do PROFNIT</td>
<td>Atividades Chave

- Pesquisa bibliográfica;
- Análise de normas e dados;
- Elaboração de um manual de boas práticas.</td>
<td rowspan="2">Proposta de Valor

- Ofertar um ambiente cibernético mais seguro no Brasil</td>
<td>Relacionamento

Manual prático e funcional</td>
<td rowspan="2">Segmento de Clientes

- Empresas, setor público e sujeitos que tenham interesse em proteger suas criações intelectuais de ataques cibernéticos.</td>
</tr>
<tr>
<td>Recursos Chave

- Revistas de produção acadêmica;
- Sítios oficiais de governos na internet;
- Livros.</td>
<td>Canais

- Site do PROFNIT/UnB.</td>
</tr>
<tr>
<td colspan="3">Estrutura de Custos

Custo relativo à edição do manual, caso haja necessidade de contratação de serviço especializado.</td>
<td colspan="2">Fontes de Receita

Oriundo da própria mestranda.</td>
</tr>
</table>

APÊNDICE C – Artigo submetido à publicação

INTELIGÊNCIA ARTIFICIAL NO JUDICIÁRIO

RESUMO

O artigo em apreço visa apresentar as mudanças contemporâneas no uso de novas tecnologias nas atividades do judiciário. Insta discutir a posição contemporânea e a situação do judiciário e como ela pode ser melhorada com o uso da tecnologia LegalTech. A fim de elucidar esta problemática de pesquisa a pergunta central é: de que forma a democracia digital pode contribuir para o aperfeiçoamento dos julgamentos, do controle social de políticas públicas? A inovação como política pela qual o Estado opta beneficiará os mecanismos da democracia participativa? A partir do presente estudo, foi possível concluir que, a partir do alinhamento da Tecnologia Artificial e dos recursos da tecnologia da informação e comunicação (TICs), a democracia participativa pode caminhar no mesmo sentido e aumentar o grau de alcance dos seus mecanismos participativos e de controle e reduzir ou eliminar obstáculos existentes pela sua forma tradicional de exercício.

Palavras-chave: Judiciário; Inteligência Artificial; Democracia participativa.

ARTIFICIAL INTELLIGENCE IN THE JUDICIARY

ABSTRACT

The present article aims to present contemporary changes in the use of new technologies in the activities of the judiciary. It urges to discuss the contemporary position and the situation of the judiciary and how it can be improved with the use of LegalTech technology. In order to elucidate this research problem, the central question is: how can digital democracy contribute to the improvement of judgments, of social control of public policies? Will innovation as a policy by which the State chooses to benefit the mechanisms of participatory democracy? From this study, it was possible to conclude that, from the alignment of Artificial Technology and the resources of information and communication technology (ICTs), participatory democracy can move in the same direction and increase the extent of its participatory and control mechanisms and reduce or eliminate existing obstacles through its traditional form of exercise.

Keywords: Judiciary; Artificial intelligence; Participatory democracy.

INTRODUÇÃO

O uso da Inteligência Artificial (IA), está cada vez mais difundido entre os diversos campos de atuação e é apontado como protagonista nos processos de inovação, de modo que não se trata mais de "se", mas de "quando", principalmente na área jurídica.

Contudo, para melhor compreender as temáticas que cercam o tema hoje, é necessário, em primeiro lugar, abordar o conceito de IA, embora uma formulação exata seja ainda um desafio. Para John McCarthy, um dos primeiros a empregar a expressão "Inteligência Artificial", IA é:

> […] a ciência e engenharia de fazer máquinas inteligentes, especialmente programas inteligentes de computador. Está relacionado à tarefa semelhante de usar computadores para entender a inteligência humana, mas a IA não precisa se limitar a métodos biologicamente observáveis. [tradução nossa] (2007)[1]

Para Urwin (2019, p. 92), "inteligência artificial é uma ferramenta construída para auxiliar ou substituir o pensamento humano"[2]. E para Wildisen (2015) "IA é a teoria e o desenvolvimento de sistemas de computador que irão realizar tarefas que normalmente requereriam inteligência humana"[3].

Portanto, é possível através dos três conceitos apresentados, perceber um escalonamento na compreensão da dimensão da IA. Para McCarthy, trata-se basicamente de uma ferramenta inteligente; já Urwin atribui a essa ferramenta a tarefa de auxiliar ou substituir o pensamento humano; enquanto Wildisen já insere a ideia de máquina substituindo o homem nas tarefas que lhe competem. E essas percepções vão sofrendo ajustes e reconsiderações conforme o avanço da tecnologia, daí a dificuldade em se fechar um conceito.

Por sua vez, para a ciência do Direito, IA é a capacidade de atuação racional com o objetivo de realizar predições, o que vai acontecer a partir do uso de algoritmos, que na definição de Pedro Domingos, é uma sequência de instruções que diz a um computador o que fazer (DOMINGOS, 2015, p. 2). Quanto ao seu funcionamento, os algoritmos podem ser definidos em duas espécies: os programados e os não programados.

