O DIREITO PENAL NA QUARTA REVOLUÇÃO INDUSTRIAL: A EXPANSÃO RAZOÁVEL FRENTE AOS CRIMES CIBERNÉTICOS

CRIMINAL LAW ON THE FOURTH INDUSTRIAL REVOLUTION: THE REASONABLE EXPANSION AGAINST CYBER CRIMES

Paulo Roberto Aguiar de Lima Filho
UFPE

Resumo

A Quarta Revolução Industrial é uma realidade, ainda que a maioria das pessoas não se dê conta disso. Cada vez mais, informatizamos a vida humana, originando-se uma fertilidade nunca antes vista para a atuação criminosa por meio da tecnologia da informação ou contra esta. O presente trabalho busca inserir o Direito Penal no contexto da Revolução 4.0, abordando alguns pressupostos fundamentais, como as ideias de bem jurídico e sua exclusiva proteção, bem como a de expansão razoável do Direito Penal a partir da concepção de tecnologia da informação como bem importantíssimo à sociedade que requer proteção jurídico-penal. Levando-se isso em consideração, trata-se de abordar o tema dos crimes cibernéticos, analisando-se a possível existência de uma deficiência da legislação penal, para tanto sendo tomadas como parâmetros a Convenção de Budapeste e a CPI dos Crimes Cibernéticos.

Palavras-chave

Direito Penal. Quarta Revolução Industrial. Crimes cibernéticos. Convenção de Budapeste.

Abstract

The Fourth Industrial Revolution is a reality, even though most people don't realize it. Increasingly, we informatize human life, giving birth to a fertility never before seen in respect to the criminal activity through information technology or against it. The present work aims to insert Criminal Law in the context of the Industry 4.0, addressing some fundamental assumptions, such as protected legal interest and its exclusive protection, as well as the reasonable expansion of Criminal Law, from the conception of information technology as a very important asset for the society, requiring legal-penal protection. Taking this into account, the work deals with addressing the theme of cybercrimes, analyzing the possible existence of a deficiency in the brazilian Criminal Law, taken the Budapest Convention and the brazilian Parliamentary Inquiry Commission on Cybercrimes as parameters.

Keywords

Criminal Law. Fourth Industrial Revolution. Cybercrimes. Budapest Convention.

INTRODUÇÃO

As palavras voam, os escritos permanecem. Esse aforismo, segundo alguns concebido em um discurso do senador Romano Caio Tito[1], revela-se verdadeiro com relação ao filósofo Heráclito de Éfeso, o qual imortalizou em seus fragmentos algumas das mais célebres frases de todos os tempos, muitas delas destacando a mutabilidade das coisas: "não se pode entrar duas vezes no mesmo rio, pois novas águas estão sempre fluindo"; "todas as coisas estão em constante fluxo"[2].

Talvez sua concepção sobre a essência de tudo possa ter sido dificilmente apreendida num período em que as coisas se moviam em uma velocidade bastante lenta se comparada à que se tem revelado nesses últimos tempos. Com efeito, o mundo conhecido era, ao mesmo tempo, maior e menor, conforme lição de Eric Hobsbawm[3]: era menor geograficamente, em virtude de só se conhecer parte do mundo habitado; e demograficamente, por ser a população bastante menor em termos numéricos. Era maior, todavia, em termos de comunicação e praticidade, não dispondo de meios de transporte ou de formas de comunicação aptas a conectar pessoas e distâncias em tempo hábil.

E, como tudo muda, o fluxo de mudanças em si também mudou. Existe hoje um processo de diferenciação extraordinariamente mais rápido na sociedade: tecnologias, crenças, instituições e relações encontram-se em um estado de imensa volatilidade. A nível de ilustração, cite-se o exemplo do professor Yuval Noah Harari:

---

[1] TROLLOPE, Anthony. The Last Chronicles of Barset: The Chronicles of Barsetshire, Oxford, University Press, 2014, p. 759

[2] RUSSEL, Bertrand. História do pensamento ocidental: a aventura dos pré-socráticos a Wittgenstein, Rio de Janeiro, Ediouro, 2001, p. 29.

[3] Apesar de formulada sobre a década de 1780, é logicamente aplicável ao mundo dos pré-socráticos. HOBSBAWM, Eric J. A era das revoluções: 1789 – 1848, Rio de Janeiro/São Paulo, Paz e Terra, 2019, 41ª ed. p. 27-30.

> Se, por exemplo, um camponês espanhol tivesse adormecido no ano 1000 e despertado quinhentos anos depois, ao som dos marinheiros de Colombo a bordo das caravelas Niña, Pinta e Santa Maria, o mundo lhe pareceria bastante familiar. Apesar das muitas mudanças na tecnologia, nos costumes e nas fronteiras políticas, esse viajante da Idade Média teria se sentido em casa. Mas se um dos marinheiros de Colombo tivesse caído em letargia similar e despertado ao toque de um iPhone do século XXI, ele se encontraria em um mundo estranho, para além de sua compreensão. "Estou no Céu?", ele poderia muito bem se perguntar, "Ou, talvez, no Inferno"?[4]

Em complemento à lição do autor, pode-se imaginar alguém que tenha adormecido na década de 1950 e acordado em 2019[5]. O mundo seria completamente outro: computadores portáteis, televisões mais finas (enquanto pessoas mais gordas), smartphones – em cujas telas todo o conhecimento produzido pela humanidade pudesse ser acessado com alguns toques – aparelhos voadores, impressoras (que imprimiriam desde ideias e teorias a casas e membros do corpo humano) e, talvez mais incompreensível e impactantemente, uma rede de conexões interpessoais

---

[4] HARARI, Yuval Noah. **Sapiens:** Uma breve história da humanidade, Porto Alegre, L&PM, 2017, 29ª ed., P. 257.

[5] O ano de 2019 foi escolhido de propósito, tendo em vista que 2020 não se pode considerar nem de longe um ano típico (ainda que na volatilidade crescente da ordem das coisas), em virtude da pandemia do coronavírus, que atingiu brutalmente todo o planeta Terra no início do ano de 2020. Essa pandemia, conquanto tenha sido, de um lado, um abrupto golpe no cotidiano mundial, foi, por outra perspectiva, uma prova de que os tempos realmente são outros, assim como o são as relações sociais, e tudo que delas consequentemente advém.

baseada numa realidade extremamente complexa: a virtual. Tudo isso com um adicional – a interconectividade de todos esses elementos endêmicos do novo século.

Heráclito poderia enxergar com ainda maior clareza e certo grau de concretização sua perspectiva nos dias de hoje, em que, segundo Harari, há um *perpetum mobila:*

> Nos últimos dois séculos, o ritmo das mudanças se tornou tão rápido que a ordem social adquiriu um caráter dinâmico e maleável. Agora existe em um estado de fluxo permanente. Quando falamos de revoluções modernas, tendemos a pensar em 1789 (a Revolução Francesa), 1848 (as revoluções liberais) ou 1917 (a Revolução Russa). Mas o fato é que, atualmente, todo ano é revolucionário. Hoje, até mesmo uma pessoa de 30 anos pode dizer honestamente a adolescentes incrédulos: "quando eu era jovem, o mundo era completamente diferente". A internet, por exemplo, só se disseminou no início dos anos 1990, há pouco mais de vinte anos. Hoje não podemos imaginar o mundo sem ela.

Apesar das mudanças estruturais, certas coisas permanecem sendo o padrão. Isso acontece com o Direito, que é por excelência o mecanismo apto a ensejar certa estabilidade às relações sociais. Essa afirmação se revela verdadeira até certo ponto, visto que o Direito passa por testes de eficácia constantemente, não sendo raras algumas inovações doutrinárias, jurisprudenciais e legislativas, numa tentativa de adaptar o velho panorama jurídico às novíssimas circunstâncias por que passa a sociedade mundial.

A situação é marcante no Direito Penal, que tem sido instado a lidar com novas formas de criminalidade, sobretudo a cibernética, que,

num mundo hiperconectado, encontra terreno fértil para seu alargamento. Apresentam-se algumas dificuldades de ordem legislativa e investigativa, sobretudo relacionadas à tensão existente entre proteção de bens jurídicos e garantias individuais.

Portanto, destina-se esta exposição a abordar aspectos relevantes desse novo contexto de necessária, porém imprescindivelmente cautelosa expansão do Direito Penal antes os *cybercrimes*, vinculada à Indústria 4.0.

O primeiro tópico trata de inserir o leitor no novo panorama que é a Quarta Revolução Industrial, fazendo uma breve retrospectiva das revoluções anteriores.

O segundo tópico trata do Direito Penal em um momento de tensão: busca-se fazer uma análise de seu objeto de proteção (os bens jurídicos) e, posteriormente, revelar a necessidade de uma expansão razoável em virtude da importância e da necessidade de proteção da tecnologia da informação, que se constitui como um bem jurídico-penal.

O terceiro tópico aborda especificamente os crimes cibernéticos, tratando de conceituá-los, especificá-los, examiná-los enquanto espécies de sua modalidade "própria" e analisar alguns de seus aspectos problemáticos para o Direito Penal. Em seguida, busca-se entender se há alguma deficiência da legislação penal brasileira frente aos crimes cibernéticos, no tocante à sua tipificação, utilizando-se como parâmetros a Convenção de Budapeste e a Comissão Parlamentar de Inquérito dos Crimes Cibernéticos.

1. UM NOVO PANORAMA

Durante muito tempo, apontou-se a existência de apenas duas realidades distintas: a de ordem objetiva e a de ordem subjetiva. Um fenômeno é objetivo quando existe independentemente da consciência e da crença humanas. O ar, o chão, o sol, a arma, o computador e a radioatividade são realidades objetivas. Por outro lado, um fenômeno é

subjetivo quando sua existência depende da consciência e das crenças de um único indivíduo, de modo que desaparece ou muda a depender de se aquele indivíduo em particular muda suas crenças. Os sonhos são uma realidade subjetiva.

A dicotomia deixa de existir, no entanto, quando se dá conta da existência de uma terceira realidade: a realidade de ordem intersubjetiva. Nas palavras do professor Yuval Noah Harari,

> intersubjetivo é algo que existe na rede de comunicação ligando a consciência subjetiva de muitos indivíduos. Se um único indivíduo mudar suas crenças, ou mesmo morrer, será de pouca importância. No entanto, se a maioria dos indivíduos na rede morrer ou mudar suas crenças, o fenômeno intersubjetivo se transformará ou desaparecerá. Fenômenos intersubjetivos não são fraudes malévolas nem charadas insignificantes. Eles existem de uma maneira diferente de fenômenos físicos como a radioatividade, mas seu impacto no mundo ainda pode ser gigantesco. Muitas das forças mais importantes da história são intersubjetivas: leis, dinheiro, deuses, nações.[6]

O direito, realidade intersubjetiva, conforme exposto, sempre lidou com a ocorrência de fenômenos (atos ou fatos) objetivos, ou seja, concretos ou concretizáveis, dotados muitas vezes de aspectos subjetivos, a depender dos quais a relação que se estabelece é totalmente distinta. Um mercador que vende seu produto a um comprador, entregando-lhe o bem mediante determinado pagamento, realiza um contrato de compra e venda.

---

[6] HARARI, Yuval Noah. Sapiens: Uma breve história da humanidade, Porto Alegre, L&PM, 2017, 29ª ed., P. 124-125.

O subjetivismo da relação pode ser levado em consideração, por exemplo, na hipótese de investigação da presença de dolo ou fraude. No Direito Penal, a presença do elemento subjetivo é ainda mais forte: Se A, totalmente culpável, sem causas de justificação e mediante uso de instrumento pérfuro-contundente, com *animus necandi*, causa o óbito de B, estar-se-á diante do crime de homicídio doloso. Dito de outro modo, os elementos subjetivos perfeitos em realidades objetivas, em maior ou menor medida, sempre constituíram a dinâmica jurídica. Entretanto, o dinamismo histórico não admite rigidezes.

Existe hoje uma nova forma de realidade; uma nova dimensão: a dimensão cibernética (virtual ou digital), na qual não há tantas barreiras físicas, e a qual se desenvolve em uma velocidade surpreendente, sendo uma das principais responsáveis pelo que se convencionou chamar "disrupção". Nessa realidade, pessoas e coisas interagem em um nível nunca antes visto, de modo que as distâncias se relativizam, e todas as áreas do agir humano passam por transformações antes inimagináveis. Seres humanos e máquinas trabalham de forma tão estreita e similar, que às vezes se torna difícil restringir certas atividades como exclusividade de somente um dos dois, enjeitando-se o outro.

1.1 INDÚSTRIA 4.0

A sociedade humana, ao longo de sua existência, tem passado por diversas mudanças estruturais, as quais decorrem de alterações em elementos significativos de parte de sua vida. Tome-se como exemplo o que muitos entendem ter sido a primeira grande revolução por que passou o ser humano: a Revolução Agrícola – momento histórico em que começamos a dedicar quase todo nosso tempo e esforço a manipular a vida de algumas espécies de plantas e animais, em detrimento de viver coletando as primeiras e caçando os segundos[7].

[7] *Idem, ibidem,* P. 87.

Posteriormente, vieram modificações agudas no modo como as sociedades se organizam e como seus indivíduos se relacionam, produzem e fazem uso do poder. Duas merecem especial destaque: a Revolução Francesa e a Revolução Inglesa (ou Primeira Revolução Industrial), que, em grande medida, moldaram de maneira reconhecível o mundo como se concebe hoje, com significativo impacto nos modos de produção e nos seus desencadeamentos lógicos.

