UNIVERSIDADE FEDERAL DE UBERLÂNDIA – UFU

VITOR ALBERTO MIRANDA MORAES

A TUTELA DOS BENS JURÍDICOS NOS CRIMES INFORMÁTICOS: A AUSÊNCIA DE UMA POLÍTICA PÚBLICA EM ÂMBITO CRIMINAL

Uberlândia, 2021

A TUTELA DOS BENS JURÍDICOS NOS CRIMES INFORMÁTICOS: A AUSÊNCIA DE UMA POLÍTICA PÚBLICA EM ÂMBITO CRIMINAL

Artigo apresentado como Trabalho de Conclusão de Curso, requisito parcial para a obtenção do título de Bacharel em Direito, pela Universidade do Federal de Uberlândia, Faculdade de Direito Professor Jacy de Assis.

Orientador: Prof. Me. Karlos Alves Barbosa

Uberlândia, 2021

A TUTELA DOS BENS JURÍDICOS NOS CRIMES INFORMÁTICOS: A AUSÊNCIA DE UMA POLÍTICA PÚBLICA EM ÂMBITO CRIMINAL

Trabalho de Conclusão de Curso apresentado como requisito parcial para a obtenção do título de Bacharel em Direito, pela Universidade do Federal de Uberlândia, Faculdade de Direito Professor Jacy de Assis.

Uberlândia, 26 de setembro de 2021

BANCA EXAMINADORA

_____

Prof. Me. Karlos Alves Barbosa

_____

Profª. Dra. Simone Silva Prudêncio

DEDICATÓRIA

Este trabalho é dedicado a todas as dificuldades e obstáculos que enfrentei durante meu percurso da graduação, sem os quais não teria aprendido, crescido e evoluído.

AGRADECIMENTOS

Grato à minha família, que me apoiou em momentos de imensa dificuldade.

Agradeço aos professores da Faculdade de Direito pelo inestimável conhecimento que obtive ao longo dessa jornada, em especial ao meu orientador, Prof. Karlos Alves, por comigo compartilhar um pouco da sua experiência e excelência acadêmica na produção deste trabalho, grato à Professora Simone Silva Prudência, que contribui para o sucesso da apresentação deste trabalho.

"A glória é tanto mais tardia, quanto mais duradoura há de ser, porque todo fruto delicioso amadurece lentamente." (Arthur Schopenhauer)

RESUMO

Neste tralho, será feita uma pesquisa por revisão bibliográfica e da legislação brasileira acerca da proteção de bens jurídicos nos casos de crime informático. Buscar-se-á demonstrar a importância de mudar o foco da punição estatal para a proteção objetiva via políticas públicas. Para tanto, este estudo ocupa-se, em operação introdutória, de discorrer sobre o que é bem jurídico e sua utilidade para o direito, sob a ótica da instrumentalização do direito como meio para proteção de bens jurídicos, especialmente em âmbito criminal. Continuamente, analisa-se a prática de atos criminosos no meio informático, buscando a definição do que é crime informático, a diferença entre os crimes informáticos cujo objeto de violação é um bem jurídico informático e aqueles crimes em que se verifica o uso da tecnologia da informação como apenas uma ferramenta na execução do delito, além de comentar quais crimes informáticos foram adicionados ao ordenamento jurídico, com foco nas alterações trazidas pelas Leis 12.737/2012 e Lei 11.829/2008. Além disso, discorrer-se-á uma análise dos crimes informáticos utilizando a teoria TCC: Técnica, comportamento, crime, elaborada por Damásio de Jesus. Por fim, será realizada um breve comentário crítico do "estado de coisas" da proteção dos bens jurídicos na internet no Brasil.

Palavras-chave: Bem jurídico. Crime informático. Direito Penal Digital. Sociedade da informação.

ABSTRACT

In this work, a search will be made by bibliographic review and Brazilian legislation on the protection of legal assets in cases of computer crime. It will seek to demonstrate the importance of shifting the focus from state punishment to objective protection via public policies. Therefore, this study is concerned, in an introductory operation, with discussing what is a legal asset and its usefulness for the law, from the perspective of the instrumentalization of law as a means to protect legal assets, focusing on the criminal system. The practice of criminal acts in the computer environment is continuously analyzed, seeking to define what is a computer crime, the difference between computer crimes whose object of violation is a computer legal asset and those crimes in which the use of computer technology is verified. information as just a tool in the execution of the crime, in addition to commenting which computer crimes were added to the legal system, with a focus on the changes brought about by Laws 12,737/2012 and Law 11,829/2008. In addition, an analysis of computer crimes will be discussed using the TCC theory: Technique, conduct, crime, developed by Damásio de Jesus. Finally, a brief critical comment will be made on the "state of affairs" of the protection of legal assets on the internet in Brazil.

Keywords: Legal assets. Cybercrimes. Digital Criminal Law. Information society.

SUMÁRIO

1 INTRODUÇÃO

A segunda metade do século XX trouxe evoluções estrondosas para a tecnologia da informação, como o surgimento do telefone celular, os computadores de mesa (*desktops*) e a internet. Em um período histórico muito curto houve uma explosão no avanço dos meios de transmissão de informação.

Após o fim do período histórico conhecido como Guerra Fria, a tecnologia da informação passou a ser fundamental para o desenvolvimento do mundo, sendo que os países que dominam a produção desta mercadoria atingiram significativos índices de crescimento além de relevância econômica internacional no novo milênio.

O século XXI concretizou a revolução da Internet, que foi transformada no principal meio de difusão de informações da atualidade. Essa poderosa ferramenta constitui a principal forma de câmbio informacional, bem como ferramenta de pesquisa, automação de produção e, com o advento das redes sociais, o principal meio de interação e integração da pessoa na sociedade.

A volatilidade e velocidade com a qual as informações disponíveis na rede são inseridas e movimentadas cria um aumento de risco, uma vez que informações de praticamente toda população podem ser encontradas em algum banco de dados. Esses dados podem ser utilizados para lesionar bens jurídicos, demandando a atenção do Direito Penal.

No atual modelo de sociedade conectada, cabe ao direito penal zelar pela proteção dos novos bens jurídicos quando todos os outros ramos do direito não o fizerem, bem como proteger aqueles já existentes no ordenamento jurídico, mas que podem ser violados por novas condutas. Mas o que são os bens jurídicos?

Bem jurídico deve ser entendido como o objeto de proteção do tipo penal, coisa ou valor socialmente relevante. Segundo Regina Maria Bueno de Godoy “os valores mais importantes identificados por uma sociedade expressam-se através da eleição pelo legislador de bens jurídicos dignos de proteção” (GODOY, R. M. B de. A proteção dos bens jurídicos como fundamento do Direito Penal. São Paulo, 2010. PUC.).

Cabe ressaltar que relações e fatos tornam-se juridicamente relevantes quando afetam ou criam um novo bem ou valor, que pode ser material ou não material. Se esse produto do fato juridicamente relevante é ameaçado em um momento qualquer, torna-se objeto do direito penal. Os bens jurídicos protegidos são, mormente, abstratos e devem ser delimitados pelo próprio ordenamento jurídico, pois é dever do Estado à proteção de valores e bens interessantes à

determinada sociedade. Exemplos de bens jurídicos assegurados pelo ordenamento jurídico pátrio são: vida, propriedade e liberdade.

Em virtude da volatilidade social e da lentidão necessária ao processo legislativo, nem todas as formas de lesão a bens jurídicos estarão presentes na legislação positivada. O surgimento de agressões à bens de relevância jurídica e a repercussão social dessas condutas é que impulsionam o Poder Legislativo a tipificar determinadas condutas.

Deve-se considerar que, como têm demonstrado a História, a simples criminalização de condutas não resolve o problema da agressão a bem jurídico, sendo o Direito Penal incidente quando todos os outros meios de controle legal e os meios de coação social falharam. O próprio conceito de bem jurídico atua, também, como limitador do *jus puniendi* do Estado, uma vez que ele não pode restringir direitos e aplicar penas diversas das previstas em lei.

Antes a essas considerações, afere-se que a função primordial do Direito Penal não é a de impor castigo, mas a de proteger os bens jurídicos. Essa proteção se dá através da positivação de limites aceitáveis. Mas, como essa proteção é feita no caso de crimes informáticos? Esta pergunta será respondida ao longo deste trabalho.