Os algoritmos programados seguem as operações definidas, de modo que a informação é adicionada ao sistema, o algoritmo trabalha essa informação e o resultado (*output*) é gerado. Já os algoritmos não programados, conhecidos por usarem a técnica *machine learning*, operam de modo que os dados e o resultado desejado são carregados no sistema (*input*), que por sua vez produz o algoritmo (*output*) que transforma um no outro (FERRARI; BECKER, 2017). Então, é formada uma cadeia de aprendizagem da máquina onde ela vai criando a própria programação.

A forma mais conhecida de *machine learning* é aquela que emprega algoritmos supervisionados, na qual

---

[1] "It is the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable." McCARTHY, John. **What is Artificial Intelligence?** Stanford University: Revised November 2007. Não paginado. Disponível em: <http://www-formal.stanford.edu/jmc/whatisai/whatisai.html>. Acesso em: 16 mar. 2021.

[2] "[...] artificial intelligence is a tool constructed toa id or substitute for human thought." URWIN R. **Artificial Intelligence**: The Quest for the Ultimate Thinking Machine. London: Arcturius, 2016. Arquivo Kindle, p. 92.

[3] "AI is the theory and development of computer systems which will perform tasks that normally require human intelligence." WILDISEN, Greg. Is artificial intelligence the key to unlocking innovation in your law firm? Legal Week, 12 Nov. 2015. Não paginado. Disponível em: <https://www.law.com/international-edition/2015/11/12/is-artificial-intelligence-the-key-to-unlocking-innovation-in-your-law-firm/?slreturn=20210216150814>. Acesso em: 16 mar. 2021.

o sistema é alimentado com dados selecionados por seres humanos. Um exemplo são as redes neurais artificiais (com *back propagation*). Como o próprio nome sugere, são espelhadas no cérebro humano e têm um modelo de aprendizagem baseado em erros e acertos que vai, progressivamente, detectando as decisões mais alinhadas com os objetivos que se pretende atingir. Nestes casos, o sistema é carregado com um objetivo (*output*) e diversos *inputs*, que serão testados em múltiplos cenários. Quando se atinge o resultado almejado, o roteiro mais eficiente recebe um peso na programação e, dessa forma, as camadas neurais internas (*hidden layers*) mais assertivas passam a dominar a tarefa e a entregar resultados mais precisos (RUMERLHART; HILTON; WILLINANS, 1986, p. 533).

Uma segunda categoria é a dos algoritmos não supervisionados. Nesse grupo, os dados que alimentam o sistema não são rotulados, deixando o algoritmo de aprendizagem encontrar estrutura nas entradas fornecidas por conta própria. Pode ser utilizado tanto como um objetivo em si mesmo, quanto como um meio para atingir um fim.

Há ainda uma terceira categoria que se refere aos algoritmos de reforço (*reinforced learning algorithms*), que são treinados para tomar decisões. Os acertos ou erros do *output* são computados e utilizados para refinar o algoritmo, focando na performance.

Essa sofisticação dos algoritmos de *machine learning* ilustra a capacidade e o nível de evolução tecnológica já alcançada pela sociedade, mas também gera novas demandas aos principais atores no campo da inovação, notadamente, governos, indústrias e universidades.

METODOLOGIA OU ESCOPO

Para realização da pesquisa, adotou-se como metodologia científica a dedução, a partir de técnica de pesquisa bibliográfica e documentação indireta. Foi realizado aporte teórico acerca dos conceitos que envolvem a Inteligência Artificial, o uso de robôs, bem como o estudo das formas que se manifestam através da utilização de recursos tecnológicos nesses espaços, especialmente, nos julgamentos, e efetivação de políticas públicas.

Para o levantamento bibliográfico foram realizadas buscas nas plataformas Google Acadêmico; Periódicos Capes, através do acesso CAFe, pelo login vinculado a Universidade de Brasília; Connected Papers ; Academia.edu e Dialnet. Além disso, os autores realizaram pesquisas em páginas do governo do Brasil ligados à segurança e informação, nomeadamente Ministério da Defesa e Governo Digital.

A pesquisa foi feita a partir dos termos “IA+”, “judiciário+” e “inovação+” no campo de palavras-chave do título ou descrição. Utilizou-se o caractere de truncagem “+” para obtenção de variações das palavras e o operador booleano “AND” para obtenção de resultados cruzados entre os termos, isto é, entre as palavras-chave. Por fim, buscou-se dar preferência para resultados recentes.

RESULTADOS E DISCUSSÃO

No ano de 2013, em Wisconsin, EUA, ocorreu o caso que se tornaria paradigmático à discussão do uso de IA e seus limites. Em fevereiro do referido ano, após furtar um veículo, ser perseguido pela polícia e se envolver em um tiroteio, Eric Loomis foi preso em flagrante. Ao ser levado à presença de um juiz, determinou-se que respondesse ao processo em liberdade e, posteriormente, em seu julgamento, como resultado dos atos descritos somados a um passado já conhecido pela justiça, foi condenado a seis anos de prisão.