Quando se fala em Revolução Industrial, fala-se de um período cujo nascimento costumeiramente é estabelecido na década de 1780, em que houve alteração massiva do trato do ser humano com suas confecções, substituindo-se ferramentas por máquinas, pessoas por motores e produção artesanal por industrial – em uma escala nunca antes vislumbrada. Com maestria, leciona Hobsbawm:

> O que significa a frase "a revolução industrial explodiu"? Significa que a certa altura da década de 1780, e pela primeira vez na história da humanidade, foram retirados os grilhões do poder produtivo das sociedades humanas, que daí em diante se tornaram capazes da multiplicação rápida, constante, e até o presente ilimitada, de homens, mercadorias e serviços. Esse fato é hoje tecnicamente conhecido pelos economistas como a "partida para o crescimento autossustentável". Nenhuma sociedade anterior tinha sido capaz de transpor o teto que uma estrutura social pré-industrial, uma tecnologia e uma ciência deficientes, e consequentemente o colapso, a

> fome e a morte periódicas impunham à produção.[8]

Esclarece o autor que o evento iniciado no século XVIII não teve um fim estabelecido; não se "completou": "a mudança revolucionária se tornou norma desde então". [9] Considerando esse importante aspecto da revolução industrial, decidiu-se dividi-la em diferentes fases, sendo certamente a nascida no século XVIII a sua inicial. Sucedeu essa primeira fase a chamada "Segunda Revolução Industrial".

A Segunda Revolução Industrial diz respeito ao período compreendido entre os anos de 1860 e 1914 (o que pode variar um pouco a depender da análise dos autores), no qual houve a invenção (ou a descoberta) de um grande número de tecnologias: "eletricidade, motor de combustão interna, indústrias químicas, ligas, petróleo, ligadas à comunicação elétrica (telégrafo, telefone e rádio) e encanamento interno".[10]

Em trabalho publicado no ano de 1931, no The Economic Journal[11], H. Stanley Jevons sustenta que a Segunda Revolução Industrial se deu a partir da confluência de três ramos epistemológicos distintos. O primeiro seria o desenvolvimento da contabilidade, que deixou de ser uma mera ferramenta de registro de eventos pretéritos para tornar-se uma

---

[8] HOBSBAWM, Eric J. A era das revoluções: 1789 – 1848, Rio de Janeiro/São Paulo, Paz e Terra, 2019, 41ª ed., p. 59.

[9] *Idem, ibidem*. P. 60.

[10] MOHAJAN, Haradhan Kumar. "The Second Industrial Revolution has Brought Modern Social and Economic Developments". Journal Of Social Science And Humanities, v. 6, Chittagong, jan. 2020. Disponível em: https://www.researchgate.net/publication/338670501_The_Second_Industrial_Revolution_has_Brought_Modern_Social_and_Economic_Developments. Acesso em: 01 abr. 2020.

[11] JEVONS, H. Stanley. "The Second Industrial Revolution". The Economic Journal, [s.l.], v. 41, n. 161, Oxford, mar. 1931.

ciência aplicada destinada a ajudar o *businessman*. Em segundo lugar, encontrar-se-ia o esforço dos engenheiros na aplicação das ciências puras a fim de atribuir segurança e economia à construção de pontes, navios etc. Sustenta o autor que métodos antigos, como tentativa e erro, foram substituídos por cálculos e medidas exatos. Por fim, é citado o constante crescimento na competição entre empresas de manufatura e um mercado crescente, de modo que se tornou atrativa a produção em massa.

O escritor americano Jeremy Rifkin, em icônico trabalho denominado The Third Industrial Revolution, sustenta que as grandes revoluções econômicas na história ocorrem quando novas tecnologias de comunicação convergem com novos sistemas de energia. Diante disso, argumenta que na década de 1990 houve o encontro da Internet[12] com formas sustentáveis de energia, dando origem a uma poderosa infraestrutura suficiente para uma Terceira Revolução Industrial. Mas a origem dessa revolução se pode retroagir algumas décadas.

Há quem diga que se iniciou na década de 1950[13], mas aparentemente a gênese dessa terceira revolução encontra-se no fim da década de 1960. Brian H. Roberts[14], pesquisador da Universidade de Camberra, leciona que

---

[12] Por ser aqui mencionada diversas vezes, constituindo o cerne de diversas questões apresentadas, tenha-se em mente Internet como "o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes", nos termos do art. 5º. I, do Marco Civil da Internet (Lei 12.965 de 2014), o qual é o maior arcabouço legislativo a tratar de Internet no Brasil.

[13]**Meet the Three Industrial Revolutions**. Disponível em: https://trailhead.salesforce.com/pt-BR/content/learn/modules/learn-about-the-fourth-industrial-revolution/meet-the-three-industrial-revolutions#:~:text=Beginning%20in%20the%201950s%2C%20the,the%20Internet%E2%80%94the%20digital%20revolution. Acesso em: 29 out. 2020.

[14] ROBERTS, Brian. The Third Industrial Revolution: Implications for Planning Cities and Regions. Disponível em

> Um dos primeiros gatilhos da Terceira Revolução Industrial começou em 1969, com o desenvolvimento da ARPANET (Rede da Agência para Projetos de Pesquisa Avançada), que foi uma rede de comutação de pacotes antecipada e a primeira rede a implementar o conjunto de protocolos TCP/IP. Isso desencadeou o desenvolvimento da Internet, e com isso a era da informação. Similarmente a outras revoluções, a Terceira Revolução Industrial é gerada principalmente por avanços tecnológicos nos fatores de produção, distribuição e energéticos.

"As palavras são testemunhas que muitas vezes falam mais alto que os documentos". Tal sentença foi utilizada pelo historiador Eric Hobsbawm ao medir a importância das Revoluções Francesa e Inglesa a partir do surgimento, naquele período, de novas palavras: '"indústria', 'fábrica', 'classe média', 'capitalismo"' etc., que hoje são de uso corrente. Se tomarmos como exemplo as palavras "internet", "uso de dados", "smatphone", "*drone*", "hacker", "cybersegurança", "download", "software" etc., teremos uma indicação, portanto, de quão importante é a fase por que passa a humanidade. Há quem diga, a propósito, que já estamos vivendo uma nova revolução: a Quarta Revolução Industrial – ou Indústria 4.0.

De acordo com Klaus Schwab[15], fundador e Presidente Executivo do Fórum Econômico Mundial, a despeito das vozes de acadêmicos no sentido de essa Quarta Revolução ser apenas mais um

---

https://www.researchgate.net/publication/275644911_THE_THIRD_INDUSTRIAL_REVOLUTION_Implications_for_Planning_Cities_and_Regions. Acesso em: 06 de abril de 2020.

[15] SCHWAB, Klaus. **A quarta revolução industrial**, São Paulo, Edipro, 2016, P. 12-13.

aspecto da Terceira, há três razões sustentando uma superação, o nascimento de uma Quarta Revolução Industrial. A primeira delas é a velocidade: "ao contrário das revoluções industriais anteriores, esta evolui em um ritmo exponencial e não linear. Esse é o resultado do mundo multifacetado e profundamente interconectado em que vivemos". Completa afirmando que "as novas tecnologias geram outras mais novas e cada vez mais qualificadas". Em segundo lugar, de acordo com o autor, encontram-se a amplitude e profundidade: a Quarta Revolução Industrial "tem a revolução digital como base e combina várias tecnologias, levando a mudanças de paradigmas sem precedentes da economia, dos negócios, da sociedade e dos indivíduos". Argumenta, inclusive, que essa revolução "não está modificando apenas o 'o que' e o 'como fazemos' as coisas, mas também 'quem' somos". Por fim, cita o impacto sistêmico, de modo que a Quarta Revolução Industrial "envolve a transformação de sistemas inteiros entre países e dentro deles, em empresas, indústrias e em toda sociedade".

Pode-se dizer que a Quarta Revolução Industrial teve início na virada do século, baseando-se na revolução digital, a qual se caracteriza por uma "internet mais ubíqua e móvel, por sensores menores e mais poderosos que se tornaram mais baratos e pela inteligência artificial e aprendizagem automática (ou aprendizado de máquina) "[16].

Segundo Schwab,

> As tecnologias digitais, fundamentadas no computador, *software* e redes, não são novas, mas estão causando rupturas à terceira revolução industrial; estão se tornando mais sofisticadas e integradas, e, consequentemente, transformando a sociedade e a economia global. Por esse motivo, os professores Erik Brynjolfsson e Andrew McAfee, do *Massaschussets Institute of Technology*

[16] *Idem, ibidem.*

> (MIT) disseram que este período é "a segunda era da máquina" no título do livro publicado por eles em 2014; estes dois professores afirmam que o mundo está em um ponto de inflexão em que o efeito dessas tecnologias digitais irá se manifestar com "força total" por meio da automação e de "coisas sem precedentes".[17]

Aponta o autor, finalmente, que ondas de novas descobertas ocorrem ao mesmo tempo em áreas que vão "desde o sequenciamento genético até a nanotecnologia, das energias renováveis à computação quântica", sustentando que a fusão das novas tecnologias e a interação entre os domínios físicos, digitais e biológicos é o diferencial dessa incipiente revolução. Prova disso é o que se costuma chamar de Internet das Coisas (*Internet of Things* – IoT), conceito que diz respeito à interconexão dos objetos do dia-a-dia com a internet: eletrodomésticos, roupas, automóveis...[18]Entretanto, não apenas elementos cotidianos básicos hoje se inter-relacionam através da internet. Com efeito, redes militares e civis são responsáveis pelo controle da dinâmica de boa parte da vida estatal: desde a infraestrutura (fontes de energia, redes de eletricidade, saúde, controle de tráfego aéreo e malha ferroviária) até o intercâmbio de conteúdos sensíveis à estrutura do próprio Estado.

À medida que crescem as possibilidades de uso positivo da internet e dos mecanismos próprios à Quarta Revolução Industrial, surgem igualmente problemas cada vez mais complexos. Relevante destaque merecem as atitudes nocivas à segurança, de maneira geral. Em

---

[17] *Idem, ibidem.*

[18] ZAMBARDA, Pedro. **Internet das Coisas**: entenda o conceito e o que muda com a tecnologia. 2014. Disponível em: https://www.techtudo.com.br/noticias/noticia/2014/08/internet-das-coisas-entenda-o-conceito-e-o-que-muda-com-tecnologia.html. Acesso em: 13 abr. 2020.

um mundo hiperconectado, é fértil o espaço para a criatividade delitiva e para a atuação de novos sujeitos desestabilizadores. Estes anteriormente não se poderiam apresentar como verdadeiras ameaças à normalidade da vida humana, mas, por causa da sensibilidade e da virtualidade dos sustentáculos da comunicação e infraestrutura, podem abalar o estado de tranquilidade; podem gerar efeitos catastróficos e impactar significativamente a dinâmica regular de uma sociedade:

> Assim como as armas nucleares a princípio tornaram possível, da mesma forma desenvolvimentos tecnológicos podem criar um cenário para formas inéditas de guerra. Em particular, uma guerra cibernética pode desestabilizar o mundo ao conceder a pequenos países e grupos não estatais a capacidade de lutar com eficácia contra superpotências. Quando os Estados Unidos combateram o Iraque em 2003, levaram o caos a Bagdá e a Mossul, mas nem uma única bomba foi lançada sobre Los Angeles ou Chicago. No futuro, no entanto, um país como a Coreia do Norte, ou o Irã, poderia utilizar bombas lógicas para interromper a transmissão de energia na Califórnia, explodir refinarias no Texas e fazer trens colidirem em Michigan ("bombas lógicas" são códigos de software maliciosos plantados em tempos de paz e operados à distância. É altamente provável que esses códigos já tenham sido contaminados em que controlam

> instalações vitais de infraestrutura nos Estuados Unidos e em muitos outros países).[19]

2. O DIREITO PENAL EM UM MOMENTO DE TENSÃO

Para alcançar seus fins, o Direito prescreve (ou proscreve) condutas, através de proposições normativas inseridas em fórmulas jurídicas[20]. Segundo Rudolf Von Jhering, "a definição usual de direito reza: direito é o conjunto de normas coativas válidas num Estado". Complementa aduzindo que "o conteúdo da norma é um pensamento, uma proposição (proposição jurídica), mas uma proposição de natureza prática, isto é, uma orientação para a ação humana".[21]

Conforme muito conhecida lição do jurista italiano Norberto Bobbio, o Direito é uno e indivisível. Entretanto, como ciência, comporta distinções[22], a fim de ser melhor estudado e a fim de que suas compartimentalizações sejam mais bem esclarecidas.

A depender do valor atribuído a determinados bens, sua proteção será maior ou menor pelo Direito; será mais ou menos enérgica; possibilitará resposta mais branda ou mais severa àqueles que contra si se comportarem, lesivamente. Nesse sentido, sobreleva-se o Direito Penal quando se fala em proteção e retribuição. Assim, é um ilícito jurídico o fato social que contrariar o ordenamento jurídico, sendo o ilícito penal sua

---

19 HARARI, Yuval Noah. **Homo deus**: uma breve história do amanhã, São Paulo, Companhia das Letras, 2016, P. 26.

20 GUSMÃO, Paulo Dourado de. Introdução ao estudo do direito, Rio de Janeiro, Forense, 2015, 46ª ed., P. 83.

21 JERING, Rudolf Von *apud* FERRAZ JÚNIOR, Tércio Sampaio. Introdução ao estudo do direito: técnica, decisão, dominação, São Paulo, Atlas, 2015, 8ª ed., P. 71.

22 REALE, Miguel. **Lições preliminares de direito**, São Paulo, Saraiva, 2002, 27ª ed., P. 339.

modalidade mais grave, por lesar os bens mais importantes dos membros da sociedade[23].

Cara é a lição de Brandão, analisando a perspectiva de Franz von Liszt a respeito da altivez com que responde o Direito Penal às transgressões humanas:

> Prossegue Liszt dizendo que três são as formas de coação do Estado: 1ª execução coativa ou forçada; 2ª restabelecimento das coisas no estado anterior; 3ª pena, como castigo à desobediência. É na terceira forma que o Direito Penal se manifesta O direito penal tem a missão peculiar de aplicar "a defesa mais enérgica dos interesses especialmente dignos e necessitados de proteção, por meio da ameaça e execução da pena, considerada como um mal contra o delinquente".[24]

Mas essa altivez com que o Direito Penal responde a certas transgressões não é desprovida de garantias, como foi outrora. Basta pensa no caso fictício (porém verossímil) de Jean Valjean, descrito por Victor Hugo em Os Miseráveis: por ter roubado uma fatia de pão passou 19 anos sofrendo duras penas; perdendo seu direito de ser considerado gente – isso tudo em nome da lei. Merece transcrição a letra da música "Look Down", do filme homônimo, que relata o diálogo entre Jean Valjean (Hugh Jackman) e o policial Javert (Russell Crowe):

> - Agora, prisioneiro 24601, acabou sua pena e a condicional começa. Você sabe o que isso significa.
> - Sim... significa que estou livre.