Neste trabalho a questão supra será respondida através da pesquisa bibliográfica e documental, com foco nas leis e doutrinas do direito . Além disso, será apresentada uma análise crítica sobre a atual proteção que o sistema jurídico confere à vítima em casos de delitos informáticos.

2 PROBLEMATIZAÇÃO

A pesquisa científica exige o confronto de hipóteses com a finalidade de se confirmar ou denegar as hipóteses levantadas pelo cientista. É possível que a pesquisa também seja baseada na buscas para respostas.

No âmbito de um Direito Digital, onde o que há perante os pesquisadores é nada menos que um mar a ser desbravado, uma vez que ainda estudam-se eventos ocorridos dez anos atrás, enquanto surge novos crimes que violam a intimidade de milhões de usuários da maior rede social existente na atualidade, como no caso de vazamento de dados do Facebook.

O *Big Data* cria sistemas de informação capazes de aprender por si só (*machine learning*), por meio da seleção, mineração, análise e elaboração de tabelas de dados, mas os juristas ainda imaginam como a criminalidade virtual ocorre e por quais métodos ela é aperfeiçoada. Deve-se considerar o uso de um mesmo sistema de informação pode ser empregado para fins lícitos e ilícitos, como qualquer outra ferramenta já desenvolvida pelos seres humanos.

O escândalo da Cambridge Analytica, empresa que prestava serviços de pesquisas, coleta dados e informações ao Facebook, revelado em 2018, trouxe à tona o poder do uso mau intencionado de dados vazados de clientes, além de ter demonstrado que as redes de comunicação via internet não filtram o acesso dos usuários às *fake news*[1], não previnem vazamentos de dados e informações particulares, não filtram adequadamente conteúdo anunciado na plataforma etc. Nesse caso, foi o suficiente para determinar o vencedor da eleição presidencial do país com maior poder econômico da atualidade.

Nessas situações, um elemento que claramente influenciou para a possibilidade de ocorrência desses eventos é o risco.

Mendes (Mendes, 2015, págs. 19-28), explica a teoria do risco de Ulrich Beck afirmando que o capitalismo consolidado e tardio do Séc. XX evoluiu rapidamente, de modo que as novas invenções e necessidades do capital resultam em um aumento do que é chamado de risco, de tal forma que o risco é uma "consequência do desenvolvimento científico e cultural" que não podem ser temporal e espacialmente contidos. O aumento excessivo dos riscos, por sua vez, sobrecarrega o Estado, que passa a limitar as liberdades, já que ele passa a ser o principal garante em uma sociedade abarrotada de riscos e, caso não adote medidas que possibilitem a mitigação do risco, pode ocorrer o colapso das estruturas, já que o Estado é o último e principal garante na modernidade.

1 Desinformação ou boato veiculado como se notícia fosse. O boato (*hoax*), é considerado um tipo de ameaça cibernético por Damásio de Jesus.

Ao se aplicar a visão de Beck, explicada por Mendes, abstraída no âmbito do Direito Penal Digital, pode-se inferir que as novas tecnologias trazem a possibilidade de existências de novos tipos penais ou, no mínimo, a criação de qualificadoras para os crimes já existentes.

Cabe ao Direito Penal a utópica tarefa de apaziguar a sociedade e oferecer uma resposta punitiva, retributiva e ressocializadora contra aqueles que vilipendiam bens jurídicos de forma violenta para, dessa forma, tentar atenuar o risco social.

Ao proteger caros valores sociais, o Direito Penal colabora para uma maior estabilidade social, uma vez que os indivíduos imersos naquele contexto passam a ver que as instituições realmente se importam com seus anseios, reduzindo os riscos gerados por uma ansiedade coletiva.

Com os bens jurídicos digitais não é diferente, uma vez que a ideia de segurança criada pela valoração do bem jurídico digital na esfera do direito penal, centrado na ideia de políticas criminais de uma sociedade democrática, implica um Estado que efetivamente se importe com aqueles valores, de modo que haverão de ser tomadas medidas para garantir o acesso dos seus cidadãos ao mar da virtualização, com a garantia de que aqueles que almejarem causar dano a eles serão punidos.

Agora, quando o tema é bem jurídico digital deve-se buscar o significado de bem jurídico digital e como protegê-lo. Nesse desiderato, para ajudar a elucidar essa inquietação, foram elaboradas as perguntas:

1. **O que é bem jurídico digital?**
2. **Qual a função do bem jurídico digital?**
3. **O que é crime informático?**
4. **Qual a Legislação brasileira norteadora da tutela dos bens jurídicos informáticos no Brasil?**

2.1 O QUE É BEM JURÍDICO DIGITAL?

Segundo a definição do dicionário Michaelis, um bem é “todo e qualquer fator capaz de gerar condições ideais ao bem-estar, ao aprimoramento e ao progresso de um indivíduo ou de uma comunidade”, também podendo ser o “conjunto de princípios e regras de conduta, em determinada época e em um grupo determinado, considerados fundamentais para propiciar o desenvolvimento e o aperfeiçoamento dos indivíduos e do grupo, salvaguardadas a vida e a dignidade de todos” (MICHAËLIS; MICHAELIS, 2021).

O conceito de bem jurídico nasce fora da esfera penal, sendo a própria noção de bem uma característica de uma sociedade liberal, pautada na liberdade individual, propriedade material, propriedade imaterial, bem como na autodeterminação, de tal forma que pode-se aferir uma das preocupações do Direito enquanto ciência social é com a proteção dos valores individuais essenciais para uma vida em sociedade.

Claus Roxin aponta:

> Desde a concepção ideológica de contrato social, os cidadãos, como possuidores do Poder estatal, transferem ao Legislador somente as atribuições de intervenção jurídico-penais que sejam necessárias para o logro de uma vida em comunidade livre e pacífica, e eles fazem isso somente na medida em que este objetivo não se possa alcançar por outros meios mais leves. A ideia que se subentende a essa concepção e que se deve encontrar um equilíbrio entre o poder de intervenção estatal e a liberdade civil, que então garanta a cada um tanto a proteção estatal necessária como também a liberdade individual possível(…). O Estado deve garantir, com os instrumentos jurídico-penais, não somente as condições individuais necessárias para uma coexistência semelhante (isto é, proteção da vida e do corpo, da atuação voluntária, da propriedade etc), mas também as instituições estatais adequadas para este fim (justiça, sistema tributário saudável, administração livre de corrupção..), sempre e quando não se puder alcançar isso de uma maneira melhor. Estes objetos e valores são os bens jurídicos. Circunstâncias reais, dadas ou finalidades necessárias, para uma vida livre e segura, que garanta todos os direitos humanos e civis para cada um na sociedade ou para um funcionamento de um sistema estatal que se baseia nestes objetivos.”

A Roxin, importa que “bens jurídicos devem ser delimitados racionalmente, de forma empírica e científica, não devendo proteger apenas sentimentos, convicções e tabus.”(ROXIN. 2009. 2ª Edição.) Deste trecho é possível inferir que as situações que vão de encontro a moral não ferem bens jurídicos, porque, caso fossem danos jurídicos, o Direito seria despido de seu caráter científico e passaria a ser dotado de simples função política.

Guilherme Nucci, por sua vez, aduz que “há bens tutelados pelo Direito, eleitos pelo ordenamento jurídico como indispensáveis à vida em sociedade, merecendo proteção e cuidado. A partir dessa escolha, o bem se transforma em bem jurídico”. (NUCCI, 2020, pág. 78)

Além disso, todos os princípios do direito penal orbitam o conceito de bem jurídico. Nas palavras do autor:

> (…) em razão dele são tecidos tipos penais incriminadores, formando a ilicitude penal; conforme o grau de lesão provocado ao bem jurídico, ingressa-se na avaliação da culpabilidade, tanto na parte concernente à formação do delito, como também no âmbito da aplicação da pena, afinal, bens jurídicos fundamentais demandam penas mais severas. (NUCCI, 2019, pág. 79)

Eis que, se bem jurídico é um conceito criado a partir de um valor social que passa a ser juridicamente protegido, então ele muda a cada vez que se altera a maneira como a população percebe o mundo e a própria realidade na qual estão inseridos.

Nessa senda, o direito penal precisa ser atualizado de modo a incluir as novas perspectivas de valoração, de modo que o ordenamento penal e a política criminal passem a zelar pelos objetos que a sociedade aceita como essenciais para uma vida pacífica.