O que chamou atenção no caso foi o fato de a negativa da liberdade provisória e o patamar aumentado da pena terem sido definidos a partir do parecer de que Loomis apresentaria alto risco de violência, reincidência e evasão. Entretanto, esse parecer não foi emitido pelo juiz da causa, mas sim por um software de origem privada chamado COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), que à época, era alugado pelo Poder Judiciário e que funcionava a partir de um algoritmo secreto, ao qual os julgadores não tinham acesso, o que não impediu, entretanto, que a decisão pela prisão de Loomis fosse fundamentada apenas com base no resultado do algoritmo (ISRANI, 2017).

A defesa, diante de tal resultado, recorreu à Suprema Corte de Winsconsin, requerendo o acesso aos critérios que levaram o software a classificá-lo como uma pessoa de alto risco, ao que obteve uma resposta negativa sob o fundamento de que a questão ainda não estaria madura para julgamento por se tratar de tema ainda muito recente. Desta forma, foi negado a Loomis pela justiça acessar o código-fonte do algoritmo, e na mesma linha, os representantes legais da Northpointe Inc. (atualmente, Equivant), desenvolvedora do COMPAS, defenderam que a forma de operação do sistema estaria protegida por segredo industrial.

Ainda durante o julgamento na Suprema Corte de Wisconsin, através de um relatório emitido pela ONG ProPublica, se descobriu que o COMPAS era enviesado contra afro-americanos (ANGWIN, 2016). Mas, apesar desse exemplo de distorção no viés do algoritmo, a Suprema Corte de Winsconsin negou o recurso de Loomis, declarando que a sentença recebida por ele seria a mesma que pudesse porventura decorrer de uma avaliação humana. Loomis, então, recorreu à Suprema Corte Americana, apresentando o *writ of certiorari*, que também foi negado.

O caso em questão ilustra o papel de agente decisório que os sistemas de IA podem chegar a protagonizar na sociedade e seus impactos. Com essa nova realidade sendo implementada em diversos setores, novos questionamentos e desafios surgem, reforçando a necessidade de uma sólida base regulatória que dê segurança aqueles que podem vir a ser atingidos pelo desempenho dessa tecnologia e que assegure um patamar de responsabilização pelas decisões tomadas por meio de máquinas.

Um dos aspectos que geram preocupação é a opacidade que surge através da janela entre a programação humana na base do algoritmo e o comportamento autônomo desenvolvido por este, de modo a criar a própria programação.

> [...] os problemas relacionados à falta de transparência dos processos e os resultados viciados por dados de baixa qualidade vêm levantando muitas discussões e preocupam a comunidade jurídica (SANTOS; PEREIRA; GANDRA, 2019).

Sobre o problema da opacidade/transparência, analisa Joshua A. Kroll (2018, p. 9):

> O antídoto natural para a opacidade é a transparência, e a transparência é frequentemente citada como, pelo menos, um componente de uma solução para problemas de governar sistemas de computador. Embora transparência seja muitas vezes tomada para significar a divulgação de código-fonte ou dados, [...], isso não é necessário nem suficiente para melhorar a compreensão de um sistema, e não captura o significado completo de transparência [...] a transparência exige uma mistura de entendimento de como um sistema funciona, de entender por que ele funciona dessa maneira e de uma percepção por parte das pessoas afetadas de que os mecanismos e processos de um sistema funcionam para atingir os objetivos corretos. [tradução nossa][4]

Logo, é possível inferir do trecho citado acima que a mera divulgação de código-fonte, por si só, mostra-se apenas parcialmente eficaz aos fins pretendidos, pois o código de programação dos algoritmos que

[4] "The natural antidote to opacity is transparency, and transparency is often cited as at least a component of a solution to problems of governing computers systems. While transparency is often taken to mean the disclosure of source code or data, [...], this is neither necessary nor sufficient for improving understanding of a system, and it does not capture the full meaning of transparency [...] transparency demands a mix of understanding how a system works, understanding why it works in that way, and a perception on the part of affected people that the mechanisms and processes of a system function to achieve the correct goals. To that end, sufficient transparency may simply mean disclosing the fact and scope of data processing in a computer system, as is required by the GDPR in the EU. However, When transparency is demanded, it is important to be clear over what transparency is required na to whom that transparency is intended." KROLL, Joshua A. the fallacy of inscrutability. Philosophical Transactions of the Royal Society, London, n. 376, p. 9, 2018. Disponível em: https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0084. Acesso em: 20 mar. 2021.

operam em *machine learning* carregam tão somente as regras de aprendizagem do *software*, e a decisão surge da interação entre essas regras e os dados. Motivo pelo qual a IA está em constante mudança e qualquer acesso tornar-se-ia obsoleto dali a semanas.