---

[23] BITTENCOURT, Cézar Roberto. Tratado de direito penal: parte geral, São Paulo, Saraiva, 2016, 22ª ed., P. 35.

[24] LISZT, Franz von *apud* BRANDÃO, Cláudio. Teoria jurídica do crime, São Paulo, Atlas, 2015, 4ª ed., P. 92.

> - Não! Siga à risca seu itinerário. Esse emblema da vergonha você vai mostrar até morrer. Alerta que você é um homem perigoso.
> - Roubei uma fatia de pão. A criança de minha irmã estava perto de morrer... passando fome.
> - E vai passar de novo, a não ser que você aprenda o significado de lei.
> - Eu aprendi o significado desses 19 anos – um escravo da lei!
> - 5 pelo que você fez, o resto por tentar fugir! Sim, 24601!
> - Meu nome é Jean Valjean![25]

A dura e fria lei, por si só, já não é parâmetro para medir a justiça do Direito Penal. Hoje, concebe-se o Direito Penal no contexto de um Estado Democrático de Direito. Nesse contexto, o Direito Penal tem por função a proteção de bens jurídicos fundamentais[26], sendo isso seu objetivo e, ao mesmo tempo, um destacado princípio que se impõe como limite ao poder punitivo do Estado.

2.1. NOÇÕES SOBRE BEM JURÍDICO

Para Luís Régis Prado, "o Direito Penal é o setor ou parcela do ordenamento jurídico que estabelece as ações ou omissões delitivas, cominando-lhes determinadas consequências jurídicas – penas ou medidas de segurança (conceito formal) ". De outro lado, sustenta o autor, "refere-se também a comportamentos considerados altamente reprováveis ou

---

[25] OS MISERÁVEIS. Direção de Tom Hooper. Produção de Tim Bevan, Eric Fellner, Debra Hayward e Cameron Mackintosh. Intérpretes: Hugh Jackman. Roteiro: William Nicholson. Música: Claude-Michel Schönberg e Anne Dudley. S.I.: Working Title Films, Cameron Mackintosh Ltd. e Relativity Media, 2012. (158 min.), son., color. Legendado.

[26] BITTENCOURT, Cézar Roberto. Tratado de direito penal: parte geral, São Paulo, Saraiva, 2016, 22ª ed., P. 43.

danosos ao organismo social, que afetam gravemente bens jurídicos indispensáveis à sua própria conservação e progresso (conceito material).[27]

A menção ao bem jurídico, hoje tão claramente integrante do conceito material de crime, foi fruto de um longo desenvolvimento teórico, sendo possível distinguir quatro fases, preciosamente exploradas por Cláudio Brandão[28]: a ideia anteriormente dominante, sustentada por Anselm von Feuerbach; o nascimento da ideia de bem jurídico, com Johann Michael Franz Birbnaum; a concepção de *Rechtsgut*, no positivismo de Karl Binding; e a construção do bem jurídico a partir do neokantismo.

Consoante o autor, no início do séc. XVIII, Feuerbach buscou apresentar o objeto de proteção do direito penal, relacionando-se essa proteção com a função que atribuiu ao direito penal. Para Feuerbach, essa função seria a tutela de direitos externos – os direitos subjetivos, os quais, por sua vez, seriam "o conjunto dos direitos privados ou individuais, atribuídos às pessoas que são as titulares desses direitos"[29]. Assim, para o autor, entre os princípios primeiros do direito punitivo situar-se-ia o seguinte "toda pena jurídica dentro do Estado é a consequência jurídica, fundada na necessidade de preservação de direitos externos, de uma lesão jurídica e de uma lei que comine um mal sensível"[30]. Portanto, para Feuerbach, com a ocorrência dessa lesão, o próprio direito seria atingido. "A ação criminosa do homicídio não lesionaria a vida, mas o direito à vida"[31].

Como antítese à posição de Feuerbach, está a teoria do jurista alemão Johann Michael Franz Birnbaum. Este sustentou não se poder afirmar que a missão do direito penal é tutelar os interesses e direitos

---

27 PRADO, Luís Régis. Curso de direito penal brasileiro: parte geral e parte especial, São Paulo, Editora Revista dos Tribunais, 2015, 14ª ed., P. 67.
28 BRANDÃO, Cláudio. Teoria jurídica do crime, São Paulo, Atlas, 2015, 4ª ed., P. 9-16.
29 *Idem, ibidem.*
30 *Idem, ibidem.*
31 *Idem, ibidem.*

subjetivos "porque o direito, em si mesmo, nunca é lesionado". Entretanto, por ser materializado em bens (objetos do direito), estes, sim, podem ser lesionados. Esclarece Brandão:

> Para Birnbaum, somente os bens, e não os direitos podem ser classificados como inatos e adquiridos; logo, somente eles poderão ser lesionados. Por sua vez, se o delito representa uma lesão, seu objeto de tutela não poderá ser o direito, mas somente o bem decorrente do direito. Isso posto, não se pode dizer que o crime, por exemplo, viola o direito à vida, mas somente se pode dizer que ele viola a vida, pois é esta última que será lesionada com a ação criminosa, traduzindo o objeto de tutela penal, isto é, o bem decorrente daquele delito.[32]

Em 1872, época em que vigorava a mentalidade do positivismo jurídico, ou seja, aquela mentalidade na qual se buscava a aplicação do método científico indutivo[33]para a descoberta do conhecimento, Karl Binding construiu a nomenclatura bem jurídico (*Rechtsgut*). Para esse autor e os que comungavam de sua concepção de verdade, "o direito era o que o Estado dizia sê-lo, não buscando nenhum elemento transcendente para pôr em questão a legitimidade do seu conteúdo". Dessa maneira, há um afastamento da concepção apresentada por Birnbaum, segundo a qual o direito daria proteção a um bem anteriormente existente. De acordo com Binding, não haveria bem antes da norma, porquanto caberia ao legislador construir a noção do que viria a ser bem jurídico: "para Binding a norma é

---

[32] *Idem, ibidem.*

[33] BITTENCOURT, Cézar Roberto. Tratado de direito penal: parte geral, São Paulo, Saraiva, 2016, 22ª ed., P. 96.

a única fonte do bem jurídico. Ela o revela e, ao fazê-lo, revela também qual é o objeto de proteção, fazendo a delimitação do conteúdo da lesão. Isto porque esta última – a lesão – será a violação do bem jurídico".

O positivismo não reinou soberano por muito tempo. Em face de uma reação à metodologia do positivismo, surgiu uma nova corrente: o neokantismo. Para essa corrente, deveria haver uma separação metodológica a respeito dos objetos de investigação das ciências naturais e das ciências culturais. Enquanto para os objetos das primeiras se explicará o objeto, para as ciências da cultura se compreenderá o objeto. Sendo todo o Direito uma ciência cultural, a essência conceitual do que seria o bem jurídico estaria nesta esfera (cultural), em que é possível se estabelecerem signos positivos ou negativos aos objetos. A partir dessa ruptura metodológica, a dogmática penal toma as linhas do método neokantiano como base.

O bem jurídico, que se traduz em determinados bens da vida, da comunidade, como a existência do Estado, a vida, a saúde, a liberdade, a propriedade etc., [34]é uma valoração em face do objeto da ação, bem como uma função que visa a esclarecer a finalidade da lei penal. Brandão assevera que "o bem jurídico pode ser definido como o conteúdo material do crime, traduzido no valor tutelado pelo direito"[35]. E o conceito material de crime, por sua vez, é a limitação do poder de punir, no momento em que este se afasta do Direito Penal.

2.2. PRINCÍPIO DA EXCLUSIVA PROTEÇÃO DE BENS JURÍDICOS

A despeito de não ser o único princípio limitador do poder punitivo estatal[36], o princípio da exclusiva proteção de bens jurídicos é

---

[34] WELZEL, Hans. Derecho penal: parte general, Buenos Aires, Roque Depalma Editor, 1956, P. 2.

[35] BRANDÃO, Cláudio. Teoria jurídica do crime, São Paulo, Atlas, 2015, 4ª ed., P. 16.

[36] Bittencourt cita os princípios da legalidade, da reserva legal, da intervenção mínima, da irretroatividade da lei penal, da adequação social, da insignificância, da ofensividade, de

considerado por Santiago Mir Puig como uma das manifestações de uma abordagem político-criminal mais global: a que parte da necessidade de postular o uso mais restritivo possível do Direito Penal, supondo-se a concepção do Direito Penal como um "mal menor", que só seria admissível na medida em que fosse extremamente necessário[37]. Para o autor, considerar-se-ia necessária a intervenção do Direito Penal quando o exigisse a proteção de bens jurídicos-penais. Entende que, para que um bem jurídico seja considerado um bem jurídico-penal, duas são as condições: deve o bem a) revestir-se de suficiente importância social; e b) necessitar de proteção pelo Direito Penal[38].

Essa "extrema necessidade" reflete o que alguns chamam de princípio da fragmentariedade do Direito Penal. Explica Bittencourt:

> Nem todas as lesões que lesionam bens jurídicos são proibidas pelo Direito Penal, como nem todos os bens jurídicos são por ele protegidos. O Direito Penal limita-se a castigar as ações mais graves praticadas contra os bens jurídicos mais importantes, decorrendo daí o seu caráter fragmentário, uma vez que se ocupa somente de uma parte dos bens jurídicos protegidos pela ordem jurídica. Isso, segundo Régis Prado, "é o que se denomina caráter fragmentário do Direito Penal. Faz-se uma tutela seletiva do bem jurídico, limitada àquela tipologia agressiva que se revela

culpabilidade, da proporcionalidade e de humanidade, não sendo aqui destrinchados por acabar distanciando-se um pouco do objeto do presente trabalho. BITTENCOURT, Cézar Roberto. Tratado de direito penal: parte geral, São Paulo, Saraiva, 2016, 22ª ed., P. 49-71.

37 PUIG, Santiago Mir. **El derecho penal en el Estado social y democrático de derecho**, Barcelona, Editorial Ariel S.A., 1994, p. 159.

38 *Idem, ibidem,* p. 162.

> dotada de indiscutível relevância quanto à gravidade e intensidade da ofensa"[39].

Por cominar um exercício de poder coercitivo que impõe privação de direitos[40], como dito linhas atrás, não pode ser o Direito Penal banalizado, somente sendo passível de expansão quando houver circunstâncias que razoavelmente assim exijam, como o surgimento de novos bens jurídicos – situação que se acentua no contexto da Quarta Revolução Industrial.

2.3. A EXPANSÃO RAZOÁVEL

O professor Jesús-Maria Silva Sánchez, catedrático da Universitat Pompeu Fabra, em sua obra "La expansión del derecho penal: aspectos de la política criminal en las sociedades postinudstriales", buscou examinar o fenômeno do crescente uso do Direito Penal para lidar com situações que exsurgem na sociedade pós-industrial, tentando encontrar limites para o uso dessa ferramenta altamente gravosa.

De antemão, é importante observar que os termos sociedade pós-industrial, sociedade de risco, pós-modernidade e Indústria 4.0 estão intimamente relacionados, abordando momentos que podem se suceder cronologicamente, mas que de certa maneira dizem respeito a um mesmo fenômeno: as mudanças trazidas em decorrência da cada vez mais alta volatilidade das relações humanas.

Ato contínuo, segundo o autor, há uma tendência claramente dominante na legislação dos países à introdução de novos tipos penais, bem como um agravamento dos já existentes ou uma reinterpretação das garantias clássicas. Há também uma criação de novos bens jurídicos, a ampliação dos espaços de riscos jurídico-penalmente relevantes, a

---

[39] BITTENCOURT, Cézar Roberto. Tratado de direito penal: parte geral, São Paulo, Saraiva, 2016, 22ª ed., P. 55.

[40] ZAFFARONI, Eugênio Raul *et al.* **Derecho penal**: parte general, Buenos Aires, Ediar, 2002, 2ª ed., p. 45-46.

flexibilização de regras de imputação e relativização dos princípios político-criminais de garantias. Isso tudo reflete aquilo que denomina expansão do Direito Penal[41].

Consoante Silva Sánchez, essa expansão tem diversas causas, tais como o surgimento de novos interesses, a aparição de novos riscos, a institucionalização e a sensação da insegurança etc. – havendo uma multiplicação da expansão em decorrência da globalização econômica e da integração supranacional[42].

Descabidamente, o expansionismo é meramente uma aparente solução fácil aos problemas sociais, revestindo-se de mero simbolismo. Tratando anteriormente de ideia relacionada, Marcelo Neves aborda a noção de "legislação simbólica", que permeou debates na Teoria do Direito e na Ciência Política alemãs[43]. Para esse autor, é simbólica a legislação quando prevalece seu significado político-ideológico latente em detrimento de seu sentido normativo-jurídico aparente.

Levando-se em consideração o perigo do expansionismo e da legislação meramente simbólica e a necessidade da manutenção de garantias, deve-se entender que não há como deixar de criminalizar certas condutas no ambiente cibernético, por tratar-se de nova realidade seguramente carente de proteção e pelo aumento das possibilidades delitivas dentro dessa realidade. Trata-se de uma "expansão razoável":

> El Derecho penal es un instrumento cualificado de protección de bienes jurídicos especialmente importantes. Sentado esto, parece obligado tener em cuenta la posibilidad de que su expansión obedezca, al menos em parte, ya a la aparición de

41 SÁNCHEZ, Jesús-Maria Silva. La expansión del derecho penal: aspectos de la política criminal en las sociedades postindustriales, Madrid, Civitas, 2001, 2ª ed., p. 20.
42 *Idem, ibidem,* p. 25-79.
43 NEVES, Marcelo. A constitucionalização simbólica. São Paulo, Editora WMF Martins Fontes, 2011, 3ª ed., p. 1.