Então, quando é criada uma empresa que opera transações financeiras unicamente por via digital, a lei deve passar a proteger os novos bens que com ela surgirem, mesmo que seja um novo bem totalmente imaterial, não perceptível na dimensão física, mas pode ser valorado monetariamente por meio de comparação a uma moeda. Este é o caso das criptomoedas[2], mas também pode ser o caso de músicas, álbuns, e até mesmo dados pessoais.

É plena a certeza de que a Constituição Federal de 1988 protege bens imateriais, como a vida, a dignidade da pessoa humana, a honra, o livre desenvolvimento da personalidade, a saúde entre outros.

Por vezes, tais bens caem na senda dos conceitos jurídicos indeterminados, sendo indeterminados da mesma maneira que a própria ideia de bem jurídico. A indeterminação dos conceitos não decorre de sua ausência de significado, mas da polissemia ou da mutabilidade dos valores que os criaram, de modo que a determinação recai sobre a Sociologia Jurídica, hermenêutica do Direito, além da construção histórica da jurisprudência.

A ideia de vida, por exemplo, pode ser considerada como o intervalo que vai desde a concepção, do nascimento, do nascimento com vida até o momento em que se cessa de forma permanente a respiração, os batimentos cardíacos ou a atividade cerebral. A variação de tal conceito varia a depender da cultura, momento histórico.

De maneira semelhante a honra, que segundo Nelson Rosenvald e Cristiano Chaves de Farias “é a soma de todos os conceitos positivos que uma pessoa goza em sociedade”. Já foi admitido pelo ordenamento jurídico, por exemplo, o homicídio em defesa da honra matrimonial, aberração que felizmente já foi expurgada do direito brasileiro. (FARIAS; ROSENVALD, 2008. P. 149.)

Já para o autor Luiz Régis Prado, bem jurídico é “o conceito central do tipo, em torno do qual giram os elementos objetivos e subjetivos e, portanto, um importante instrumento de interpretação”. (PRADO. 2018. Pág. 46)

2. Ativo digital, utilizado com finalidade de troca, sem a intermediação de uma instituição financeira centralizada (Banco Central).

No caso do conceito bem jurídico digital, trata-se de valor constituído por equipamentos, linhas de código, valores, informações, imagens e registros, que existem para servir às pessoas, gerando consequências na vida em sociedade e, portanto, não são dissociadas das normas do Direito.

Por meio da internet ampliou-se a exposição do indivíduo no mundo virtual, uma vez que ele ou qualquer pessoa com um equipamento informático conectado à rede passa a ser uma geradora de dados, de maneira que um grupo de pessoas utilizando qualquer dispositivo conectado à *world wide web*[3] é uma verdadeira mina de dados, uma vez que cada clique gera conteúdo que será explorado pelas grandes empresas da tecnologia da informação que operam as informa internet, as *big techs*, como deixou claro "O Dilema das Redes" e "Privacidade Hackeada", dois documentários que demonstram de forma facilmente compreensível o poder do *Big Tech* em todas as esferas da vida social.

Isso porque ao gerar dados de navegação e acesso, as redes sociais capturam informações privadas íntimas do indivíduo, desde suas senhas até seus hábitos de consumo, que informações utilizadas com a finalidade de direcionar os sistemas de anúncios que sustentam economicamente essas plataformas. Se essas informações caem em mãos criminosas, serão instrumentalizadas contra o usuário.

Como será explicado em capítulos posteriores, essas informações podem ser utilizadas com a finalidade ou invasão a sistemas informáticos, por meio de um ataque de *botnet*[4].

Caso se concretizem o crime acima referido, a violação, fora essencialmente perpetrada ao se burlar a privacidade de um indivíduo, podendo, posteriormente, resultar em prejuízos patrimoniais a terceiros, destinatários do ataque cibernético.

Ocorre que já fora reconhecida no sistema jurídico-penal nacional a existência de bens jurídicos informáticos, inicialmente pela Lei 12.737/2012, ao inserir no Código Penal o artigo 154-A, *ipsis literis*:

> "Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui

3. A *world wide web* (www) é a camada da *internet*, a rede mundial de computadores, mais acessível aos usuários comuns.
4. Sistema de máquinas zumbi que, por meio da captura de um servidor, passam a ser controladas por quem as capturou.

> crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

Assim, não há que se criar divergências quanto existência de bens jurídicos digitais, mas quanto às medidas de proteção e tipificação de condutas violadoras. Apesar disso, a mera tipificação penal é apenas um dos passos para uma a proteção da sociedade no mundo virtual.

Antes de se positivar algo, garantindo a esse objeto a proteção normativa e agregando a ele centralidade nas políticas de construção social, é necessário considerar sua finalidade, para que a penalização seja proporcional à violação. Adiante será abordada a finalidade dos bens jurídicos, tendo como centralidade a defesa dos bens jurídicos no âmbito informático.

2.2 QUAL A FUNÇÃO DE UM BEM JURÍDICO DIGITAL?

Zampier, considera que um bem deve atender a uma necessidade subjetiva: a autorrealização. Para o autor, o bem jurídico pode "preencher questões de ordem patrimonial, existencial ou mesmo ambas"(ZAMPIER, 2020, pág. 61). Em contínuo raciocínio, o autor considera que somente um bem que satisfaça alguma necessidade humana merece o amparo jurídico.

Em um paralelo traçado com a Filosofia Clássica, a noção de satisfação de necessidade pode ser comparada a ideia de autorrealização, entendida por meio da ideia de felicidade. Platão considerava que o conhecimento leva à virtude e esta, por sua vez, conduz ao caminho do bem e da felicidade.

Epicuro considerava que a serenidade interior, na ausência de dor física, é a síntese da felicidade. Em comum, tanto Platão quanto Aristótales buscaram a felicidade como a finalidade da existência humana (CASTILHO, Filosofia Geral e Jurídica, 2016).

No séc. XVIII, após a Revolução Francesa, a ideia de busca felicidade era precedida pela necessidade de uma sociedade igual, fraterna e livre. Incutida nas cartas de independência do Ocidente, o conceito de felicidade passa a ser considerado como uma consequência de uma sociedade pautada por um ideário de Justiça e liberdade privada, com a ausência de dominância estatal ou clériga.

Hoje, sob a égide de uma sociedade pós-moderna, explicada por Zygmunt Bauman como uma sociedade líquida, que nega o passado mas anseia por um futuro idealizado, mas totalmente distópico, uma sociedade onde as relações humanas são superficiais e o insólito é aquilo que é perene, felicidade é aquilo que está sempre ao horizonte, um ideal que move a humanidade sendo, todavia, inalcançável (BAUMAN, 2001).

Apesar de elaborados em distintos momentos históricos, as três correntes de pensamento postulam a felicidade como um valor, ou até mesmo um motor da atividade humana. A partir do exposto, pode-se inferir que a felicidade é um bem.

Ocorre que este bem não necessariamente é protegido pelo Direito de maneira direta, tratando-se de um conceito extremamente vago e volátil. A fim de proteger o ideário de ser feliz, os juristas buscaram especificar valores que podem levar o homem a atingir o gozo existencial e, no caso do direito brasileiro, os bens necessários a esta realização estão dispostos principalmente nos Títulos I e II da Constituição Federal de 1988.

A função dos bens jurídicos, *prima facie*, é uma função política, porque é baseada em um ideário de uma nação expresso em suas normas e estabelece um objeto de proteção formal. Demandas sociais, tais como a igualdade racial, a propriedade e a probidade da Administração Pública, foram aceitas pelos órgãos estatais e admitidas no ordenamento jurídico, sendo que diversas formas de violação desses valores são valoradas como crime.

A título de exemplo, pode-se falar da violação da dignidade humana na injúria racial (art. 140, §3° do Código Penal), da propriedade no furto (art. 155 do Código Penal) e da incolumidade da Administração no crime de advocacia administrativa (art. 321 do Estatuto Repressivo).

De forma secundária, há de se pontuar que os bens jurídicos têm o finco de limitar o alcance da intervenção estatal na esfera privada, definindo as fronteiras do poder de punição do Estado aos infratores.

Uma terceira função, seria a positivadora, que promove a estratificação escrita daquilo que se almeja defender. Prescrevendo condutas negativas ou positivas em relação ao alvo da valoração jurídica cria-se uma perenidade e um sentimento de segurança de que aquilo que está escrito é o parâmetro a ser seguido.