Relacionado ao conflito da opacidade, surge a problemática do viés do algoritmo, uma vez que este, a partir dos dados coletados, aprende e replica o que está acontecendo na sociedade, gerando, por vezes, padrões enviesados de dados. A esse respeito

> Sem controle da qualidade desses dados, estamos sujeitos a codificar nossos preconceitos e vieses. A inteligência artificial criada por *machine learning* não deixa de ser, por isso, uma extensão da cultura e do senso comum. (FERRARI; BECKER, 2017, p. 01)

Portanto, a ausência de controle sobre a qualidade desses dados, pode gerar sérias consequências, inclusive de ordem ética.

> [...] algoritmos muitas vezes criam ou acentuam assimetrias de poder e oportunidades, afetam a meritocracia e induzem resultados, de modo que a regulamentação deve garantir que seu uso não seja traduzido em decisões ou diretrizes de política pública injustas e ilegais. (COUTINHO; KIRA, 2019, p. 01)

Pelas implicações que as questões éticas da IA podem gerar, no ano de 2020 foram investidos US$ 186 milhões em empresas que exploram questões éticas da IA e oferecem ferramentas para identificar e remover esses vieses e, entre dezembro de 2020 e maio de 2021, esse valor já alcança US$ 100 milhões (ESTADÃO, 2021). Startups e grandes empresas do setor da tecnologia tem se empenhado em desenvolver soluções para esse problema e a tendência é que os movimentos regulatórios acompanhem a questão.

Assim, tais facetas da IA (dentre outras), impulsionam um esforço, em especial da esfera jurídica, no sentido de regular, mas sem cercear, a disponibilidade de meios e estruturas para desenvolver a IA. Neste sentido, tem se observado uma onda de inciativas regulatórias por parte de diversos países a fim de estabelecer uma relação harmônica entre a promoção de inovação e os direitos individuais e coletivos, sem violar os direitos constitucionais (POSNER, 2014).

Neste sentido, por apresentarem maior maleabilidade e capacidade de abordarem temas ainda incertos e em constante construção através de relatórios, recomendações e resoluções em geral, cada vez mais tem-se levantado a possibilidade de trazer do Direito Internacional para o campo da tecnologia e inovação a figura das normas denominadas *soft laws.* Sobre esse mecanismo

> [...] diante da dificuldade em manter-se um sistema normativo atualizado - e credível - a soft law permite que atores estatais (e não estatais) desenvolvam compromissos com uma margem de flexibilidade que a hard law não possui. (GREGÓRIO, 2016, p. 5)

Outra vantagem desse sistema seria a maior agilidade em promover as negociações e alterações necessárias visando o acompanhamento dos avanços nos setores. Contudo, a ausência de força coercitiva destas normas deve ser levada em consideração, desta forma, observa-se que seu potencial está concentrado em instigar nas nações a boa vontade para desenvolver políticas de cooperação e em funcionar como estímulo e inspiração para medidas legislativas internas mais rígidas.

Em maio de 2018, o Comitê de Ciência e Tecnologia da *House of Commons* do Reino Unido, publicou o parecer "*Algorithms in decison-making*" (2018), fruto da inquietação quanto à repercussão jurídica, política e social do crescimento de inovações e tecnologias que tem propiciado a tomada de decisões algorítmicas. Pavlich (2011, p. 168) infere acerca do que tais desenvolvimentos podem significar para o futuro do campo do direito e da sociedade demarcado pela jurisprudência, a sociologia do direito, os estudos sociojurídicos.

Na oportunidade, o governo do Reino Unido apresentou ao Comitê o plano para a criação do "*Centre for Data Ethics and Innovation*", cujo objetivo será a "supervisão do futuro desenvolvimento de algoritmos e das 'decisões' que eles tomam" (LONDON, 2021).

Em outubro de 2020, Margrethe Vestager, comissária digital e antitruste da União Europeia, comunicou as novas regras dirigidas às plataformas digitais com vultuosa base de dados e negócios lucrativos de publicidade *online*, com o fim de esclarecer o funcionamento dos algoritmos e de fornecer a pesquisadores e agentes reguladores acesso aos dados e aos arquivos de anúncios (FORBES, 2020).

Na mesma direção, complementando o pacote de ações para promover um espaço digital mais seguro e transparente na União Europeia, que possibilite a responsabilização por atos em desacordo com direitos fundamentais e boas práticas de mercado, foram lançados os programas *Digital Services Act* e *Digital Markets Act* (EC.EUROPA).