> nuevos bienes jurídicos – de nuevos intereses o de nuevas valoraciones de intereses preexistentes –, ya al aumento de valor experimentado por algunos de los que existían con anterioridad, que podría legitimar su protección a través del Derecho penal. Las causas de la probable existencia de nuevos bienes jurídico-penales son, seguramente, distintas. Por um lado, cabe considerar que antes no existían – o no com la misma incidência –, y em cuyo contexto há de vivir la persona, que se ve influída por uma alteración de aquéllas. (...) Por otro lado, debe aludirse al deterioro de realidades tradicionalmente abundantes y que em nuestros días empiezan a manifestar-se como bienes escasos, atribuyéndoseles ahora um valor que anteriormente no se les asignaba, al menos de modo expresso; por ejemplo el medio ambiente. En tercer lugar, hay que contemplar el incremento essencial de valor que experimentan, como consecuencia del cambio sócia y cultural, ciertas realidades que siempre estuvieron ahí, sin que se reparara em las mismas; por ejemplo, el patrimônio histórico-artístico. Entre otros factores. (...) Lo que interessa poner de relieve (...) es tan sólo que seguramente existe um espacio de expansión razonable.[44]

[44] SÁNCHEZ, Jesús-Maria Silva. La expansión del derecho penal: aspectos de la política criminal en las sociedades postindustriales, Madrid, Civitas, 2001, 2ª ed., p. 25-26.

A propósito, entende Silva Sánchez que a criminalidade associada aos meios informáticos e à internet é seguramente o melhor exemplo de como o progresso técnico dá lugar, em âmbito da delinquência dolosa tradicional, à adoção de novas técnicas como instrumento que permita produzir resultados especialmente lesivos.[45]

2.4 TECNOLOGIA DA INFORMAÇÃO: BEM JURÍDICO-PENAL

Já há mais de 15 anos, Peter Csonka apontava a necessidade de proteção das redes de computação, citando pelo menos três motivos. O primeiro deles seria o fato de a internet ter transformado o mundo em uma sociedade de informação, na qual virtualmente inexistem fronteiras – tanto para boas coisas quanto para a criminalidade. O segundo deles diz respeito a serem suas implicações de longo alcance, uma vez que praticamente qualquer tipo de informação eletrônica está agora acessível a qualquer usuário da Internet em qualquer lugar do mundo e a qualquer momento. O terceiro relaciona-se à necessidade de proteção por serem as redes de computador uma promessa de uma nova era de comércio eletrônico, oferecendo serviços e bens, cujos valores logo poderiam superar os bilhões de dólares[46].

Em 2020, mais do que nunca, restou comprovado como as relações humanas vivem uma hiperconexão. Com a irrupção da pandemia de Covid-19, os governos de modo geral não tiveram escolha, senão determinar que as pessoas evitassem contato umas com as outras – distanciamento social – ou, mais gravemente, não saíssem de casa – *lockdown*. Em virtude disso, quase todos os aspectos da vida humana foram informatizados.

Nesse contexto, observou-se a intensificação do uso das mídias sociais: não podendo se encontrar fisicamente, as pessoas mantiveram suas

---

[45] *Idem, ibidem,* p. 28.

[46] M. CHERIF BASSIOUNI (Itália). Osservatorio Permanente Sulla Criminalità Organizzata (org.). Cybercrime: conferenza Internazionale, Milão, Dott. A. Giuffrè, 2004, p. 5.

relações interpessoais através de aplicativos, cada qual com o seu escopo – apesar de nenhum deter realmente uma exclusividade. As funcionalidades podem resumir-se em conversar (por texto ou por vídeo) e compartilhar conteúdos, principalmente fotos e vídeos – mas também notícias e ideias.

Partindo para panoramas menos restritivos, no sentido de abarcarem mais pessoas ao mesmo tempo, o ensino a distância (EAD) foi a solução encontrada para que a educação não fosse impossibilitada; a realização de *lives* foi o meio de que dispuseram os artistas para gerar entretenimento e renda; e o comércio eletrônico (*e-commerce*) teve um aumento de 145% no primeiro semestre de 2020[47].

De acordo com as estimativas do Fórum Econômico Mundial, há atualmente 4,5 bilhões de usuários de Internet. São gastos US$1.000.000,00 por minuto na Amazon. As plataformas Zoom e Microsoft Teams hospedam 208.333 e 52.083 pessoas por minuto, respectivamente, em um contexto de ambiente de trabalho remoto. US$240.000,00 são transferidos por minuto no Venmo (serviço de pagamento móvel). As expectativas são de aumentos nesses números: se não pelo advento da internet 5G, então pelo aumento no acesso à internet[48] – havendo quem fale em Internet Universal Básica[49].

Mas essa informatização das relações interpessoais (comerciais ou não) ainda não é o realmente assustador – está havendo, sem que a maioria das pessoas perceba, uma informatização da realidade objetiva e uma

---

[47] Vendas no e-commerce crescem 145% no 1º semestre e dobram faturamento de lojistas. 2020. Disponível em: https://www.ecommercebrasil.com.br/noticias/vendas-e-commerce-crescem-semestre/. Acesso em: 29 out. 2020.

[48] ALI, Aran. Here's what happens every minute on the internet in 2020. 2020. Disponível em: https://www.weforum.org/agenda/2020/09/internet-social-media-downloads-uploads-facebook-twitter-youtube-instagram-tiktok/. Acesso em: 14 out. 2020.

[49] FRAZIER, Kevin. COVID-19 Shows we need Universal Basic Internet now. 2020. Disponível em: https://www.weforum.org/agenda/2020/05/covid19-coronavirus-united-states-internet-acess-universal-basic/. Acesso em: 15 out. 2020.

subjetivação da realidade informática. Fala-se da Internet das Coisas (*Internet of Things* – IoT) e da inteligência artificial. Especial destaque merece aquela, por já ser alvo de ataques.

A Internet das Coisas consiste numa conexão dos itens que se utilizam no dia a dia, como carros, eletrodomésticos, roupas etc., à rede mundial de computadores. Mas não só isso. Também possibilita que Estados se utilizem de mecanismos para melhorar a infraestrutura das cidades, dando origem às chamadas *Smart Cities* ou cidades inteligentes. Citem-se alguns exemplos:

> Amsterdã, por exemplo, tem feito experiências com a oferta de unidades de armazenamento de energia doméstica e painéis solares para residências conectadas à rede inteligente da cidade. Essas baterias ajudam a diminuir o estresse na rede nos horários de pico, permitindo que os residentes armazenem energia fora dos horários de pico. Os painéis solares também permitem que os residentes vendam a energia sobressalente dos painéis de volta à rede. (...) Paris estreou um programa de compartilhamento de carros elétricos chamado Autolib em 2011 e, desde então, aumentou a frota de veículos para 3.000. Os veículos conectados podem ser rastreados via GPS e os motoristas podem usar o painel do carro para reservar vagas de estacionamento com antecedência. Londres anunciou no início deste ano que começaria os testes em um projeto de estacionamento inteligente que permitiria aos motoristas localizar vagas rapidamente e eliminar a necessidade de longas buscas por uma vaga aberta. Isso, por sua vez, aliviaria o congestionamento do tráfego

> urbano. A capital do Reino Unido também planeja testar programas de compartilhamento de carros elétricos e bicicletas. Enquanto isso, Copenhague começou a usar sensores para monitorar o tráfego de bicicletas da cidade em tempo real, o que fornece dados valiosos sobre como melhorar as rotas de bicicletas na cidade. Isso é crucial, pois mais de 40% dos moradores da cidade se deslocam diariamente de bicicleta. A América do Norte ficou para trás, embora seja a região mais urbanizada do mundo, com mais de 80% de sua população em centros urbanos. Ainda assim, existem muitos projetos de cidades inteligentes em funcionamento nesses países, especificamente no que diz respeito à segurança pública e ao trânsito. A cidade de Nova York testou a tecnologia de detecção de tiro em delegacias de polícia no Brooklyn e no Bronx, e o prefeito quer expandir esses testes pela cidade. Camden, New Jersey, implementou tecnologia semelhante.[50]

Assim, temos basicamente todas as atuações humanas que sempre tomaram lugar na realidade objetiva sendo realizadas na realidade virtual. O risco é cada vez maior.

---

[50] MEOLA, Andrew. **How smart city technology & the Internet of Things will change our apartments, grids and communities**. 2020. Disponível em: https://www.businessinsider.com/iot-smart-city-technology#:~:text=What%20is%20a%20smart%20city,utilities%20and%20services%2C%20and%20more.. Acesso em: 15 out. 2020.

Reuben Jackson fez, no contexto da pandemia, uma intensa análise do aumento da *cyber* criminalidade. Consoante o autor, viu-se esse tipo de criminalidade "tirar vantagem das mudanças apressadas para o trabalho remoto, atacar infraestruturas críticas sobrecarregadas, como indústrias de saúde, e visar alvos mais amplos nas organizações". A propósito, em investidas explorando a vulnerabilidade dos dispositivos *IoT*, casas inteligentes, empresas inteligentes e sistemas de controle conectados a infraestruturas críticas tiveram ataques aumentados em 46%[51]. Nesse sentido, o Ministro do Superior Tribunal de Justiça informou que, em decorrência do distanciamento social, o número de furtos e roubos decresceu significativamente, mas os crimes cibernéticos tomaram seu lugar.[52]

Some-se a isso o advento das criptomoedas (ou criptoativos). Segundo definição do Banco da Inglaterra, são um tipo de dinheiro eletrônico que usam um sistema *peer-to-peer*[53], não havendo banco central

---

[51] JACKSON, Reuben. How cybercrime has evolved since the pandemic hit: opportunistic agility is running rampant among hackers and scammers, 2020. Disponível em: https://bigthink.com/technology-innovation/cybercrime-evolved-during-pandemic?rebelltitem=1#rebelltitem1. Acesso em: 15 out. 2020.

[52] BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. Crime cibernético tomou lugar de roubos e furtos na pandemia, diz ministro Humberto Martins. 2020. Disponível em: http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Crime-cibernetico-tomou-lugar-de-roubos-e-furtos-na-pandemia--diz-o-ministro-Humberto-Martins.aspx. Acesso em: 23 nov. 2020.

[53] "Peer to peer (traduzível para "pessoa para pessoa") são sistemas computacionais que estão conectados a outros por meio da Internet. Arquivos podem ser compartilhados diretamente entre os sistemas em rede sem a necessidade de um servidor. Em outras palavras, cada computador em um sistema Peer to Peer se torna servidor de arquivo e cliente" *in* **P2P**. Disponível em: https://techterms.com/definition/p2p#:~:text=Stands%20for%20%22Peer%20to%20Peer,as%20well%20as%20a%20client.. Acesso em: 23 out. 2020.

ou governo para administrar o sistema ou intervir se algo der errado[54]. A propósito, uma das perspectivas a respeito das criptomoedas é exatamente de ser um modismo especulativo altamente vulnerável a *cyber* ataques.[55]

De acordo com pesquisa realizada pela *Norton Cyber Security Insight Reports* em 2017, o Brasil ficou em segundo lugar em termos de perdas financeiras provocadas por crimes cibernéticos, ficando atrás somente da China. Segundo se informa, naquele ano cerca de 62 milhões de brasileiros foram vítimas de crimes cibernéticos, totalizando um montante de 80 bilhões de reais em perdas.[56][57]

Portanto, não há como negar a importância que a tecnologia da informação (a informática, a segurança da informação ou o sistema informático[58]) tem na sociedade contemporânea. Não há tampouco como negar a necessidade de proteção dessa tecnologia pelo Direito Penal. Perfazem-se, então, os requisitos citados por Mir Puig para que um bem jurídico seja passível de tornar-se um bem jurídico-penal. Nesse sentido, importante é a lição de Paulo Ernani Bergamo dos Santos:

> A segurança da informação passa a bem jurídico-penal de natureza difusa, segundo o trinômio

---

[54]**What are cryptoassets (cryptocurrencies)?** Disponível em: https://www.bankofengland.co.uk/knowledgebank/what-are-cryptocurrencies. Acesso em: 15 out. 2020.

[55] DOW, Sheila. **What's the future of cryptocurrencies?** 2018. Disponível em: https://www.weforum.org/agenda/2018/08/cryptocurrencies-are-useful-but-will-not-save-us. Acesso em: 15 out. 2020.

[56] **REVISTA DE SEGUROS,** CNSeg, v. 93, n. 909, Rio de Janeiro, abril-junho, 2019. Disponível em: https://cnseg.org.br/publicacoes/revista-de-seguros-n-909.html. Acesso em: 29 out. 2020, p. 33.

[57]Para o relatório em sua totalidade: 2017 Norton Cyber Security Insights Report. 2017. Disponível em: https://www.nortonlifelock.com/us/en/newsroom/press-kits/ncsir-2017/#:~:text=Uncover%20the%20discrepancies%20behind%20consumers,21%2C000%20consumers%20in%2020%20countries.. Acesso em: 29 out. 2020.

[58] Não há uniformidade quanto ao nome do bem jurídico nem seu perfeito delineamento, mas giram em torno do processo de movimentação de informações através da tecnologia.

> "perda de confidencialidade (quebra de sigilo de senha) – perda de integridade (manipula-se uma informação de acesso restrito) – perda de disponibilidade (erro no sistema causado por intrusão de terceiros e causando impossibilidade de acesso à informação por quem precisa dela)" (ROSSINI, 2004, p. 31-53), gerando conflito entre os interesses dos usuários da internet atingidos pela conduta e os interesses de grandes empresas prestadoras de serviço na internet, como provedores de conteúdo e provedores de acesso[59].

Mas o que efetivamente seria tecnologia da informação?

Tecnologia da informação "refere-se ao componente tecnológico de um sistema de informação, ou seja, o conjunto de conhecimentos científicos aplicados ao processo de informação"[60]. Pode também ser conceituada como "a ciência e atividade de uso de computadores e softwares para armazenar e enviar informações".[61]

Pode-se observar que, atrelado à ideia de tecnologia da informação, está intrinsecamente ligado o conceito de dados, os quais são, basicamente, informações. A sociedade ocidental, atentando para a importância desses elementos, tem agido no sentido de atribuir-lhes maior proteção.