Segundo Luiz Régis Prado o bem jurídico-penal é dotado de 6 funções, a saber:

> "(…)
> 1. *Função dogmática:* é função, por assim dizer, doutrinária de reconhecimento do sistema penal vigente. Consiste ela na valorização do papel central que ocupa o bem jurídico na formação do delito, e sua consideração de modo prevalentemente objetivo.
> 2. *Função de garantia ou de limitação ao direito de punir do Estado:* o bem jurídico é erigido como conceito limite na dimensão material da norma penal. Em relação a essa função, alude-se que o legislador é formalmente livre de penalizar ou não uma conduta, mas não substancialmente é árbitro da sua escolha.
> 3. *Função teleológica ou interpretativa:* como um critério de interpretação dos tipos penais, que condiciona seu sentido e alcance à finalidade de proteção de certo bem jurídico. Implica em buscar a compreensão do significado do tipo legal abstratamente previsto.
> 4. *Função de orientação político-criminal:* opera numa perspectiva metajurídica que utiliza o conceito de bem jurídico como parâmetro de critérios orientadores no plano da política criminal. O conceito de bem jurídico opera como critério de legitimação da norma penal, de matiz político liberal e democrático;
> 5. *Função individualizadora:* como critério de medição da pena, no momento concreto de sua fixação, levando-se em conta a gravidade da lesão ao bem jurídico. Essa função não deixa de ser também função de garantia, consistente em reconstruir a concreta ofensa a um interesse merecedor de tutela, legitimando assim a incriminação de uma conduta na perspectiva de um Direito Penal do fato
> 6. *Função sistemática ou classificatória:* como elemento classificatório decisivo na formação dos grupos de tipos da parte especial do Código Penal. Os próprios títulos ou capítulos da parte especial são estruturados com lastro no critério do bem jurídico em cada caso pertinente. Na medida em que o bem jurídico se situa no ponto central dos diferentes tipos penais da parte especial do Código e sendo uma exigência para o legislador orientar sua atividade na proteção de bens jurídicos, vem a ser "um dos pontos de vista (...) para conceber o núcleo material dos injustos, comum a todo comportamento ilícito". Em suma: essa função aparece como guia ao reagrupamento dos delitos em uma ordem legal representativa de uma hierarquia de valores (…) (PRADO, 2019, págs. 44-45)

No âmbito do Direito PEnal Digital, não é diferente, na medida em que os bens jurídicos digitais são valores, privados ou públicos, que determinam o que o Estado deve proteger. Todavia, essa proteção não pode caracterizar autorização para ingerência estatal ilimitada na vida dos cidadãos, de modo que a inviolabilidade das comunicações e informações telemáticas deve ser preservada, de tal maneira que apenas nas hipóteses da Lei esses direitos podem ser mitigados, especialmente em caso de investigação criminal.

Também deve-se atentar para a proteção das liberdades públicas, a exemplo da liberdade reunião pacífica que, na internet, ocorre por meio de fóruns online, *lives* e da comunicação em grupos de redes sociais, com fim de se garantir a liberdade de expressão, desde que respeitados os limites legais, tais como a vedação à propagação do discurso de ódio, além da proibição de difamação, calúnia ou a invasão de sistemas telemáticos/informáticos.

Sob a perspectiva do Direito Penal Digital, ao se tipificar uma conduta de modo a tornar crime a violação de determinado bem, o legislador entrega à seara do processo penal a função de remediar um dano a determinado bem jurídico que não pôde ser contido por meios menos gravosos.

Apesar de bens jurídicos informáticos não poderem ser transmutados em objetos palpáveis por ser o ciberespaço intangível, ele não é irreal, uma vez porque é composto de diversas máquinas que operam por códigos que se expandem e modificam-se a cada nova interação entre uma pessoa e uma máquina, ou mesmo entre máquinas programadas com sistemas de inteligência artificial que possibilitam o autoaprendizado dos dispositivos computadorizados, o chamado *machine learning*.

Entretanto, há um vão para a efetivação daquilo que a lei dispões e o fluxo de desenvolvimento tecnológico proporcionado pela *web*, já que esta última muda a todo instante, enquanto a primeira depende de demorados processos legislativos.

Como será explicado adiante, existem diversas técnicas e condutas que podem violar um bem jurídico, sendo que as principais são *Trojan horse*, *Ramsonware*, vírus, *Worms*, *Phishing*, *spam* e *hoaxe*.

Novas técnicas de agressão virtual, chamadas ameaças, são criadas diariamente, diversas sem uma tipificação penal específica, mesmo produzindo dano a valores legalmente protegidos, o que torna extremamente difícil que a previsão em lei penal resulte em efetiva proteção social, deixando em aberto a dúvida de como deve ser uma estrutura de proteção dos bens jurídicos.

Independentemente do refinamento que os cibercriminosos adotarem em suas técnicas de invasão, na grande maioria dos casos concretos os bens atingidos são pretéritos à própria existência da internet.

Assim, é possível que novas condutas violem a integridade das redes e sistemas, a incolumidade pública, a honra, a intimidade, o patrimônio ou qualquer outro bem jurídico, uma vez que a tecnologia da informação é um dos meios para se atingir objetivos, não um fim em si própria.

Portanto, é elementar que independentemente da ameaça virtual o ordenamento penal confira penalidade à determinadas condutas, guardados os devidos limites para a persecução penal, de modo que não seja necessária nova atualização normativa a cada novo *malware* desenvolvido.

Antes de penalizar, deve o sistema jurídico nacional prever e discriminar o que é crime informático, além de criar métodos para contenção e proteção dos usuários da internet, conteúdo que será abordado nos capítulos seguintes.

2.3 O QUE É CRIME INFORMÁTICO?

O Direito Penal brasileiro considera crime como o fato típico, antijurídico e culpável.

A doutrina de Maximilianos Führer e Maximiliano Führer explica que fato típico é aquele que se adequa ao tipo penal incriminador; antijurídica é a conduta contrária ao direito. (FÜHRER, C. A.; R. E. FÜHRER, 2018, pág. 28).

Tipicidade é a adequação da conduta de um agente ao conteúdo de uma normal penal, enquanto a antijuridicidade é a conduta que é contrária ao direito. A tipicidade e a antijuridicidade são os elementos que compõe o crime, sendo que a culpabilidade é elemento necessário ao se analisar a possibilidade de penalização do agente e diz respeito a vontade de um agente de produzir determinado resultado.

A título de exemplo, caso um fato típico seja praticado por pessoa inimputável, que não possua consciência da potencial ilicitude da conduta ou que não se possa exigir conduta diversa, não há culpa.

No âmbito virtual, o crime informático nada mais é que o fato típico, ilícito e culpável praticado por meio de sistemas informatizados.

Então, o que seriam os crimes virtuais? Em uma simples resposta chega-se à conclusão de que seriam quaisquer "ações típicas, antijurídicas e culpáveis cometidas contra ou pela utilização de processamento automático de dados ou sua transmissão em que a internet seja o principal objeto ou instrumento do crime". (ACHA, 2016)

No mesmo sentido o crime informático é conceituado por Damásio de Jesus e J. A. Milagre, como sendo "fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação". (JESUS; MILAGRE, 2016, pág. 49)

É importante frisar que ideia de crime informático não é universal, e varia entre os diferentes sistemas penais que existem no mundo. A Europol, Polícia da União Europeia, adota um conceito duplo, no qual se considera que os "*cyber-dependent crimes* são aqueles que referem-se a qualquer delito cometido por meio de uma rede computadorizada[5], sendo *cyber-enable crimes* os crimes tradicionais cujo cometimento é facilitado por redes de computadores[6].

Já a *Organization for Economic Cooperation and Development* (OECD), de 1986, utilizam o conceito do crime eletrônico (SCHJOLBERG, p. 8), sendo este "qualquer

5. *Cyber-dependent crime:* crime dependente de meio virtual
6. *Cyber-enalbled crime:* crime possibilitado por meio virtual.

comportamento ilegal, aético ou não autorizado envolvendo processamento automático de dados e, transmissão de dados, podendo implicar a manipulação de dados ou informações, a falsificação de programas, o acesso e/ou o uso não autorizado de computadores e redes".

O alvo de um ataque pode ser qualquer bem jurídico, seja material ou imaterial, sendo que o Código Penal Brasileiro, em seu art. 154-A, admite a invasão de dispositivo informático com a finalidade de alterar dados, sem a expressa autorização do proprietário, em uma clara hipótese de violação de bem jurídico imaterial.