Focado nas questões éticas, em 2019 foi relançado pela União Europeia o "*Ethics guidelines for trustworthy AI*", no qual a organização fazendo uma intersecção entre os campos da moral, da ética e da IA, estabelece diretrizes para a construção de uma IA confiável e alinhada às necessidades humanas e ao bem comum. Neste sentido, estabelece o guia

> IA confiável tem três componentes [...]: (1) deveria ser legal, cumprindo todas as leis e regulamentos aplicáveis (2) deveria ser ética, garantindo cumprimento a princípios e valores éticos e (3) deveria ser robusta, tanto do ponto de vista técnico quanto social, já que, mesmo com boas intenções, sistemas de IA podem causar danos não intencionais. [tradução nossa] (ETHICS GUIDELINES FOR TRUSTWORTHY AI, 2019, p. 2)

A política de tecnologia e inovação vem sendo um processo de real intensificação na União Europeia, com a missão de que inovar é preciso (BIJOS; NASCIMENTO, 2019, p. 53)

No Brasil, por sua vez, foi elaborada a Lei Geral de Proteção de Dados Pessoais (LGPD, 2018), Lei nº 13.709 de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica de direito público ou privado, com o fim de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Isto é, a LGPD surgiu como uma ferramenta de tutela coletiva para a proteção de direitos individuais e promoção de modelos econômicos. Para efetivar essa proteção, foi criada também a Autoridade Nacional de Proteção de Dados (ANPD).

Percebe-se, portanto, um movimento conjunto por parte de países e blocos em tutelar a evolução da implementação da IA no cotidiano, de modo que ela se torne uma aliada, e não uma ameaça. Com a internacionalização dos direitos humanos, cumpre ao Estado proteger o direito dos indivíduos, que estão acima dos direitos do Estado e independem do status de cidadão de um Estado particular (AMARAL JUNIOR, 2015, p. 206).

CONCLUSÃO

Como marcos conclusivos ressaltamos o impacto da utilização da Inteligência Artificial (IA) em tribunais nacionais e internacionais. Os processos em questão balizam a funcionalidade e a situação atual da tecnologia através da sua crescente integração com esses sistemas.

O impacto gerado pela IA no judiciário compreende a identificação, leitura e análise inteligente de documentos e imagens. Através da implementação de processos inteligentes será possível verificar a integridade, a celeridade e a transparência na condução dos julgamentos. Portanto, fica evidente não se tratar de um vilão que, a qualquer custo, pretende tomar o lugar do julgador humano, mas sim, de uma

ferramenta valiosa no auxílio das atividades cotidianas que, quando delegadas aos operadores da justiça, exigem tempo e dedicação que poderiam ser melhor aplicados em tarefas de maior complexidade que de fato exigem o atuar que somente o ser humano é capaz de suprir.

O resultado final apontará os relevantes benefícios para tornar a justiça mais efetiva, visando ao bem-estar social dos cidadãos envolvidos e do sistema judiciário como um todo, sem relegar a segundo plano a importância de um sistema regulatório eficaz que promova um ambiente seguro a todas as partes envolvidas neste processo de adaptação tecnológica.

PERSPECTIVAS FUTURAS

Outra faceta da promoção de inovação, para além das ferramentas de defesa e incorporação de novas tecnologias, é a inovação como política pela qual o Estado opta, conforme entrevista do Embaixador Lewi de Israel no Paraguai (LEWI, 2017). Isto é, a inovação como parte da agenda política de um país. A partir desse ideal, surge a ideia de GovTech, aliando a tecnologia a demandas governamentais.

Com a aplicação deste processo, a Estônia tornou-se referência em governo digital. Com isso, os cidadãos podem acessar a maioria dos serviços públicos *online*, deixando a burocracia de filas e longos prazos no passado. Dado o alto tráfego de dados, a arquitetura de informação também passou por transformações.

> Na Estônia, é utilizado uma sistema chamado X-Road, uma camada de dados distribuídos sem um banco de dados central e cujas informações só podem ser acessadas com a autenticação de dois fatores. Cada agência governamental administra seus próprios dados e acessa aqueles que lhe são pertinentes conforme a necessidade e as possibilidades de acesso oferecidas pelo sistema. Isso garante privacidade, evitando que pessoas não autorizadas possam ver ou copiar os dados de outras pessoas, e também integridade, de modo que os dados não possam ser alterados maliciosamente. (GOVTECH BRASIL, 2018).

Apesar da discrepância em proporção, a Índia também tem trabalhado sobre essas bases e obtido êxito desde 2010. A partir da criação do *Aadhaar*, foi possível mapear e incluir pessoas que até então estavam fora do radar, na vida econômica e no acesso a tecnologias de comunicação. Outra medida importante foi a redução do uso de dinheiro vivo a partir de uma interface de pagamento unificada. Quanto à arquitetura de informação para suportar tal conjunto, o país também defende o uso de um sistema em camadas, ao contrário de uma arquitetura monolítica, reproduzindo um sistema já ultrapassado (INDIA, 2018).