---

[59] BRASIL. MINISTÉRIO PÚBLICO FEDERAL. Crimes cibernéticos: coletânea de artigos, Brasília, MPF, 2018, 3ª ed., p. 163.

[60] SIQUEIRA, Fernando de. **Conceitos de Tecnologia de Informação**. Disponível em: https://sites.google.com/site/uniplisistemasdeinfogerenciais/aulas/1---conceitos-de-tecnologia-de-informacao. Acesso em: 20 out. 2020.

[61] Meaning of information technology in English. Disponível em: https://dictionary.cambridge.org/dictionary/english/information-technology. Acesso em: 28 out. 2020.

Em 25 de maio de 2018, passou a vigorar no âmbito da União Europeia a GDPR – *General Data Protection Regulation*[62] –, visando a proteger os dados dos usuários, que constantemente são captados pelas empresas. Assim, a lei estabelece regras de gerenciamento dessas informações.

No Brasil, entrou em vigor em agosto de 2020 a Lei Geral de Proteção de Dados – LGPD[63] –, dispondo sobre o tratamento de dados pessoais, com o objetivo de proteger a privacidade, a liberdade e o livre desenvolvimento da personalidade da pessoa natural. Essa lei é a responsável no ordenamento jurídico brasileiro por determinar o que vêm a ser dados:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a

---

[62] UNIÃO EUROPEIA. Regulamento nº 2016/679, de 27 de abril de 2016. **Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 april 2016**. Bruxelas, 27 abr. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 29 out. 2020

[63] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Lei Nº 13.709, de 14 de agosto de 2018.** Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 29 out. 2020.

> utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Os dados são não raras vezes o objeto material do crime – se é que assim se podem chamar, visto que não são uma realidade objetiva nem demandam um corpo para constituir-se. A propósito, podem ser replicados infinitamente.

3. CRIMES CIBERNÉTICOS

3.1 PROBLEMAS TERMINOLÓGICOS

Antes de uma conceituação mais aprofundada, cumpre-se analisar a terminologia utilizada. Conforme leciona Ângelo Roberto Ilha da Silva: "a terminologia apresenta uma variedade desafiadora, falando-se em crimes informáticos, crimes digitais, crimes virtuais, crimes cibernéticos, resultando numa ausência de concordância terminológica"[64]. Para o autor, crimes informáticos são gênero do qual os crimes cibernéticos são espécie. A diferença é que, apesar de ambos serem cometidos com a utilização de um computador, os crimes cibernéticos são perpetrados no âmbito ou por meio da Internet[65].

Fabrízio Rosa também aponta dificuldades terminológicas enfrentadas ao tratar dos crimes cibernéticos:

> Kohn utiliza *computer criminals* para designar seus praticantes. Jean Pradel e Cristian Feuliard referem-se a "infrações cometidas por meio de computador". Há ainda quem prefira a expressão "crimes de computador", "cybercrimes", "computer crimes", "delito informático", "crimes virtuais", "crimes eletrônicos" ou, ainda, "crimes

---

[64] SILVA, Ângelo Roberto Ilha da *et al.* Crimes cibernéticos: racismo, cyberbullying, deep web, pedofilia e pornografia infantojuvenil, infiltração de agentes por meio virtual, obtenção das provas digitais, nova lei antiterrorismo, outros temas, Porto Alegre, Livraria do Advogado, 2018, 2ª ed., p. 90.

[65] *Idem, ibidem.*

> digitais", "crimes cibernéticos", "infocrimes", "crimes perpetrados pela internet", denominações distintas, mas que, no fundo, acabam por significar basicamente a mesma coisa.[66]

Apesar de a Lei nº 12.737 de 2012[67] – marco legislativo importante na tipificação desse tipo específico de criminalidade no ordenamento jurídico brasileiro – utilizar o termo crimes informáticos, neste trabalho se utiliza o termo crime cibernético (ou *cybercrime)* na mesma acepção; não no sentido restrito empregado por Ilha da Silva.

Isso se dá pelos seguintes motivos: a) ser o termo utilizado na Convenção de Budapeste de 2001 ao tratar eminentemente de crimes cometidos com ou contra computadores (não se exigindo uso da internet); b) ser o termo usado na CPI dos crimes cibernéticos, que constitui importante fonte para o presente trabalho; c) diversas instituições assim denominarem essa espécie de criminalidade, como o Fórum Econômico Mundial, a SaferNet Brasil, o Ministério Público e diversas polícias brasileiras, ao instituírem delegacias especializadas; d) se assim não fosse, estar-se-ia excluindo deste trabalho o crime de interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública – que, apesar de não usar necessariamente a internet, é um dos *cybercrimes* potencialmente mais lesivos, tendo o condão de desestabilizar grandes infraestruturas.

---

66 ROSA, Fabrízio *apud* JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo, Saraiva, 2016, p. 50.

67 BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.. **Lei Nº 12.737, de 30 de novembro de 2012**. Brasília, DF, 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm#:~:text=Disp%C3%B5e%20sobre%20a%20tipifica%C3%A7%C3%A3o%20criminal,Art.. Acesso em: 29 out. 2020.

Utilizar a internet é, portanto, prescindível – ainda que bastante provável. Imprescindível é a utilização de alguma ferramenta informática – computador ou outra.

3.2 CONCEITUAÇÃO DE CRIMES CIBERNÉTICOS NO BRASIL

O Direito Penal é uma obra-prima (ainda que inacabada). Poucos ramos do Direito possuem seu objeto tão cientificamente delineado. Nesses outros ramos, a ausência de perfeita delineação não poucas vezes é a causa de excessos do poder público no manuseio da coisa pública; é a causa de excessos nas relações jurídicas privadas, em que uma parte acaba sobrelevando-se injustamente. Não se tenta dizer que o Direito Penal é imune a falhas; possui, todavia, uma sistematização reveladora de intenso trabalho acadêmico, podendo-se dizer invejável. Essa cientificidade foi concebida com o desenvolvimento da teoria do crime,[68] sendo esse o seu objeto primário[69].

O conceito formal de crime abrange três elementos: a tipicidade, a antijuridicidade (ou ilicitude) e a culpabilidade. Os dois primeiros dizem respeito ao fato criminoso, enquanto o terceiro relaciona-se ao autor desse fato. Apesar de sua divisão, é imprescindível ter-se em mente que o fenômeno delituoso existe abrangendo seus elementos conjuntamente, sendo essa divisibilidade destinada ao melhor entendimento da grande síntese em que, conforme lição de Luis Jiménez de Asúa, consiste a ação:

> Los que propugnamos semejante diferencia entre los elementos de lacto punible, jamás hemos negado que el fenómeno delito viva existência conjunta. Como el organismo fisiológico o patológico, es um todo que sólo puede

[68] BRANDÃO, Cláudio. "Bem jurídico e norma penal: a função da antinormatividade na teoria do crime". **DELICTAE: Revista de Estudos Interdisciplinares sobre o Delito**, v. 3, n. 4, Belo Horizonte, p. 07-45, jul. 2018.

[69] TAVARES, Juarez. Teorias do delito: variações e tendências, São Paulo, Revista dos Tribunais, 1980, P. 3.

> comprenderse si se estudia o se aprecia em su total armonía o em su complejo doliente. Pero el fisiólogo no sabrá como funcionan em conjunto huesos y músculos, vísceras y vasos, si no los estudió uno a uno en la disciplina que se llama anatomia. Estudiemos analíticamente el delito para comprender bien la gran síntesis en que consiste la acción u omisión que las leyes sancionan. Sólo así escaparemos, a la par, del confusionismo dogmático y de la tiranía política.[70]

Observe-se que essas três partículas do crime orbitam um elemento comum: a conduta humana. Com efeito, leciona Brandão que a conduta humana é a pedra angular da Teoria do Crime, sendo o suporte no qual se formularão todos os juízos que compõem o conceito de crime: "a tipicidade é a adequação da conduta com a norma; a antijuridicidade é o juízo de reprovação da conduta; e a culpabilidade é o juízo de reprovação sobre o autor da conduta"[71]. Em complemento, informa Juarez Tavares que "todas as concepções ou modelos de construção do delito podem reduzir-se, em última análise, a teorias sobre a ação"[72]. Exatamente na análise da conduta humana (em si e em suas circunstâncias) será possibilitada a definição de um crime como cibernético.

---

[70] ASÚA, Luis Jiménez de. Principios de derecho penal: la ley y el delito, Buenos Aires, Abeledo-Perrot, 1997, P. 204.
[71] BRANDÃO, Cláudio. Teoria jurídica do crime, São Paulo, Atlas, 2015, 4ª ed., P. 23.
[72] TAVARES, Juarez. Teorias do delito: variações e tendências, São Paulo, Revista dos Tribunais, 1980, p. 7.

Um crime cibernético é um fato típico, ilícito e culpável cometido por meio da tecnologia da informação ou contra esta[7374].

3.2.1 TIPOLOGIA DOS CRIMES CIBERNÉTICOS E BREVÍSSIMAS CONSIDERAÇÕES SOBRE SEU SUJEITO ATIVO

Tal qual acontece com os crimes militares, omissivos, funcionais etc., é possível distinguir os tipos de crimes cibernéticos. Assim, a depender do que efetivamente se pode lesionar, os crimes cibernéticos podem ser classificados em próprios (puros), impróprios (impuros) ou mistos, sendo essa a distinção mais importante[757677].

Os crimes cibernéticos próprios são aqueles em que o bem jurídico ofendido é a tecnologia da informação em si – ainda que outros também sejam ofendidos reflexamente; os impróprios são aqueles em que a tecnologia da informação é apenas o meio utilizado para a agressão a outros bens jurídicos – ainda que o bem jurídico tecnologia da informação também seja, mediatamente, lesionado. Os mistos, por sua vez, lesionam tanto a tecnologia da informação quanto outro bem jurídico-penal tutelado. A diferença reside no bem jurídico que efetivamente o criminoso

---

73 No mesmo sentido, mas desconsiderando a culpabilidade como seu elemento: JESUS, Damásio de; MILAGRE, José Antônio. Manual de crimes informáticos, São Paulo, Saraiva, 2016, p. 49.

74 "Celso Antonio Pacheco Fiorillo e Christiany Pegorari Conte definem os crimes informáticos como "os ilícitos perpetrados por intermédio da Internet ou com o auxílio desta, causando algum tipo de dano à vítima" *in* SOARES, Daniel Menah Cury. **Crimes informáticos:** uma breve resenha e apontamento de complicações. 2019. Disponível em: https://migalhas.uol.com.br/depeso/308978/crimes-informaticos--uma-breve-resenha-e-apontamento-de-complicacoes. Acesso em: 19 out. 2020.

75 Há quem fale em crimes "informáticos" mediatos, mas não parece de grande relevância a distinção.

76 Apesar de falar em crimes informáticos, pelos motivos já expostos, pode-se aplicar a tipologia ao termo crimes cibernéticos. JESUS, Damásio de; MILAGRE, José Antônio. Manual de crimes informáticos, São Paulo, Saraiva, 2016, p. 52-53.

77 CRESPO, Marcelo *apud* BRASIL. MINISTÉRIO PðBLICO FEDERAL. Crimes cibernéticos: coletânea de artigos, Brasília, MPF, 2018, 3ª ed., p. 16.

tem por finalidade lesionar – um critério teleológico, portanto. Nesse mesmo sentido, brilhante é a definição das espécies de crimes cibernéticos presente no Relatório Final da CPI dos Crimes Cibernéticos, de que brevemente se tratará linhas abaixo. Apesar de utilizar terminologia diversa, sua conceituação é perfeita.

> a) Os crimes virtuais puros englobam toda e qualquer conduta ilícita cujo objetivo seja a violação da integridade física ou lógica do sistema computacional, isto é, tem como finalidade atacar o software (programa), hardware (componente físico do computador, tais como: CPU, monitor, teclado, circuito), dados, sistemas e meios de armazenamentos, etc;
>
> b) Os crimes virtuais mistos são as condutas em que a utilização de meios computacionais é condição necessária para a efetivação da conduta, embora o bem jurídico lesado seja diverso do informático, tais como a transferência ilícita de valores em uma "homebanking" ou a prática de "salemislacing" (retirada diárias de pequenas quantias em milhares de contas, também conhecida como retirada de saldo).
>
> c) Os crimes virtuais comuns são aqueles em que os dispositivos computacionais são utilizados apenas como instrumento para a realização de um delito já tipificado pela lei penal, constituindo-se em apenas mais um meio de execução desses delitos, tal como ocorre nos seguintes crimes, já tipificados pela lei penal: o estelionato (art. 171 do CP), a ameaça (art. 147 do CP - Código Penal), os crimes contra a honra (arts. 138 a 140 do CP), a veiculação de pornográfica infantil (art. 241-A do

> Estatuto da Criança e do Adolescente – Lei nº 8.069/90), o crime de violação ao direito autoral (art. 184 do CP), entre outros[78].

Assim, os crimes virtuais puros correspondem aos crimes cibernéticos puros ou próprios; os crimes virtuais mistos correspondem aos crimes cibernéticos mistos; e os crimes virtuais comuns correspondem aos crimes cibernéticos impuros ou impróprios.

Quanto ao sujeito ativo dos crimes cibernéticos, é comumente utilizada a expressão *hacker*, o que revela uma ausência de tecnicidade, sendo preferível a palavra *cracker*. Nesse sentido:

> Um *hacker* é uma pessoa intensamente interessada no funcionamento misterioso e recôndito de qualquer sistema operacional de computador. *Hackers* geralmente são programadores. Portanto, obtêm conhecimento avançado em sistemas operacionais e linguagens de programação. Eles podem descobrir falhas em sistemas e as razões para essas falhas. *Hackers* constantemente buscam mais conhecimento, gratuitamente compartilham suas descobertas e nunca lesionam dados intencionalmente. Um *cracker* é aquele que quebra ou de outra maneira viola a integridade do sistema de máquinas remotas com intenção maliciosa.