Em âmbito de interpretação do fato típico, seja para qualificação da conduta ou aplicação da pena, há a necessidade de se desmembrar a atividade criminosa para facilitar o seu estudo. Com esta, finalidade Damásio de Jesus criou a Teoria TCC: Técnica, comportamento e crime (JESUS; MILAGRE, 2016).

De acordo com este autor, a técnica é "método, procedimento, software ou processo informático utilizado e que pode caracterizar um comportamento" (JESUS; MILAGRE, 2016, pág. 26). A partir deste conceito, ele leciona que a técnica pode ser executada manualmente, com subtécnicas, métodos automatizados ou ferramentas.

A exemplo o autor evoca uma situação na qual determinado agente obtém acesso indevido a dados de um repositório pode estar utilizando a técnica de *sql injection*[7], que nada mais é que a inserção de dados e comandos falsos em um sistema programado na linguagem *SQL*. Todavia, poderia o agente utilizar um panteão gigantesco de ameaças.

Ocorre que algumas técnicas são mais comuns que outras, por serem mais simples de executar, a saber:

1. Vírus: *software* (programa computadorizado) malicioso (*malware*) capaz de alterar ou destruir dados, arquivos, sistemas e até programas inteiros.
2. Trojan (cavalo de Troia): *malware*[8] embutido em um *software* legítimo, com capacidade para visualizar e/ou alterar dados em um sistema informático.
3. *Spyware* (programa espião): *software* que após ser instalado em um sistema, é capaz de monitorar os hábitos de uso da vítima naquele sistema, motivo pelo qual é amplamente utilizado por empresas que oferecem aplicativos gratuitos.
4. DoS e DDoS: *Denail of Service* (negação de serviço) e *Distributed Denail of Service* (negação de serviço coordenada) são duas ferramentas pela qual um atacante inviabiliza o acesso a um servidor que processa dados e informações de determinado sistema. A diferença entre eles é que no segundo há uma pluralidade de máquinas

7. "Técnica consistente em alterar parâmetros ou instruções que são executadas sobre uma ou mais tabelas de um banco de dados, por meio da linguagem SQL (Structured Query Language), permitindo o acesso indevido, alteração, inclusão ou destruição de informações". (JESUS; MILAGRE, 2018)
8. Programa de computador malicioso.

sendo controladas por um ou mais atacantes. O TSE já foi alvo de um ataque coordenado via DDoS durante o processo eleitoral de 2020.

5. *Hoax* (boato): Utilizado para espalhar desinformação por meio de *fake news* (notícias falsas), não caracteriza uma invasão a sistemas, mas a criação de mentiras, estruturadas como se fosse notícias, ou mesmo adulteração de conteúdo jornalístico-informacional, com finalidade de criar caos entre a população alvo, gerando desconfiança e desorientação, principalmente em relação a temas políticos. Exemplo recente ocorreram nas manifestações dos caminhoneiros no feriado de independência, aonde muitos manifestantes foram iludidos por uma falsa notícia que alertava para a decretação do estado de sítio pelo Presidente da República.
6. *Ramsonware*: técnica de ataque de instala um *malware* em um dispositivo informático, normalmente baixado por meio de um sítio aparentemente legítimo na *internet*, que sequestra o acesso a dados armazenados naquele sistema, exigindo um resgate que deve ser pago por criptomoedas em determinado prazo, sob a ameaça de destruição de todos os dados e informações capturadas pelos atacantes. Esta técnica foi instrumentalizada para invadir o sistema Processo Judicial Eletrônico (PJe) do Tribunal de Justiça do rio Grande do Sul.

Por seu turno, o "comportamento é uma ação realizada por meio de uma ou mais técnicas, cometida por um ou mais agentes, por ação ou omissão, em face de redes de computadores, dispositivos informáticos ou sistemas informatizados. No mesmo exemplo citado acima, por meio da técnica *sql injection*, o agente praticou o comportamento 'invasão de sistema informático'"(DAMÁSIO; MILAGRE, 2016).

O comportamento de um criminoso pode ser tanto ativo, a exemplo de ataque invasivo direto a uma rede de computadores, quanto passivo, a exemplo da inserção em página legítima da *web* de uma "isca", um *malware* escondido em um anúncio que, após um clique de uma pessoa que esteja navegando por aquela página, causará algum tipo de dano ao sistema operacional da vítima, como um *ramsonware*, por exemplo, a fim de utilizar a legitimidade daquele domínio como isca para "pescar" suas vítimas.

Finalmente, a ideia de "crime (engloba) um ou vários comportamentos, utilizando-se de uma ou mais técnicas, que ofendem um ou mais bens ou objetos jurídicos protegidos pelo Direito. Mantendo o mesmo exemplo, a 'invasão de sistema informático' pode ser ou não considerada crime, dependendo do país em que é praticada".

Portanto, o comportamento é a ação que utiliza uma técnica como uma arma para se perpetrar um crime informático, não constituindo uma técnica um crime em si mesma.

A fim de se proteger o bem jurídico, é de fundamental importância o estudo acerca as técnicas mais relevantes, bem como condutas que criminosos possam utilizar, pois isso oferece um norte aos legisladores, investigadores, juízes e demais profissionais da segurança da informação.

Diante disso, é necessário estudar algumas condutas que podem ser consideradas relevantes para o Direito Digital. Dentre elas, podem ser elencadas:

1. Acesso ilegítimo: acesso sem autorização, não necessariamente com a violação de medidas de segurança (invasão). O acesso deve ter intenção ilegítima.

2. Interceptação ilegítima: uso de meios técnico, em transmissões não públicas para interceptar e capturar informações.

3. Interferência de dados (dano informático): ato intencional e ilegítimo realizado por um ou mais agentes, no escopo de danificar, apagar, deteriorar, alterar ou eliminar dados informáticos.

4. Interferência em sistemas: conduta daquele que, dolosamente, causa obstrução grave, intencional e ilegítima, ao funcionamento de um sistema informático, por meio de introdução, transmissão, danificação, eliminação, deterioração ou supressão de dados informáticos

5. Uso abusivo de sistemas: produzir, vender, obter, utilizar, importar ou distribuir dispositivo ou programa informático concebido para prática de outras condutas criminosas ou mesmo senhas, códigos de acesso e dados informáticos que permitam o acesso indevido a sistemas.

6. Falsidade ou fraude informática: introdução, alteração, eliminação ou supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que sejam considerados ou utilizados legalmente como se fossem autênticos.

7. Burla informática: ato intencional e ilegítimo, do qual origine dano, mediante introdução, alteração, eliminação ou supressão de dados informáticos, ou qualquer intervenção no sistema informático com a intenção de benefício econômico. É também conhecida como sabotagem informática.

8. Furto de dados ou vazamento de informações: copiar ou mover, indevidamente, informações protegidas ou confidenciais.

9. Pichação informática ou *defacement*: Conduta daquele que indevidamente altera layout de páginas web, sites e *intranets*. Na grande maioria das vezes a pichação pressupõe uma invasão.

10. Envio de mensagens não solicitadas: Também conhecido como spam, consiste no envio de mensagens não solicitadas por qualquer meio, principalmente e-mail, e que de algum modo possam causar dano ou prejuízo a outrem. Não existe legislação no Brasil para o spam.

O uso indevido de sistemas informáticos, ainda que autorizado, possibilita a ocorrência de prejuízo ao titular ou cessionária do sistema, atrapalhando seu funcionamento, ou causando prejuízo a terceiros que utilizam o sistema, atentando contra seu perfeito funcionamento ou disponibilidade. Embora tenhamos fragmentos normativos, não se tem um único tipo penal que se amolde com simetria nas condutas informáticas.

Ainda há que se falar que as condutas descritas nos tipos penais inseridos no Código Penal pela Lei n. 12.737/2012 trazem a distinção entre os crimes informáticos próprios e os crimes informáticos impróprios. Os tipos penais previstos na Lei n. 12.737/2012 são crimes afetos, via de regra, à categoria de crimes informáticos próprios, onde o bem jurídico protegido é a segurança dos dispositivos e dados informáticos, sendo o crime informático o ato típico, antijurídico e culpável por meio ou contra a tecnologia da informação. No crime informático, a informática é o bem ofendido ou meio para ofensa de bens jurídicos.