Outro exemplo de sucesso no processo de inovação é Israel, com o diferencial de que, para alcançar êxito, o país optou por estimular o crescimento de todo o ecossistema por meio de financiamentos e aproximação entre os interesses governamentais e startups focadas no desenvolvimento de novas tecnologias (LEVY, 2017). Aliado a isso, a peculiaridade de ser um país jovem, cercado por conflitos, com uma população de imigrantes que, independentemente do sexo, obrigatoriamente cumprem o serviço militar, de modo a proporcionar aos cidadãos vasta experiência em tomadas de decisão, liderança e estratégia, além de diminuir barreiras sociais, dada a atuação na mesma unidade de pessoas provenientes de contextos sociais diversos, fazem o perfil do povo de Israel ser compatível com as qualidades necessárias para o empreendedorismo e a inovação (LEWI, 2018).

Nesta escalada rumo à inovação integrada a prestação do serviço público, o Brasil vem avançando de forma contínua com auxílio das TICs e se aproximando cada vez mais do ideal de um governo plenamente integrado às tecnologias disponíveis (conforme demonstra a imagem abaixo) e, a exemplo de Israel, também vem se aproximando do setor das startups como forma de alavancar a eficiência do serviço público, como deixa claro a Lei Complementar nº 182/2021, conhecida como o Marco Legal das Startups e do Empreendedorismo Inovador.

Gráfico 1: Linha do tempo – Governo Eletrônico

Fonte: Governo Digital (2021)

Para atingir esse objetivo, como não poderia deixar de ser, o Brasil também já se utiliza da tecnologia de IA no serviço público. Notadamente no judiciário, recebeu destaque em 2018, a implementação do robô VICTOR, IA nascida de uma parceria entre a Universidade de Brasília e o Supremo Tribunal Federal com o fito de dinamizar a tramitação de processos com temas de repercussão geral sob sua jurisdição:

> O objetivo inicial é aumentar a velocidade de tramitação dos processos por meio da utilização da tecnologia para auxiliar o trabalho do Supremo Tribunal. A máquina não decide, não julga, isso é atividade humana. Está sendo treinado para atuar em camadas de organização dos processos para aumentar a eficiência e velocidade de avaliação judicial. Os pesquisadores e o Tribunal esperam que, em breve, todos os tribunais do Brasil poderão fazer uso do VICTOR para pré-processar os recursos extraordinários logo após sua interposição (esses recursos são interpostos contra acórdãos de tribunais), o que visa antecipar o juízo de admissibilidade quanto à vinculação a temas com repercussão geral, o primeiro obstáculo para que um recurso chegue ao STF. Com isso, poderá impactar na redução dessa fase em 2 ou mais anos (STF, 2018).

Apesar de representar um avanço, o robô VICTOR gerou na sociedade desconfiança, principalmente quando contraposto ao aspecto do viés da máquina (tendência de adesão por parte do ser humano à sugestão dada pelo *software*). Entretanto, é inegável que ele representa uma tendência, reforçando a necessidade de aliar os movimentos de inovação às leis, sistemas e processos que regulem o acesso e o uso dessas tecnologias.

Ainda, outros Tribunais do país têm recorrido ao auxílio desta inteligência em razão da celeridade que ela proporciona. Por exemplo, o Tribunal de Justiça de Minas Gerais possui o Radar; o Tribunal de Justiça do Rio Grande do Norte possui o Poti, o Jerimum e o Clara; o Tribunal de Justiça de Rondônia possui o Sinapse; o Tribunal de Justiça de Pernambuco possui o Elias; o Superior Tribunal de Justiça possui o Sócrates.

Percebendo essa expansão, em 2019, o Conselho Nacional de Justiça (CNJ) editou a cartilha "Inteligência Artificial no Poder Judiciário Brasileiro" onde abordou as iniciativas concretas adotadas pelo judiciário brasileiro para se alinhar à tecnologia. Na cartilha foi apresentada a plataforma Sinapses e seus recursos de auditoria visando uma conduta ética e jurídica adequada, mostrando a preocupação e consciência do setor público com os riscos que envolvem a IA.

> O sistema Sinapses é uma plataforma para desenvolvimento e disponibilização em

> larga escala de modelos de IA, também comumente conhecido como "Fábrica de Modelos de IA". Essa terminologia se deve ao fato de a plataforma possibilitar que o processo de entrega dos modelos seja acelerado em uma escala não permitida quando o desenvolvimento ocorre da forma tradicional [...] No Sinapses [...] o sistema cliente (que irá consumir a inteligência) opera de forma totalmente independente do processo de construção dos modelos de IA, por intermédio micro serviços, também conhecidos como APIs. Ocorre assim uma total liberdade para as equipes de DataScience e também de desenvolvedores, trabalhando em uma abordagem fracamente acoplada. (CNJ, 2019, p. 21)

> No Sinapses é possível gerenciar o comportamento dos modelos em produção, provendo um ciclo que permite sua auditoria. Isso é possível, uma vez que cada modelo pode ter suas predições auditadas a cada requisição, gerando um relatório [...] A partir dessas informações e do processo de desenvolvimento que cada modelo possui dentro da plataforma (extração, treinamento, algoritmo, dependências), torna-se possível garantir uma oferta mínima de revisão do processo de sugestões realizadas pela IA. (CNJ, 2019, p. 24)