---

[78] CÂMARA DOS DEPUTADOS (Brasil). Congresso Nacional. **CPI - Crimes cibernéticos**: comissão parlamentar de inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país.. Brasília: __, 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D%3E+RCP+10/2015. Acesso em: 29 out. 2020.

> Após conseguirem o acesso não autorizadamente, os crackers destroem dados vitais, negam serviços legítimos aos usuários ou causam problemas para seus alvos. Crackers podem ser facilmente identificados pela malícia de suas ações[79][80].

Ainda cumpre destacar, como fez a já citada CPI, as figuras dos desenvolvedores e dos operadores:

> Desenvolvedores são criminosos que se dedicam propriamente à construção das ferramentas computacionais utilizadas para a prática de ilícitos no ciberespaço. Em geral esses criminosos vendem ou alugam suas ferramentas para o grupo dos operadores utilizando a própria internet, por vezes se valendo até mesmo de mídias sociais como o Facebook para divulgar seus "serviços" e "produtos". Já os operadores são aqueles que utilizam as ferramentas computacionais para o efetivo cometimento dos crimes cibernéticos. Neste ponto, cumpre mencionar que, tipicamente, uma investigação policial bem-sucedida redunda no desbaratamento de um grupo de operadores de

---

[79]Hackers and crackers. 2002. Disponível em: https://www.informit.com/articles/article.aspx?p=30048#:~:text=They%20might%20discover%20holes%20within,remote%20machines%20with%20malicious%20intent.. Acesso em: 22 out. 2020.

[80] A propósito, a carreira de hacker tem se mostrado potencialmente uma das mais lucrativas do mundo, segundo matéria da Forbes: WINDER, Davey. **These Hackers Have Made $100 Million And Could Earn $1 Billion By 2025**. 2020. Disponível em: https://www.forbes.com/sites/daveywinder/2020/05/29/these-incredible-100-million-hackers-could-make-1-billion-by-2025-hackerone-bounty-millionaires/?sh=7b02fedd77b8. Acesso em: 29 out. 2020.

> crimes cibernéticos, sendo muito raro que se consiga chegar aos desenvolvedores das ferramentas.[81]

Pelo fato de haver especificidade legislativa, interessam ao presente trabalho – ao menos no presente momento – os crimes cibernéticos próprios ou mistos, até porque os impróprios podem servir de meio para a prática de uma infinidade de crimes, desde estelionato e furto até terrorismo.

3.2.2 CRIMES CIBERNÉTICOS PRÓPRIOS EM ESPÉCIE NO ORDENAMENTO JURÍDICO BRASILEIRO E LEIS CORRELATAS

Dentre as primeiras tentativas de legislar sobre crimes cibernéticos no Brasil, destaque-se o Projeto de Lei n. 84/99, o qual buscava alterar dispositivos do Código Penal[82] e do Código Penal Militar[83] em virtude de atentar-se para os riscos inerentes a um mundo cada vez mais conectado. Dessa forma, a lei traria em seu bojo diversas definições importantes (como a de dispositivos de comunicação; redes de computadores; e sistema informatizado), bem como tipificaria diversas

---

[81] CÂMARA DOS DEPUTADOS (Brasil). Congresso Nacional. **CPI - Crimes cibernéticos**: comissão parlamentar de inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país.. Brasília: __, 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D%3E+RCP+10/2015. Acesso em: 29 out. 2020.

[82] BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. **Decreto-Lei Nº 2.848, de 7 de dezembro de 1940**. Rio de Janeiro, RJ, 7 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 29 out. 2020.

[83] BRASIL. Decreto-Lei nº 1.001, de 21 de outubro de 1969. Código Penal Militar. **Decreto-Lei Nº 1.001, de 21 de outubro de 1969**. Brasília, DF, 21 out. 1969. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del1001.htm. Acesso em: 29 out. 2020.

condutas, que constituiriam crimes cibernéticos próprios. Como exemplos, podemos citar "acesso não autorizado à rede de computadores, dispositivo de comunicação ou sistema informatizado"; "obtenção, transferência ou fornecimento não autorizado de dado ou informação"; "divulgação ou utilização indevida de informações e dados pessoais"; "dano informático"; "inserção ou difusão de código malicioso" etc.

Após 12 anos em tramitação, o Projeto de Lei foi completamente modificado, de modo que sua única contribuição – como Lei 12.735/12[84], afinal – foi estabelecer a possibilidade de cessação de publicações e transmissões eletrônicas que veiculassem alguma forma de racismo, nos termos do art. 20 da Lei 7.716/89[85], sendo suas tentativas de criminalização de condutas perigosas vetadas.

Hoje, a Lei 12.737/2012 é o mais importante corpo legislativo a tratar de crimes cibernéticos no Brasil. A lei é conhecida como "Lei Carolina Dieckmann", em virtude de seu projeto ter sido sobremaneira acelerado, com a apresentação de diversos requerimentos de urgência, após um suposto vazamento de fotos íntimas da mencionada atriz na internet.

Tipifica essa lei os crimes de "invasão de dispositivo informático"; "interrupção ou perturbação de serviço telegráfico,

---

84 BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. **Lei Nº 12.735, de 30 de novembro de 2012**. Brasília, DF, 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 29 out. 2020.

85 BRASIL. Lei nº 7.716, de 5 de janeiro de 1989. Define os crimes resultantes de preconceito de raça ou de cor.. **Lei Nº 7.716, de 5 de Janeiro de 1989.**. Brasília, DF, 5 jan. 1989. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 29 out. 2020.

telefônico, informático, telemático ou de informação de utilidade pública" – modificando crime já existente –, bem como equipara cartões de crédito ou débito a documentos particulares – o que não se relaciona com crimes cibernéticos necessariamente.

Com relação ao crime de "invasão de dispositivo informático", assim dispõe o Código Penal, com o acréscimo realizado pela Lei 12.737/12:

> 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 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.
> **Ação penal**
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Observa-se, portanto, que, a despeito de haver apenas um *nomen juris*, há a criminalização de mais de uma conduta: a) a do sujeito que invade dispositivo informático, conectado ou não à internet, mediante violação indevida de mecanismo de segurança, com o especial 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; e b) a do sujeito que produz, oferece, distribui,

vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática anteriormente citada.

É importante ressaltar que o *caput* do art. 154-A prevê um elemento subjetivo do injusto[86]. Trata-se do fim específico de "obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita". Daí ser possível concluir o seguinte: caso um sujeito invada dispositivo informática violando seu dispositivo de segurança apenas por curiosidade ou diversão – ou, ainda, para provar que é capaz –, não há crime.

Como exemplo da prática desse crime, pode-se citar a possível atividade de suposta organização criminosa que teve acesso ilegal a dados de autoridades brasileiras, tendo sido alvo da operação *Spoofing,* da Polícia Federal[87], que deu origem a denúncia pelo Ministério Público Federal[88].

Já a respeito do crime de "interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública", pode-se afirmar que a novidade trazida pela Lei 12.737/12 foi inserir dois parágrafos no art. 266 do Código Penal, adicionando "serviço telemático ou de informação de utilidade pública"

---

86 Ou seja, um requisito de caráter subjetivo distinto do dolo que o tipo exige, além deste, para sua realização. MEZGER, Edmund *apud* PRADO, Luiz Regis. Curso de direito penal brasileiro: parte geral e parte especial, São Paulo, Editora Revista dos Tribunais, 2015, 14ª ed., P. 304.

87 O que se sabe sobre a Operação Spoofing e o hacker que interceptou mensagens de autoridades. 2019. Disponível em: https://g1.globo.com/politica/noticia/2019/07/24/o-que-se-sabe-sobre-a-operacao-spoofing-e-os-suspeitos-de-interceptar-mensagens-de-autoridades.ghtml. Acesso em: 29 out. 2020.

88 Operação Spoofing: MPF denuncia sete por crimes envolvendo invasões de celulares de autoridades brasileiras. 2020. Disponível em: http://www.mpf.mp.br/df/sala-de-imprensa/noticias-df/operacao-spoofing-mpf-denuncia-sete-por-crimes-envolvendo-invasoes-de-celulares-de-autoridades-brasileiras. Acesso em: 29 out. 2020.

como parte integrante do tipo; e uma causa de aumento de pena (se o crime é cometido por ocasião de calamidade pública).

Além desses dois tipos penais, pode-se acrescentar o crime previsto no art. 10 da Lei 9.296/96, alterado pela Lei 13.964/19, o qual dispõe o seguinte:

> Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei:
> Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> Parágrafo único. Incorre na mesma pena a autoridade judicial que determina a execução de conduta prevista no caput deste artigo com objetivo não autorizado em lei.

Assim, constitui crime cibernético próprio a parte do tipo penal que criminaliza a conduta de realizar interceptação de informática ou telemática sem autorização judicial ou com objetivos não autorizados em lei. Assim como os crimes anteriormente citados, essa parte específica do *caput* do art. 10 ofende especificamente o bem jurídico sigilo das comunicações, o qual é essencialmente vinculado à Tecnologia da Informação.

Por fim, citem-se os artigos. 313-A e 313-B do Código Penal, *in verbis:*

> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter

> vantagem indevida para si ou para outrem ou para causar dano
> Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.
> Modificação ou alteração não autorizada de sistema de informações
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:
> Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.
> Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.

Pode-se observar, portanto, que, além de se tutelar a Administração Pública, tutelam-se os dados (no art. 313-A) e o sistema de informações ou programa de informática (no art. 313-B)[89].

Apesar de não tratar especificamente dos aspectos penais relacionados à Internet, é de extrema valia a Lei 12.965/14[90] (Marco Civil da Internet). Essa lei estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, sendo responsável por dispor sobre

---

[89] CUNHA, Rogério Sanches. **Manual de direito penal**: parte especial, Salvador, Juspodivm, 2017, 9ª ed., p. 786-788.

[90] BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.. **Lei Nº 12.965, de 23 de abril de 2014**. Brasília, DF, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 29 out. 2020.

elementos que de certa maneira acabam se relacionando com os crimes cibernéticos (como o registro de dados, o protocolo de internet, disposições acerca de requisições investigativas e alguns deveres estabelecidos a empresas que são imprescindíveis à descoberta da autoria desses crimes).

3.2.3 PROBLEMAS ESPECÍFICOS ENVOLVENDO A CYBERCRIMINALIDADE: TÉCNICAS E CONDUTAS CRIMINOSAS, LUGAR DO CRIME E AUTORIA.

Três dificuldades específicas no tocante aos *cybecrimes* devem ser analisadas. A primeira delas diz respeito à complexidade e mutabilidade das técnicas informáticas que podem constituir fato típico, tendo sido um problema a prejudicar a proteção legislativa. A segunda diz respeito ao local do crime, especialmente relevante num contexto em que as condutas se praticam muitas vezes em ambientes objetivamente muito distantes em relação ao resultado delituoso gerado. A terceira diz respeito à dificuldade de saber quem efetivamente se utilizou de determinado instrumento de processamento de dados para cometer um crime. A primeira delas resume-se aos crimes cibernéticos próprios; as outras relacionam-se tanto aos próprios quanto aos impróprios.

Damásio de Jesus e José Antônio Milagre afirmam que a mora brasileira ao tratar de crimes cibernéticos podia ser atribuída, entre outras coisas, ao modo como tentávamos legislar. Aqui, tentamos criminalizar técnicas informáticas (em vez de condutas praticadas através dessas técnicas), mas, por serem estas mutantes, seriam inócuas supostas criminalizações primárias realizadas dessa maneira. [91][92]

---

[91] JESUS, Damásio de; MILAGRE, José Antônio. Manual de crimes informáticos, São Paulo, Saraiva, 2016, p. 29.

[92] "La falta de medidas y diferentes jurisdicciones crean vacíos legales y es que, en muchas ocasiones, la tecnología va por delante de la legislación y se busca la protección una vez ocurrido el incidente". CARO, Lucía. **Principales delitos cibernéticos del siglo XXI en España**. 2018. Disponível em: https://www.legaltoday.com/practica-

Segundo os autores, técnica, no âmbito dos crimes cibernéticos, seria o método, o procedimento, o software ou o processo informático que poderia caracterizar um comportamento humano[93]. Essa técnica pode ser executada manualmente ou por meio de subtécnicas. Citam os principais "artefatos, técnicas ou métodos informáticos" associados a uma ou mais condutas relevantes para o Direito Penal: Vírus, *Trojan*, *Sniffing, Backdoor, Spyware, Keylogging* e *Screenlogging*, *Defacement, Rootkits, DoS* e *DDoS, DNS Poisoning, Brute Force* etc.

Por se tratar de conceitos altamente técnicos, não é interessante a abordagem dessas técnicas no presente trabalho. Todavia, importa ressaltar o seguinte: por serem muitas, muito complexas e altamente mutáveis, as técnicas não devem ser o objeto das leis penais, sob pena de revestirem-se de obsolescência e possível inutilidade. O melhor método de proteger bens jurídicos através da criminalização de crimes cibernéticos é dispor sobre as condutas potencialmente lesivas nesse contexto[94] – o que será analisado linhas abaixo, ao abordar-se a Convenção de Budapeste.

O lugar do crime é outra questão que merece ser analisada quando se tratando de criminalidade cibernética.

Os limites geográficos já não são um aspecto a dificultar as práticas criminosas. Uma pessoa se utilizando de um computador em Kiev, conectada a um servidor além-mar, pode subtrair informações sigilosas que se encontram em bases de dados norte-americanas. Foi o caso do ucraniano Vadym Iermolovych, o qual invadia sistemas de

---

juridica/derecho-penal/penal/principales-delitos-ciberneticos-del-siglo-xxi-en-espana-2018-12-28/. Acesso em: 29 out. 2020.

93 *Idem, ibidem.*

94 JESUS, Damásio de; MILAGRE, José Antônio. Manual de crimes informáticos, São Paulo, Saraiva, 2016, p. 29.

veículos de mídia norte-americanos e subtraía notícias que ainda iriam ao ar, fazendo operações financeiras ilegais[95] – *insider trading*.