Nas hipóteses de sistemas informáticos serem utilizados como ferramentas para a prática de outras condutas típicas, como furtar valores de uma conta bancária utilizando dados ilicitamente obtidos do celular de uma vítima, o furto dos dados é apenas um acessório para a obtenção dos valores depositados em conta bancária. Mesma situação ocorre em um estelionato praticado por meio de sites clonados, que são criados com características de sites de empresas conhecidas e confiáveis, mas são utilizados por agentes criminosos para a obtenção de dados e informações sobre contas bancárias e cartões de créditos daqueles que acessaram o domínio virtual.

Aí reside a diferença entre crime informático e crime da internet: os crimes informáticos são praticados com o objetivo de causar dano a sistema informático, já os crimes de internet

encontram nesta um meio para atingir objeto final de dano.

2.4 QUAL A LEGISLAÇÃO BRASILEIRA NORTEADORA DA TUTELA DOS BENS JURÍDICOS INFORMÁTICOS?

Retomando a ideia sociológica do risco, na da sociedade da informação, dados e informações virtuais são indissociáveis das demais esferas da existência humana, uma vez que mais do que dados, contas em redes sociais como Instagram, Twitter, TwitchTv e YouTube representam a vida muitas pessoas, sendo meios de sustento financeiro, são entretenimento e também são as principais plataformas de interação com amigos e familiares. Destarte, também são trampolins para a prática de crimes de ódio, propagação de discursos de ódio, disseminação de desinformação (*fake news)*, estelionatos, campanhas de difamação, etc.

Isso denota que estas ferramentas necessitam de regulamentação estatal própria, para que bens jurídicos caríssimos aos usuários não fiquem completamente relegados à regulamentação interna das empresas detentoras das plataformas virtuais.

Todavia, a proteção dos valores que as pessoas projetam no ambiente virtual inicia-se fora do ambiente do Direito Penal. A boa doutrina esclarece que o âmbito penal deve ser a última ratio do Direito, sendo esta a característica de um Estado Democrático de Direito, que não instrumentaliza a *persecutio criminis* como uma simples ferramenta de coerção social e de agressão a dissidentes, opositores, críticos ou pessoas que tenham dificuldades de se encaixar aos padrões jurídicos a eles impostos.

Mencionado na Introdução, o Direito Penal moderno se ocupa de delimitar quais bens jurídicos são essenciais para a proteção. Formalmente, tal decisão é fica a cargo dos legisladores, uma vez que o Brasil adota a legalidade estrita, que determina que “não há crime sem lei que o defina nem pena sem a devida cominação legal” (art. 5°, XXXIX, da CF/88).

Diante disso, o juízo de valor positivo sobre o que deve ser protegido como bem jurídico fica a cargo dos representantes políticos do povo, uma vez que a escolha dos legisladores, pelo menos formalmente, reflete os desejos daqueles que os elegeram.

Assim, em uma sociedade democrática, espera-se que seus líderes e representantes, eleitos pelo povo, criem mecanismos legais que instituam políticas públicas voltadas à proteção dos valores e ideias que acreditem ser mais relevantes.

Por óbvio, mudanças de caráter econômico, fatos históricos relevantes supervenientes durante o curso do tempo mudarão a perspectiva daquilo que valioso e deve ser protegido, e isto aponta que os bens jurídicos nascem, de fato, fora da disciplina Direito Penal.

A norma penal não é alheia ao decurso do tempo. O direito penal do inimigo, típico de nações traumatizadas por guerras e violentos conflitos, ocorridos principalmente nos séculos XIX e XX, deu lugar a uma visão garantista, segundo a qual a punição deve ser proporcional à gravidade do delito e não deve, jamais, violar os direitos fundamentais do apenado.

Tal evolução ocorreu principalmente devido à influência da Declaração Universal dos Direitos Humanos, aprovado em dezembro de 1948 pela Organização das Nações Unidas. A influência deste documento na esfera penal foi a necessidade de reconhecer os direitos intrínsecos da condição de ser humano, o que anteriormente era negada àqueles que figuravam no banco dos réus em um processo penal. Violavam-se bens jurídicos do condenado com a finalidade de vingar o dano à bens jurídicos de terceiros.

No sistema jurídico-penal pátrio, compete ao Poder Judiciário apreciar a ameaça ou lesão a direito, momento no qual também tem a função de delimitar bens jurídico-penais (art. 5°, XXXV, da Constituição Federal), sendo que ao analisar e julgar os casos concretos, os juízes têm o poder de distinguir os fatos que violam direitos e como fazer para sancionar o infrator sem que os direitos dele sejam deixados ao relento.

Como mencionado em capítulos anteriores, o bem jurídico informático ganhou status, uma vez que se tornou o motor da sociedade da informação, e passou ser protegido por Lei, notadamente, pela Lei penalizadora.

Todavia, apesar do crescimento da legislação no que penaliza a violação de direitos digitais, a tipificação desacompanhada de políticas públicas é inócua para o Direito, porque não se não concretiza a tutela de bens jurídicos digitais unicamente com o viés punitivo, mas sim com o entroncamento da popularização das tecnologias e educação acerca da segurança em ambientes virtuais, tendo-se como paradigma a proteção de direitos fundamentais já existentes, bem como dos valores criados a partir da nova era digital.

Como dito no primeiro capítulo, os bens jurídicos são constituídos após a valoração de ideias que são alçadas ao posto de essenciais para o funcionamento de uma determinada sociedade, sendo que cabe ao Estado, por meio do Poder Legislativo, traçar parâmetros normativos para proteção e promoção desses valores, que passam a ser considerados direitos.

No Brasil, a Lei 12.965/2014, o Marco Civil da Internet, foi a primeira iniciativa direcionada a regulamentar o uso e divulgação de conteúdo na internet. O art. 2° determina que o uso da internet no Brasil é disciplinado pelos seguintes princípios:

> "I - reconhecimento da escala mundial da rede;
> II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
> III - a pluralidade e a diversidade;

> IV - a abertura e a colaboração;
>
> V - a livre iniciativa, a livre concorrência e a defesa do consumidor;
>
> VI - a finalidade social da rede", sendo que o art. 3° estabelece como princípios básicos."(BRASIL, 2014)

Já o art. 3°, estabelece as seguintes garantias aos usuários da internet no Brasil:

> "I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei."(BRASIL, 2014)

Posteriormente, o advento da Lei n.° 13.704/2018, a Lei Geral de Proteção de Dados – LGPD, trouxe uma regulação para a proteção de dados dos internautas, além de instituir a criação da Autoridade Nacional de Proteção de Dados – ANPD, órgão responsável por fiscalizar o tratamento de dados coletados nos domínios virtuais operados no Brasil.

A LGPD traz, no Capítulo II normas de tratamento de dados, cobrindo desde a caleta, processamento, armazenamento de utilização, o Capítulo IV regulamenta esse tratamento pelo Poder Público, o Capítulo III elenca direitos dos usuários e o Capítulo VII as políticas de segurança e normas de boas práticas no tratamento da informação.

Todo esta convergência do ordenamento jurídico aponta para uma regulamentação do uso da internet, fundamentado no respeito aos direitos e garantias fundamentais e ao livre desenvolvimento da sociedade brasileira, objetivando limitar a influência do *Big Tech* na vida dos cidadãos.

Ocorre que é função do Poder Executivo implementar o sistema normativo de proteção aos bens jurídicos aprovado pelo Legislativo e, por fim, função do Poder Judiciário resolver conflitos envolvendo a aplicação das normas e aplicar sanções civis e penais nos casos necessários. O fim de todas essa proteção deve ser garantir que os cidadãos possam usufruir de seus direitos no ambiente virtual ou fora dele.

Os referidos textos normativos fornecem um norte para a elaboração e aplicação de políticas públicas voltadas à segurança, respeito a direitos fundamentais e normas de funcionamento da internet e tratamento de dados no Brasil, mas não esgotam esta complexa matéria, uma vez que a positivação do Direito Digital não basta para a proteção dos cidadãos.

A efetiva proteção de qualquer direito, demanda a estruturação do sistema jurídico

nacional em torno da causa que motivou seu reconhecimento como valor social, sendo necessária a coordenação de todos os poderes para sua efetivação.

Dito isto, a tutela de bens jurídicos digitais deve ser escorada nos seguintes fundamentos:

1) Produzir normas que conceituem e delimitem bens jurídicos informáticos e tipificação penal de condutas que sejam agressivas a eles; e
2) Criação de políticas públicas, encorporadas no Poder Executivo, voltadas à promoção dos bens jurídicos informáticos por meio da proteção dos direitos fundamentais dos usuários da internet e do combate a desinformação.