Já em 2020, dando continuidade à política de ética, transparência e governança na utilização da IA pelo judiciário e inspirado pelo *"Ethics guidelines for trustworthy AI*", o CNJ aprovou a Resolução n. 332, de 21 de agosto de 2020

> A resolução inova e traz pontos importantes que não são abordoados por outro dispositivo legal vigente na legislação brasileira como os relacionados à governança e aos parâmetros éticos para o desenvolvimento e uso da Inteligência Artificial no espaço do Poder Judiciário. Ainda traz capítulos relacionados aos direitos fundamentais; não discriminação; publicidade e transparência; governança e qualidade; segurança; controle do usuário; prestação de contas e responsabilização e pesquisa, desenvolvimento e implantação das soluções computacionais para o uso da Inteligência Artificial. (BORDONI; TONET, 2021 p. 14)

Outra percepção gerada pela implementação da IA no judiciário brasileiro é a de que assim como as demais ferramentas de inovação que tem sido implementadas nos setores da sociedade, esta não deve ser encarada como um inimiga, mas sim como aliada na melhoria da prestação de serviços públicos à sociedade, sendo sua atuação uma consequência natural dos avanços que o Brasil tem feito em direção à inovação.

REFERÊNCIAS

AMARAL JUNIOR, Alberto do. **Curso de Direito Internacional Público**. São Paulo: Editora Atlas S.A., 2015.

ANGWIN, Julia; LARSON, Jeff; MATTU, Surya; KIRCHNER, Lauren. *Machine Bias*. Wisconsin, Texas, USA: **Pro Publica**, May 23, 2016. Disponível em <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em 16 mar. 2021.

BIJOS, Leila; NASCIMENTO, Risoleide de Souza. **Tecnologia, Inovação e Desenvolvimento na União Europeia**. Goiânia, Goiás: Editora Espaço Acadêmico, 2019.

BORDONI, Jovina d'Avila; TONET, Luciano. INOVAÇÃO E TECNOLOGIA NO JUDICIÁRIO. **THEMIS: Revista da Esmec**, v. 18, n. 2, p. 151-170, 2021.

BRASIL. Governo Digital. Disponível em : <https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital>. Acesso em: 26 set. 2021

BRASIL. Ministério da Defesa. Acesso à Informação. Disponível em: <https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd>. Acesso em 22 mar. 2021.

CONSELHO NACIONAL DE JUSTIÇA. **Inteligência Artificial no Poder Judiciário Brasileiro**. Brasília, 2019, 40 p. Disponível em: < https://www.cnj.jus.br/wp-content/uploads/2020/05/Inteligencia_artificial_no_poder_judiciario_brasileiro_2019-11-22.pdf>. Acesso em 28 set. 2021.

COUTINHO, Diego R.; KIRA, Beatriz. Por que (e como) regular algoritmos? In: Jota, São Paulo. 2019. Disponível em: <https://www.jota.info/tributos-e-empresas/regulacao/por-que-e-como-regular-algoritmos-02052019#:~:text=Espa%C3%A7o%20voltado%20%C3%A0%20an%C3%A1lise%20e,o%20desenvolvimento%20socioecon%C3%B4mico%20do%20Brasil.&text=Algoritmos%20s%C3%A3o%20cada%20vez%20mais,diversas%20esferas%20do%20mundo%20moderno>. Acesso em: 19 mar. 2021.

DOMINGOS, Pedro. The master algorithm: how the quest for the ultimate machine learning will remake our world. Nova York: Basic Books, 2015.

EC. EUROPA. Digital Act. Disponível em: <https://ec.europa.eu/digital-single-market/en/digital-services-act-package#:~:text=The%20Digital%20Services%20Act%20and,European%20values%20at%20its%20centre>. Acesso em 22 mar. 2021.

EUROPEAN COMMISSION. Ethics Guidelines for Trustworthy AI. Bruxelas, 2019. Disponível em: <https://ai.bsa.org/wp-content/uploads/2019/09/AIHLEG_Ethics GuidelinesforTrustworthyAI-ENpdf.pdf.>. Acesso em: 27 set. 2021.

FERRARI, Isabela; BECKER, Daniel. Direito à Explicação e Decisões Automatizadas: Reflexões sobre o Princípio do Contraditório. In: NUNES, Dierle; LUCON, Paulo Henrique dos Santos;

FERRARI, Isabela; BECKER, Daniel. Algoritmo e preconceito: é preciso que se crie uma política de *accountability* dos algoritmos. In: **Jota**, São Paulo. 12 dezembro 2017. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/algoritmo-e-preconceito-12122017. Acesso em: 19 mar. 2021.