A respeito da territorialidade no contexto de inovações digitais, leciona Patrícia Peck Pinheiro:

> No mundo tradicional, a questão da demarcação do território sempre foi definida por dois aspetos: os recursos físicos que esse território contém e o raio de abrangência de determinada cultura. A sociedade digital rompe essas duas barreiras: o mundo virtual constrói um novo território, dificilmente demarcável, no qual a própria riqueza assume um caráter diferente, baseada na informação, que, como vimos, é inesgotável e que pode ser duplicada infinitamente. (...) Para a sociedade digital, não é mais um acidente geográfico, como um rio, montanha ou baía, que determina a atuação do Estado sobre seus Indivíduos e a responsabilidade pelas consequências dos atos destes. A convergência, seja por Internet, seja por outro meio, elimina a barreira geográfica e cria um ambiente de relacionamento virtual paralelo no qual todos estão sujeitos aos mesmos efeitos, ações e reações.[96]

Entretanto, esse aspecto não se reveste de grande dificuldade para o Direito brasileiro.

---

[95]Ukranian who pleaded guilty in hacking scheme gets 30 months in prison. Disponível em: https://www.washingtonpost.com/business/economy/ukranian-who-pleaded-guilty-in-hacking-scheme-gets-30-months-in-prison/2017/05/22/8749ea1e-3efe-11e7-8c25-44d09ff5a4a8_story.html. Acesso em: 26 out. 2020.

[96] PINHEIRO, Patrícia Peck. Direito digital, São Paulo, Saraiva, 2016, 6ª ed., p. 84-86.

Segundo o Código Penal brasileiro, aplica-se a lei brasileira ao crime cometido no território nacional, sem prejuízo de convenções, tratados e regras de direito internacional (art. 5º do Código Penal). Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado (art. 6º). Adotou o Brasil, portanto, a teoria da ubiquidade[97].

Assim, no Brasil, a partir de uma leitura dos artigos acima citados, não importa qual foi o caminho percorrido pelo criminoso cibernético: aplicar-se-ão as disposições penais brasileiras quando aqui for realizada a conduta ou aqui se produzir ou dever produzir-se o resultado. Nesse sentido:

> Para a aplicação da Lei Penal, o Estado brasileiro titular do jus puniendi adotou, como regra, o princípio da territorialidade, conforme já citado art. 5º do Código Penal, sem prejuízo da incidência de outros princípios nos casos dispostos no art. 7º, inciso II, do mesmo diploma legal. E, para a definição do lugar do delito, optou o legislador penal pela adoção do Princípio da Ubiquidade (art. 6º do CP), estabelecendo que se considera praticado o crime "no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde produziu ou devera produzir-se o resultado". Da análise dos artigos acima mencionados, infere-se que, na prática de crimes por meio da internet, ocorrida no território nacional, torna-se completamente irrelevante para

97 BITTENCOURT, Cézar Roberto. Tratado de direito penal: parte geral, São Paulo, Saraiva, 2016, 22ª ed., P. 226.

> a aplicação da lei penal o local em que fica a sede da empresa provedora do serviço de internet ou onde estão armazenadas as informações telemáticas. Portanto, se um crime cibernético ocorreu no Brasil, estará sujeito à jurisdição brasileira, sendo dever do Estado investigar e reprimir as condutas delituosas praticadas e fazer cumprir as decisões emanadas de juiz brasileiro para a efetiva apuração do delito, sem a necessidade de cooperação internacional para o cumprimento da decisão.[98]

Ainda que não se considere ser o Brasil o local do crime, é possível aplicar a lei brasileira a partir da conjugação dos parágrafos 3º e 2º do art. 7º do Código Penal brasileiro, aplicando-se o princípio da nacionalidade passiva, em situação de extraterritorialidade condicionada[99]. É possível isso ocorrer quando o crime for cometido por estrangeiro contra brasileiro fora do Brasil e I) não for pedida ou for negada a extradição ou II) houver requisição do Ministro da Justiça, com as seguintes condições: a) entrar o agente no território nacional; b) ser o fato punível também no país em que foi praticado; c) estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição; d) não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena; e) não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável.

A respeito da dificuldade de descobrimento da autoria da conduta cybercriminosa, valiosíssimo é o trabalho de Guilherme

---

98 98 BRASIL. MINISTÉRIO PÚBLICO FEDERAL. Crimes cibernéticos: coletânea de artigos, Brasília, MPF, 2018, 3ª ed., p. 36.

99 BITTENCOURT, Cézar Roberto. Tratado de direito penal: parte geral, São Paulo, Saraiva, 2016, 22ª ed., P. 228.

Schmitt[100]. Segundo este, quando alguém quer cometer um crime cibernético, muito raramente se utiliza de sua real identificação pessoal – muitas vezes faz passar-se por outra pessoa.

Assim, quando se busca identificar um sujeito no contexto da Internet, deve-se partir do endereço da máquina: "nas redes de computadores, não é possível identificar o usuário visualmente ou através de documentos, mas é possível identificar o endereço da máquina que envia as informações à rede. Ou seja, o IP da máquina[101]. Este é uma identificação única para cada computador ligado à rede[102]. Nos termos da Lei 12.965/14, endereço de protocolo de internet (endereço IP) é o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais (art. 5º, III).

Esse número, que é fornecido pelo provedor de internet, pode ser estático (manter-se o mesmo) ou dinâmico (alterando-se a cada nova conexão) – o que sói ocorrer na maioria dos casos. Nesse sentido, ressalta o Manual Prático de Investigação de Crimes Cibernéticos da Procuradoria da República no Estado de São Paulo a importância da identificação da hora exata da conexão e o fuso horário do sistema:

> A identificação do IP é o primeiro e mais importante passo para a investigação de um crime cibernético, como veremos adiante. Convém, desde logo, lembrar que o investigador deve ainda identificar a hora exata da conexão e o fuso

---

100 SCHMITT, Guilherme. Crimes cibernéticos. 2014. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos#:~:text=Da%20Autoria,indevido%20de%20suas%20senhas%20pessoais.. Acesso em: 26 out. 2020.

101 *Idem, ibidem.*

102 BRITO, Edivaldo. O que é o IP?: descubra para que serve e qual é seu número. Descubra para que serve e qual é seu número. 2013. Disponível em: https://www.techtudo.com.br/artigos/noticia/2013/05/o-que-e-o-ip-descubra-para-o-que-serve-e-qual-e-seu-numero.html. Acesso em: 27 out. 2020.

> horário do sistema, pois um número IP pertence ao usuário apenas durante o período em que ele está conectado; depois, o número é atribuído a outro internauta, aleatoriamente[103].

No Brasil, o Marco Civil da Internet (Lei 12.965/14) estabelece importantíssimas disposições a respeito do tema, principalmente a respeito do dever, por parte dos provedores de Internet, de manter os registros de acesso à Internet (*logs*) por determinado prazo. Inicialmente, cumpre distinguir os tipos de registros: eles podem ser de conexão ou de acesso a aplicações de internet. O primeiro é "o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados" (art. 5º, VI). O segundo é "o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP" (art. 5º, VIII). Como se vê, a diferenciação legal aparentemente não cumpre bem sua função de distinguir os conceitos. Não obstante, isso será importante para distinguir os tipos de provedores e, consequentemente, o prazo durante o qual devem eles manter esses registros.

A despeito de a lei não deixar claro qual seria a distinção dos dois tipos de provedores, em texto brilhante, Frederico Meinber Ceroy, após minuciosa análise, explicita suas diferenças:

> Provedor de Acesso ou Provedor de Conexão é a pessoa jurídica fornecedora de serviços que consistem em possibilitar o acesso de seus consumidores à internet. Para sua caracterização, basta que ele possibilite a conexão dos terminais4

---

[103] BRASIL. Procuradoria da República no Estado de São Paulo. Ministério Público Federal. **Crimes cibernéticos**: manual prático de investigação. São Paulo: _____, 2006, p. 8

> de seus clientes à internet. Em nosso país os mais conhecidos são: Net Virtua, Brasil Telecom, GVT e operadoras de telefonia celular como TIM, Claro e Vivo, estas últimas que fornecem o serviço 3G e 4G. Quanto a este provedor, é importante frisar que o marco civil da internet operou certa alteração no mencionado conceito ao afirmar que, na provisão de conexão à internet, cabe ao administrador de sistema autônomo o respectivo dever de manter os registros de conexão. Tendo, ainda, definido como administrador de sistema autônomo a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento devidamente cadastrado no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao país.
> (...)Provedor de Aplicação de Internet (PAI) é um termo que descreve qualquer empresa, organização ou pessoa natural que, de forma profissional ou amadora, forneça um conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet, não importando se os objetivos são econômicos[104].

De acordo com o autor, a partir do conceito de Provedor de Aplicação de Internet, podem-se inferir certas situações. A primeira delas

[104] CEROY, Frederico Meinberg. Os conceitos de provedores no Marco Civil da Internet. 2014. Disponível em: https://migalhas.uol.com.br/depeso/211753/os-conceitos-de-provedores-no-marco-civil-da-internet. Acesso em: 28 out. 2020.

diz respeito à possibilidade de uma pessoa natural figurar como provedor de aplicação de internet, citando o caso de alguém que mantém um blog contendo um fórum de discussão entre usuários. Outra relaciona-se à impossibilidade de determinados administradores de sites ou aplicativos argumentarem que não são PAI por não auferirem lucros com a manutenção do site. Em ambos os casos, devem-se guardar os *logs* pelo prazo legalmente imposto.

Tendo a distinção em mente, observem-se os prazos previstos legalmente: um ano para os provedores de conexão à internet e seis meses para os provedores de aplicações de internet (arts. 13 e 15 da Lei 12.965/14).

Infelizmente, por esvaziar o sentido da norma, o Decreto nº 8.771/16[105], responsável por regulamentar o Marco Civil da Internet, dispõe, no seu art. 11, § 1º, que o provedor que não coletar dados cadastrais deverá informar tal fato à autoridade solicitante, ficando desobrigado de fornecer tais dados. Isso certamente dificulta sobremaneira o trabalho de investigação de autoria. Nesse sentido:

> Para piorar ainda mais esse exíguo prazo de armazenamento definido, o Decreto nº 8.771, de 11 de maio de 2016, que regulamentou a Lei nº 12.965/2014, definiu em seu art. 11 que "o provedor que não coletar dados cadastrais deverá informar tal fato à autoridade solicitante, ficando

[105] BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. **Decreto Nº 8.771, de 11 de Maio de 2016**. Brasília, DF, 11 maio 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm. Acesso em: 29 out. 2020.

> desobrigado de fornecer tais dados". Isso é praticamente um convite aos criminosos para utilizarem redes WiFi abertas para o cometimento de delitos[106].

Assim, para chegar-se à autoria de um *cybercrime*, devem os investigadores (polícias ou Ministério Público) partir do IP (o que se encontra através de perícia) e, posteriormente, requerer ao Poder Judiciário[107] o fornecimento, pelas empresas provedoras, de informações relacionadas à identificação do usuário de determinado IP em determinado momento, nos termos dos arts. 10[108], e 22[109] da Lei 12.965/14. Posteriormente, podem requerer a quebra de sigilo dos dados telefônicos:

106BRASIL. MINISTÉRIO PÚBLICO FEDERAL. Crimes cibernéticos: coletânea de artigos, Brasília, MPF, 2018, 3ª ed., p. 13.

107 Sobre o tema, interessante o seguinte artigo: OLIVEIRA, Eduardo Cunha. **AS SOLICITAÇÕES DOS REGISTROS DE CONEXÃO (IP) SEM AUTORIZAÇÃO JUDICIAL**. 2019. Disponível em: http://silvavitor.com.br/as-solicitacoes-dos-registros-de-conexao-ip-sem-autorizacao-judicial/. Acesso em: 28 out. 2020.

108 Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º . § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º . § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição. § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

> Como, então, saber a qual instituição pedir as informações? É simples: basta repetir as pesquisas mencionadas no item 4.1.5. Por exemplo: a qual empresa pertence o IP 200.153.238.195? Os números IP iniciados com "2002" pertencem, geralmente, a concessionárias brasileiras. Digitando o número 200.153.238.195 no site www.registro.br (no campo "procure um nome de domínio" descobrimos que o usuário conectou-se à Internet por meio de uma linha fornecida pela Telecomunicações de São Paulo S.A. -- TELESP. O próprio site já fornece o nome do responsável e o endereço para onde o ofício judicial deverá ser encaminhado. Localizado o provedor de acesso, que pode ser um provedor de Internet, uma organização particular ou uma companhia telefônica, a autoridade policial ou o Ministério Público deverá requerer ao juiz (ver modelo no anexo III) novo pedido de quebra do sigilo de dados telemáticos, desta vez para que o provedor de acesso informe as informações do usuário vinculado ao IP, em uma determinada data e horário. A concessionária deverá responder à

---

[109] Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet. Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade: I - fundados indícios da ocorrência do ilícito; II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e III - período ao qual se referem os registros.

> ordem judicial fornecendo as informações necessárias para a identificação do indivíduo usuário do IP no momento solicitado, inclusive o endereço físico.[110]

A situação reveste-se de ainda maior complexidade quando o computador (ou o que o valha) utilizado não seja de uso privado, mas de uso comum (como um computador de *lan house* ou de *cybercafés*). Nesses casos, quando se chegar até o computador, devem-se utilizar práticas outras para tentar descobrir quem o estava usando no momento do crime – através de informações provenientes de câmeras de segurança ou de registro de uso, por exemplo. Uma possível solução para tanto seria a criação de leis no sentido de obrigar tais espaços a manter cadastro dos seus usuários, o que facilitaria sobremaneira a investigação para descoberta da autoria delitiva – como foi o caso do Projeto de Lei 7100/2017, apresentado à Câmara dos Deputados, que foi arquivado[111].