A Magna Carta de 1988, em seu art. 48, inciso XII, atribuiu ao Poder Legislativo edição de conteúdo normativo referente às telecomunicações e radiodifusão, o que conferiu a este Poder a titularidade da regulamentação inicial das redes de computadores.

Neste século, o Brasil avançou significativamente na produção de conteúdo normativo voltado à proteção de bens jurídicos no âmbito virtual, bem como reconheceu a legitimidade de bens e valores imateriais, sendo que principais leis que afetam o Direito Penal Digital são as elencadas nos tópicos a seguir:

- Lei 9.983/2000: modificou o Código Penal a fim de tornar crime a divulgação indevida de informações sigilosas ou reservadas (art. 153, § 1°); a inserção de dados falsos, alteração ou exclusão de informações constantes em sistemas informáticos da Administração Pública, praticado por funcionário público; e a alteração ou modificação de "sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente" (art. 313-B). (BRASIL, 2000)
- Lei 10.764/2003: inseriu no Estatuto da Criança e do Adolescente – Lei 8.069/1990 – a tipificação da pornografia infantil, que inseriu o art. 241, no qual fora criminalizada a divulgação, por qualquer meio de comunicação, inclusive a internet, de conteúdo sexual ou cena de sexo explícito envolvendo crianças ou adolescentes. Posteriormente, a Lei 11.829/2008 modificou o art. 241, agravando suas penas, bem como inseriu o art. 241-A, que, em seu inciso II, criminaliza a conduta de quem "assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo".(BRASIL, 2003)
- Lei 12.737/2012: esta lei modificou o Código Repressivo, instituindo como crime a invasão de dispositivo informático (art. 154-A), "conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita".(BRASIL, 2012)

Ainda mais relevantes que a tipificação de condutas criminosas, as Leis 12.965/2014 (Marco Civil da Internet) e 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) trouxeram parâmetros para a efetivação de direitos e garantias fundamentais em âmbito virtual, bem como reconheceram a necessidade de se promover os direitos e garantias fundamentais de todos aqueles que utilizem a rede mundial de computadores.

O primeiro diploma legal estabelece, em seu art. 3°, princípios da rede, pautados nos direitos humanos, como a liberdade de expressão, a proteção à privacidade, a inviolabilidade do sigilo das informações transmitidas via internet; sendo que o segundo cria normas e diretrizes para a coleta, armazenamento e processamento de dados e informações das pessoas que trafegam pela *web*.

Por seu turno, a Lei 11.829/2008, de foi promulgada para modificar o Estatuto da Criança e do Adolescente com a finalidade de facilitar o combate à pornografia infantil e enrijecer as penas aplicáveis a quem praticar os crimes de produção, filmagem, armazenamento e distribuição de cenas de sexo explícito ou conteúdo envolvendo crianças. A grande novidade desta lei foi a inclusão no c*aput* do art. 241-A o uso de sistemas informáticos como crime para quem "oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar" conteúdo pornográfico ou cenas de sexo entre crianças e adolescentes.

Já a Lei 12.737/2012, veio tipificar penalmente a violação dos bens jurídicos digitais, nos quais os danos a esses valores são o cerne da conduta, através da previsão em dispositivo penal da invasão de dispositivo informático e também com a criminalização da comercialização de distribuição de *softwares* maliciosos (art. 154-A, *caput* e §1°).

Episódio que deu o nome popular de Carolina Dieckmann a Lei 12.737/2012, foi famoso caso de invasão de dispositivo informático, com a extorsão da nomeada artista, que teve fotos íntimas divulgadas na internet após ter se recusado a pagar um "resgate" pelo conteúdo furtado de seu *laptop*.

Estes avanços precisam ser complementados com criação de políticas públicas que tornem efetivas as determinações dos legisladores, que buscam responder à demanda da sociedade por segurança nas redes sociais.

A estruturação normativa, regulamentação de fornecimento de acesso e uso de dados compartilhada na rede, necessita ser implementada por um cultivo de uma cultura de segurança e valorização das informações digitais, com a criação de sistemas de investigação e repressão a crimes digitais, integrando as polícias e Ministério Público por meio do uso de inteligência para coletar informações necessárias para prevenção de crimes mais graves.

A criação da Autoridade Nacional de Proteção de Dados – ANPD, órgão do Poder

Executivo, submetido à Presidência da república, determinada pela Lei 13.709/2018, foi o começo da implementação da cultura de proteção das pessoas que utilizam a internet. Esta Lei atribuiu à ANPD um status próximo ao de uma agência reguladora e a competência para elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade (art.55-J, III). Além disso, dispõe o artigo 2° do Decreto n° 10.474/2020 acerca da competência da ANPD para a fiscalização e a implementação da Política Nacional de Proteção de Dados, bem como na promoção da informação acerca.

Apesar do notório avanço, este órgão de natureza transitória (art. 55-A, §§1° e 2° da LGPD), com a direta interferência da Presidência da República, torna o início deste órgão excessivamente capturado pelas amarras dos interesses políticos do momento. Dessa maneira, a implementação de políticas públicas para promoção de bens jurídicos, da mesma maneira que os crimes informáticos, estarão a caminhar em sintonia com os interesses políticos do ocupante da chefia do Poder Executivo.

As diretrizes que vierem a ser elaboradas pela ANPD devem incluir a implementação de uma cultura de segurança dos usuários da rede, pautada nos diplomas legislativos, objetivando a criação de uma cultura de segurança precursora da defesa do direito à intimidade na *web*.

Parte importante de qualquer política pública deve ser o combate a desinformação, que se transformou em um dos principais problemas brasileiros e trouxe gravíssimas consequências durante a pandemia de COVID-19.

Durante a maior pandemia do séc. XXI, o Brasil teve suas redes sociais, notadamente, o aplicativo de mensagens instantâneas WhatsApp, inundadas por mentidas escritas em uma estrutura textual parecida com as notícias jornalísticas. Dentre elas, destacam-se a mentira do *chip* chinês para controle da população, a afirmação falsa de que vacinas podem causar o Mal de Alzheimer e a alegação que a vacina contra o Sar-Cov-2 teria a finalidade de eliminar parte da população mundial.

Ademais, campanhas de informações falsas danificam a própria legitimidade do Estado Democrático de direito. SOARES, A. O.; e OLIVEIRA, P. O., explicam a operação das redes de informações falsas ocorre por meio de agências, como a Cambridge Analytica. Estas agências exploram a psicometria, fenômeno que explora que utiliza informações mineradas em bancos de dados públicos ou privados para traçar um perfil psicológico das pessoas que utilizam a *world wide web,* calcular as reações possíveis desse público-alvo diante de certos conteúdos, com base em probabilidade e estatística. Consecutivamente, essas agências direcionam conteúdo para aquele grupo, a fim de observar se o comportamento esperado será adotado.

Apesar da gravidade desse tipo de conduta, que explora vulnerabilidades e transforma o

ser humano em um mero acessório no processo de tomada de decisões, principalmente nas escolhas políticas, não há um real esforço para se combater a exploração desse tipo de atividade no Brasil.

Foram necessárias a publicação de notícias explicando à população as inverdades às quais estavam submetidas, como na reportagem do portal de notícias UOL "Culpa do Bill Gates? Como nasceu a *fake news* do chip na vacina e magnetismo"; ou nos boletins informativos da FioCruz "Conheça 6 '*fake news*' sobre as vacinas contra Covid-19" , um dos principais institutos de pesquisa científica do Brasil. Além disso, o Instituto Butantan publicou o estudo "*Efficacy and Safety of a COVID-19 Inactivated Vaccine in Healthcare Professionals in Brazil: The PROFISCOV Study*", demonstrando que até 96% das mortes pela doença ocorrem em grupos não vacinados da população.

Recentemente, a Lei n° 14.197/2021, que alterou o Decreto-Lei n° 2.848/1940 para incluir alguns dos crimes previstos na revogada Lei de Segurança Nacional, trazia a tipificação da "comunicação enganosa em massa", dispositivo vetado Presidente da República, situação que demonstra a falta de comprometimento real dos representantes do Estado no combate a essa prática.