FORBES. Disponível em> https://www.forbes.com.br/negocios/2020/10/gigantes-da-internet-terao-que-abrir-dados-a-reguladores-antitruste-da-ue/. Acesso em 22 mar. 2021.

GOVTECH. Como a Estônia construiu uma sociedade digital. GovTech Brasil. Disponível em: <https://govtechbrasil.org.br/>. Acesso em 23 mar. 2021.

GREGÓRIO, Fernando da Silva. Consequências sistêmicas da soft law para a evolução do direito internacional e o reforço da regulação global. **Revista de Direito Constitucional e Internacional**, v. 95, p. 299-320, 2016.

ÍNDIA. *Panorama da Índia Digital*. BrasilTech, 2018. Disponível em: https://govtechbrasil.org.br/. Acesso em 23 mar. 2021.

ISRANI, Ellora. Algorithmic due processes: mistaken accountability and attribution in State v. Loomis. Edited CHANG, Evelyn. **JOLT Digest**. Harvard Journal of Law and Technology, August 31, 2017. Disponível em <https://jolt.law.harvard.edu/digest/algorithmic-due-process-mistaken-accountability-and-attribution-in-state-v-loomis-1>. Acesso em 16 mar. 2021.

LEVY, Nuria. Israel comparte conocimiento y experiencias en innovación con Costa Rica. Generación de Innovación, la experiencia de Israel. **Revista Summa**, 08/08/2017. Disponível em: < https://revistasumma.com/israel-comparte-conocimiento-experiencias-innovacion-costa-rica/>. Acesso: 2 mai. 2021.

LEWI, Peleg. Embaixador de Israel em Guangzhou, China. *Generación de Innovación, la experiencia de Israel*, 10/04/2017. Disponível em: <https://www.youtube.com/watch?v=VCFcfwp5TJQ>. Acesso: 2 mai. 2021.

McCARTHY, John. What is Artificial Intelligence? Stanford University: Revised November 2007. Não paginado. Disponível em: <http://www-formal.stanford.edu/jmc/whatisai/whatisai.html.> Acesso em: 16 mar. 2021.

NUNES, Dierle; LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro. Inteligência Artificial e Direito Processual. 2ª edição. Salvador, Bahia: Editora *JusP*odium, 2021.

LONDON. United Kingdom of Great Britain and Northern Ireland. Science and technology committe. **Algorithms in decision-making:** fourth report of session 2017–19. 2018. Disponível em: <https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/351/351.pdf>. Acesso em: 21 mar. 2021.

LONDON. United Kingdom of Great Britain and Northern Ireland. UK Government. Centre for Data, Ethics and Innovation-. Consultation. Disponível em: <https://www.gov.uk/government/organisations/home-office/about>. Acesso em: 21 mar. 2021.

PAVLICH, Eric. **Law & Society Redefined**. Oxford University Press, 2011.

POSNER, Eric A. **The Twilight of Human Rights Law**. Oxford University Press, 2014.

RUMERLHART, David E.; HILTON, Geoffrey E.; WILLINANS, Ronald J. Learning Representations by back-propagating errors. **Nature**, v. 323, issue 9, p. 533, Oct. 1986.

SANTOS, Sarah Ribeiro do Nascimento; PEREIRA, Bruna Tarabossi; GANDRA, Guilherme Góes. Algoritmos e integração de novas tecnologias ao sistema jurídico. São Paulo, 27 abr. 2019. Não paginado. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/regulacao-e-novas-tecnologias/algoritmos-e-integracao-de-novas-tecnologias-ao-sistema-juridico-27042019>. Acesso em 19 mar. 2021.

SUPREMO TRIBUNAL FEDERAL. Estratégia de Governança Digital e a Lei da Informação: robô VICTOR. Brasília: Notícias STF, 30/05/2018. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=380038>. Acesso em: 19 mar. 2021.

UMA inteligência artificial usada para encontrar vieses na inteligência artificial. **O Estadão**. 15 ago. 2021. Disponível em: <https://internacional.estadao.com.br/noticias/nytiw,tecnologia-inteligencia-artificial-preconceito,70003805772>. Acesso em: 28 set. 2021.

URWIN R. Artificial Intelligence: The Quest for the Ultimate Thinking Machine. London: Arcturius, 2016. Arquivo Kindle, p. 92.

WILDISEN, Greg. Is artificial intelligence the key to unlocking innovation in your law firm? Legal Week, 12 Nov. 2015. Não paginado. Disponível em: <https://www.law.com/international-edition/2015/11/12/is-artificial-intelligence-the-key-to-unlocking-innovation-in-your-law-firm/?slreturn=20210216150814>. Acesso em 16 mar. 2021.

WOLKART, Erik Navarro. **Inteligência Artificial e Direito Processual**. 2ª edição. Salvador, Bahia: Editora *JusP*odium, 2021, pp. 277-297.

Anexo A – Produto Tecnológico

Como produto tecnológico, foi proposto um manual de boas práticas em cibersegurança.