3 CONSIDERAÇÕES FINAIS

Apesar da crescente tipificação penal, o número de crimes informáticos está em expansão no Brasil, acompanhando uma tendência mundial de alta, de acordo com relatório da empresa de segurança digital Norton Cybersecurity (SYNMANTECH, 2015).

O Poder Legislativo já atendeu a diversas demandas por regulamentação dos ambientes informatizados, sendo que normas foram elaboradas e incorporadas ao sistema jurídico brasileiro.

No entanto, o ambiente virtual continuará a se manter inseguro, quase que completamente, até que políticas públicas efetivas sejam implementadas para efetivar a proteção almejada pela legislação, situação que demonstra a necessidade de uma construção de uma cultura de segurança nas redes, com a finalidade de instruir usuários e criar mecanismos para reduzir o sucesso de ataques e invasões a computadores e celulares.

Essa cultura, todavia, deve ter supedâneo em políticas públicas direcionadas aos valores socialmente relevantes a serem protegidos, sendo que tais valores são precipuamente aqueles elencados na Constituição Federal, no Marco Civil na Internet e na LGPD, notadamente a intimidade e a inviolabilidade das comunicações e correspondências.

O primeiro grande órgão brasileiro de proteção de dados, ANPD, precisa criar parâmetros rígidos de controle da regularidade sobre o fluxo de informações na rede, de modo a minimizar o mal uso de dados e informações em tráfego para a prática de ilícitos, bem como instituir uma política nacional de combate à desinformação.

Desse modo, há que se perseguir a redução do impacto do direito penal na coletividade por meio da efetivação de direitos e garantias legais e seguir princípios jurídicos, evitando-se o agigantamento do Estado policial repressivo para além do necessário, enquanto se resguarda a população da invasão do Estado em âmbito privado.

Todavia, o estudo dos crimes informáticos é extremamente árdua, de modo que cada conduta não pode ser extraída de seu contexto e ambiente virtual. Este ambiente é o ecossistema no qual um *software* é construído, e diz respeito ao sistema do algorítimo matemático utilizado para estruturar um site ou aplicativo qualquer.

Esse ecossistema não é sólido e definitivo, uma vez que a *web* muda a todo momento, sendo a imutabilidade e a inconstância um marco sociológico dessa sociedade da líquida, pautada no consumo de informação e desinformação, o que demanda um foco permanente do Estado na governança, isto é, estudo, elaboração de políticas, implementação e avaliação dos planos traçados, com a finalidade de que aos poucos a proteção aos bens jurídicos existentes em

âmbito virtual venham a se tornar um pilar consolidado do direito e da política criminal brasileira.

REFERÊNCIAS

GODOY, R. M. B de. **A proteção dos bens jurídicos como fundamento do Direito Penal.** São Paulo, 2010. PUC.

VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático**. Belo Horizonte. Faculdade de Direito da UFMG. 2001.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de Crimes Informáticos**. São Paulo. Saraiva. 2016.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. **Direito Civil: teoria geral**. 7 ed. Rio de Janeiro: Lumen Juris, 2008.

PRADO, Luiz Régis. **Bem Jurídico-Penal e Constituição 8ª edição**. Rio de Janeiro. Editora Forense. 2018.

NUCCI, Guilherme de Souza. **Manual de Direito Penal**. 16ª edição. Rio de Janeiro. Forense. 2020.

ROXIN, Claus. **A proteção de bens jurídicos como função do Direito Penal**. Tradução por A. L. Callegari e N. J. Giacomolli. J 2ª edição.. Porto Alegre. Livraria do Advogado. 2008.

LEVY, Pierre. **Cybercultura**. Traduzido por Carlos Irineu costa. São Paulo. São paulo. 34. 1999.

ZAMPIER, Bruno. **Bens Digitais**. São Paulo. Foco. 2021.

BAUMAN, Zygmunt. **MODERNIDADE LÍQUIDA**. Traduzido por Plínio Dentzien. São Paulo. Editora Schwarcz - Companhia das Letras. 2001.

FÜHRER, Maximilianus C. A.; FÜHRER, Maximiliano R. E. **Resumo de Direito Penal – Parte Geral**. São Paulo. Malheiros. 2018.

DAVID, Marília Luz. Sobre os conceitos de risco em Luhmann e Giddens. Revista Eletrônica de Pós Graduandos em Sociologia Política. UFSC. 2011.

ACHA, Fernanda Rosa. Interdisciplinary Scientific Journal. ISSN: 2358-8411, Nº 6, volume 5, article nº 13.

SOARES, A. O.; OLIVEIRA, P. O. **Os limites da liberdade de expressão: *Fake News* como ameaça a democracia**. Revista de Direito e Garantis Fundamentais. FDV. Vitória. 2019.

PRIVACIDADE HACKEADA. Direção: Karim Amer, Jehane Noujaim. Estados Unidos da América. 2019. Documentário. 116 min.

O DILEMA DAS REDES. Direção: Jeff Orlowski. Estados Unidos da América.2020. Documentário. 94 min.

FRANCE PRESS. Cambridge Analytica se declara culpada em caso de uso de dados do

Facebook. Portal G1. Rio de Janeiro. 09/01/2019. Disponível em <https://g1.globo.com/economia/tecnologia/noticia/2019/01/09/cambridge-analytica-se-declara-culpada-por-uso-de-dados-do-facebook.ghtml>. Acesso em: 20/09/2021.

Kshetri, Nir (2015). **"Cybercrime and Cybersecurity Issues in the BRICS Economies,"** Editorial. Journal of Global Information Technology Management (JGITM), 18(4).

MICHAELIS, C.; MICHAELIS, H. **Dicionário Michaelis**. Melhoramentos. 2021. Disponível em <https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/bem>. Acesso em: 19/10/2021

Editorial. Journal of Global Information Technology Management (JGITM). 2015. Disponível em <https://www.tandfonline.com/doi/10.1080/1097198X.2015.1108093>. Acesso em: 29/09/2021.

United Nations -UN. Cybercrime. ***University Module Module 1: Key issues: Cybercrime in a brief Series***. Doha. 2019. Disponível em <https://www.unodc.org/e4j/en/tertiary/cybercrime.html>. Acesso em: 19/10/2021.

GOMES, Acsa. **TSE sofre com ataque hacker coordenado**. Olhar Digital. 16/11/2020. Disponível em **<**https://olhardigital.com.br/2020/11/16/seguranca/tse-sofre-com-ataque-hacker-coordenado**>**. Acesso em: 19/10/2021.

WERNECK, Natasha. **Caminhoneiros bolsonaristas choram com *fake news* de estado de sítio**. Correio Brasiliense. Brasília. 09/09/2021. <https://www.correiobraziliense.com.br/politica/2021/09/4948617-caminhoneiros-bolsonaristas-choram-com-fake-news-de-estado-de-sitio.html>. Acesso em: 09/09/2021.

_____.**Ataque Cibernético ao TJ-RS quer US$ 5 milhões para não vazar dados**. Portal Telesíntese. 30/04/2021. <https://www.telesintese.com.br/tj-rs-recupera-sei-apos-ataque-cibernetico-ransomware/>. Acesso em 28/09/2021.

VASCONCELOS, Rosália. **Culpa do Bill Gates? Como nasceu *fake news* da vacina com *chip* e magnetismo**. Tilt/UOL. 17/06/2021. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2021/06/17/a-culpa-e-de-bill-gates-saiba-como-nasceu-a-fake-news-da-vacina-com-chip.htm>. Acesso em: 20/06/2021.

MONTEIRO, Daniele. **Conheça 6 'fake news' sobre as vacinas contra a Covid-19**. FIOCRUZ. 22/04/2021. Disponível em: <http://informe.ensp.fiocruz.br/noticias/51261>. Acesso em 10/09/2021.

Editorial. **No Brasil, 96% das mortes por Covid-19 são de quem não tomou vacina; só imunização coletiva pode controlar a pandemia**. Instituto Butantan. 12/08/2021. Disponível em: <https://butantan.gov.br/noticias/no-brasil-96-das-mortes-por-covid-19-sao-de-quem-nao-tomou-vacina--so-imunizacao-coletiva-pode-controlar-a-pandemia>. Acesso em 10/09/2021.

BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 29/09/2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 29/09/2021.

BRASIL. **Lei n° 12.965, de 23 de abril de 2014**. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 29/09/2021.

BRASIL. **Lei n° 8.069 de, de 13 de julho de 1990**. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 29/09/2021.

BRASIL. **Lei 12.737 de 2012**. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 29/09/2021.