3. 3 HÁ DEFICIÊNCIA DA LEGISLAÇÃO PENAL BRASILEIRA FRENTE AOS CYBERCRIMES? UMA ANÁLISE À LUZ DA CONVENÇÃO DE BUDAPESTE E DA CPI DOS CRIMES CIBERNÉTICOS

Diante da escassa quantidade de disposições legais acerca de crimes cibernéticos, exsurge-se a questão: há deficiência da legislação penal brasileira frente a esses crimes? Em outras palavras: estamos preparados para lidar penalmente com a quantidade absurdamente grande de novas possibilidades delitivas em âmbito cibernético? Para tentar responder a

---

110 110 BRASIL. Procuradoria da República no Estado de São Paulo. Ministério Público Federal. **Crimes cibernéticos**: manual prático de investigação, São Paulo, _____, 2006, p. 27.

111PL 7100/2017. 2017. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2125353. Acesso em: 28 out. 2020.

essa pergunta, utilizar-se-ão como parâmetro a Convenção de Budapeste[112] e a CPI dos crimes cibernéticos, de 2016. Ressalve-se que, até o fim deste trabalho, o Brasil ainda não tinha aderido à Convenção.

No âmbito internacional, o mais importante corpo legislativo a tratar de *cybercrimes* é a Convenção do Conselho da Europa contra a Criminalidade Cibernética, aberta a assinaturas em 23 de novembro de 2001, na cidade de Budapeste, capital da Hungria. A referida convenção traz cinco títulos relacionados a Direito Penal, cinco títulos relacionados a Direito Processual, bem como outros tópicos envolvendo cooperação internacional, resolução de conflitos, consulta entre as partes etc.[113] Procura a Convenção harmonizar as legislações penal e processual penal dos países aderentes.

Segundo Peter Csonka,

> a Convenção é uma resposta coletiva por membros do Conselho da Europa (45 Estados) e alguns Estados não membros ao desafio do *cybercrimes*. É o resultado de 4 anos de trabalho intenso por um comitê de expertos montado em 1997 – o Comitê de Expertos em Crime no Cyberespaço (Comitê "PC-CY"), o qual foi confiado pelo Comitê de Ministros para dar seguimento às recomendações anteriores – documentos de política em caráter vinculante – a respeito de crimes de computadores e problemas processuais penais ligados à tecnologia da

---

112 CONSELHO DA EUROPA. Tratado nº 185, de 23 de novembro de 2001. **Convenção sobre o cibercrime**. Budapeste, Disponível em: https://www.cicdr.pt/documents/57891/128776/Conven%C3%A7%C3%A3o+Cibercrime.pdf/3c7fa1b1-b08e-4f66-9553-f4470f502b9c. Acesso em: 29 out. 2020.

113 JESUS, Damásio de; MILAGRE, José Antônio. Manual de crimes informáticos, São Paulo, Saraiva, 2016, p. 54.

> informação. A comitê foi dada a particular tarefa de preparar um instrumento legalmente vinculante – um tratado. O Comitê terminou seu trabalho no fim do ano de 2000, tendo trabalhado em coordenação com o G-8 e outros organismos internacionais no rascunho da Convenção sobre o *Cybercrime*.[114]

Em seu preâmbulo, a Convenção dispõe sobre sua própria importância para impedir atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, assim como a utilização fraudulenta de sistemas, redes e dados. Para tanto, via como necessário: a) assegurar a criminalização desses comportamentos; b) adotar poderes suficientes para combater essas infrações; c) facilitar a detecção, a investigação e o procedimento criminal a respeito das referidas infrações, nacional e internacionalmente; e d) estabelecer disposições materiais visando a uma cooperação internacional rápida e fiável.

Em seu Capítulo I, traz a Convenção diversas definições importantes – as quais, faltantes no ordenamento jurídico brasileiro, não raras vezes geram interpretações errôneas[115].

No Capítulo II, trata especificamente de medidas a serem tomadas a nível nacional. Na Seção 1, trata do Direito Penal material – que especificamente se relaciona com o objeto deste trabalho. Essa Seção se divide da seguinte forma: Título 1 – infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos; Título 2 – Infrações relacionada com computadores; Título

---

114 M. CHERIF BASSIOUNI (Itália). Osservatorio Permanente Sulla Criminalità Organizzata (org.). **Cybercrime**: conferenza Internazionale, Milão, Dott. A. Giuffrè, 2004, p. 3-4.

115 JESUS, Damásio de; MILAGRE, José Antônio. Manual de crimes informáticos, São Paulo, Saraiva, 2016, p. 54.

3 – Infrações relacionadas com o conteúdo; e Título 4 - Infrações relacionadas com a violação do direito de autor e direitos conexos. Os dois primeiros Títulos tratam de crimes cibernéticos próprios; o Título 3 trata de crimes cibernéticos impróprios; e o Título 4 trata de tema que não interessa ao presente trabalho.

A Comissão Parlamentar de Inquérito dos Crimes Cibernéticos, por sua vez, foi criada em 2015, visando à apuração de informações relacionadas a crimes cibernéticos no Brasil, tendo em vista os efeitos deletérios desses crimes e seu aumento significativo no país. De acordo com o Relatório Final da comissão,

> Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, o número de fraudes na Internet no Brasil aumentou 6.513% entre 2004 e 2009. A SaferNet Brasil, associação civil de direito privado, especializada no enfrentamento aos crimes e violações aos Direitos Humanos na Internet, nos últimos 09 (nove) anos recebeu e processou 3.606.419 denúncias anônimas, por meio da Central Nacional de Denúncias de Crimes Cibernéticos, envolvendo 585.778 páginas (URLs) distintas – das quais 163.269 foram removidas – conectados à Internet através de 41.354 números IPs distintos. Entre os 1.225 pedidos de ajuda e orientação psicológica atendidos pela SaferNet, em 2014, 222 foram vazamentos de fotos íntimas, situação chamada de sexting. Isso significa um aumento de 119,8% em relação a 2013. Mais da metade das vítimas tinha até 25 anos, das quais 25% tinham entre 12 e 17 anos.3 De acordo com a SaferNet, houve crescimento de 192,93% nas denúncias envolvendo páginas suspeitas de tráfico

de pessoas na comparação entre 2014 e 2013. 'O objetivo era recrutar pessoas, principalmente mulheres, inclusive adolescentes, para a prostituição em cidadessedes da Copa do Mundo', segundo Thiago Tavares, representante da entidade. A Central Nacional de Denúncias de Crimes Cibernéticos recebe uma média de 2.500 denúncias por dia envolvendo páginas na Internet contendo evidências dos crimes de Pornografia Infantil ou Pedofilia, Racismo, Neonazismo, Intolerância Religiosa, Apologia e Incitação a crimes contra a vida, Homofobia e maus tratos contra os animais. Ademais, diversas outas atividades no mercado negro da Internet são realizadas, em prejuízo considerável para o bem-estar social.

(...) Segundo a empresa, 8 de cada 10 brasileiros conectados à internet já foram vítimas de algum crime cibernético. Segundo o chefe da Unidade de Repressão a Crimes Cibernéticos da Polícia Federal, delegado Carlos Eduardo Miguel Sobral, os grupos de combate a fraudes eletrônicas foram transformados em delegacias de repressão a crimes cibernéticos. Além das fraudes eletrônicas bancárias, a Polícia Federal também investiga incidentes nas redes do Governo Federal por meio do Projeto Oráculo. A atuação é conjunta com o Departamento de Segurança da Informação e Comunicações (DSIC), órgão subordinado ao Gabinete de Segurança Institucional da Presidência da República. O DSIC é o responsável por planejar e coordenar a

> execução de atividades de segurança cibernética na administração pública federal. O Governo Federal possui 320 redes para monitorar ataques cibernéticos. Esses ambientes sofrem de 6 a 7 milhões de incidentes por ano. Desse montante, o que de fato preocupa é 1% dos casos, que são as tentativas sérias de furtos de dados. Isso representa uma média de dois mil ataques graves por hora nessas 320 redes, que partem de organizações criminosas ou de grupos de crackers mal-intencionados. Crackers invadiram a rede virtual da empresa Sony com 77 milhões de usuários do videogame Playstation. O ataque custará à empresa R$ 37,7 bilhões, segundo estimativa do Instituto Americano Ponemon.[116]

Comparem-se agora as condutas criminalizáveis consoante disposto pela Convenção de Budapeste com o ordenamento jurídico brasileiro.

A primeira delas diz respeito ao acesso ilegítimo, definido como "o acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático", podendo-se exigir que seja cometido "com a violação de medidas de segurança, com a intenção de obter dados informáticos ou outra intenção ilegítima, ou que seja relacionada com um sistema

---

116 CÂMARA DOS DEPUTADOS (Brasil). Congresso Nacional. CPI - Crimes cibernéticos: comissão parlamentar de inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país.. Brasília: __, 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D%3E+RCP+10/2015. Acesso em: 29 out. 2020, p. 8-11.

informático conectado a outro sistema informático". Para a Convenção, sistema informático (art. 1º, "a") é "qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles, *(sic)*[117] desenvolve, em execução de um programa, o tratamento automatizado de dados". Como visto, essa conduta é tipificada pelo art. 154-A do Código Penal.

A respeito desse artigo, o Relatório Final da CPI dos Crimes Cibernéticos, a partir da participação de delegados de polícia e de membros do Ministério Público, chegou à conclusão de que a redação do dispositivo dificulta sua aplicação: "o simples uso de dispositivos por terceiros, mesmo que sem autorização, não caracterizaria crime, na visão dos juízes". Além disso, "a simples quebra de sistemas de segurança ou, ainda, a alteração de páginas de internet – a chamada pichação virtual – ou de perfis nas redes sociais não configurariam automaticamente crime, de acordo com a redação dada". A propósito, uma curiosidade: apesar de a lei ser chamada "Carolina Dieckmann", não chegou a abarcar a própria situação que a atriz sofreu.[118]

Assim, a CPI sugeriu uma alteração no tipo penal, de modo que não se exigisse o elemento subjetivo do injusto (citado neste trabalho no item 3.2.2) nem a necessidade de que haja violação do mecanismo de segurança. Isso porque o acesso indevido já violaria os direitos relacionados à intimidade e à privacidade da vítima. Exigiria, entretanto,

---

[117] O texto original possui essa vírgula gramaticalmente indevida.

[118] CÂMARA DOS DEPUTADOS (Brasil). Congresso Nacional. CPI - Crimes cibernéticos: comissão parlamentar de inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país.. Brasília: __, 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D%3E+RCP+10/2015. Acesso em: 29 out. 2020, p. 209-211.

que os dados informatizados fossem expostos a risco de divulgação ou utilização indevidas.[119]

A segunda trata da interceptação ilegítima, ou seja,

> a interceptação intencional e ilegítima de dados informáticos, efectuada por meios técnicos, em transmissões não públicas, para, de ou dentro de um sistema informático, incluindo emissões electromagnéticas provenientes de um sistema informático que veicule esses dados.

No Brasil, como visto, a conduta é tipificada pelo art. 10 da Lei 9.296/90[120].

A terceira diz respeito à interferência em dados, que é "o acto de intencional e ilegitimamente danificar, apagar, deteriorar, alterar ou eliminar dados informáticos". Caso o dano resulte de invasão, impõe-se o art. 154-A do Código Penal; caso haja dano somente, então o crime será de dano, nos termos do art. 163 do Código Penal.

A quarta conduta que a Convenção fomenta criminalizar é a interferência em sistemas, a qual poderia ser traduzida como "obstrução grave, intencional e ilegítima, ao funcionamento de um sistema informático, através da introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos". A despeito de os autores Damásio de Jesus e José Antônio Milagre[121] afirmarem que o art. 266 do Código Penal cobre somente parte das

---

119 *Idem, ibidem*, p. 209.

120 Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei: Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa. Parágrafo único. Incorre na mesma pena a autoridade judicial que determina a execução de conduta prevista no caput deste artigo com objetivo não autorizado em lei.

121 JESUS, Damásio de; MILAGRE, José Antônio. Manual de crimes informáticos, São Paulo, Saraiva, 2016, p. 44.

condutas acima descritas, na realidade há cobertura total das condutas, uma vez que "interromper" ou "perturbar" serviço telegráfico, radiotelegráfico, telefônico, telemático ou de utilidade pública, "impedir" ou "dificultar-lhe" o restabelecimento abrange todo o conteúdo da conduta prevista na Convenção.

A quinta seria o uso abusivo de dispositivos eletrônicos, que abrangeria as seguintes situações. Em primeiro lugar, produzir, vender, obter, utilizar, importar, distribuir ou de outra forma disponibilizar: a) um dispositivo, incluindo um programa informático, concebido ou adaptado essencialmente para permitir a prática de uma das condutas acima previstas; b) uma palavra-passe, um código de acesso ou dados informáticos semelhantes que permitam acessar no todo ou em parte um sistema informático. Em segundo lugar, ter sob sua posse um dispositivo como o acima citado, com a intenção de ser utilizado com o objetivo de cometer qualquer uma das infrações acima referidas. Com exceção da posse de algum dispositivo conforme o exposto, o Brasil de alguma maneira já criminaliza as condutas acima mencionadas: no art. 154-A, § 1º, do Código Penal, ao tipificar a produção, o oferecimento e a venda de dispositivos utilizáveis para invadir dispositivos informáticos alheios; e no art. 325, §1º, I[122]. Entretanto, ressalve-se que este último crime fica restrito ao âmbito da Administração Pública.

A sexta conduta prevista pela Convenção diz respeito à falsidade informática, consistente na introdução, alteração, eliminação ou supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que estes sejam considerados ou utilizados

[122] Art. 325 - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação: Pena - detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave. § 1o Nas mesmas penas deste artigo incorre quem: I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública.

para fins ilegais, sendo ou não diretamente legíveis e inteligíveis. No Brasil, a conduta pode amoldar-se ao tipo penal do art. 299[123] do Código Penal, no caso de dados privados; ou ao tipo penal do art. 313-A do Código Penal[124], no âmbito da Administração Pública.

A sétima conduta prevista pela Convenção trata da burla informática, conceituada como o ato intencional e ilegítimo que dê origem à perda de bens a terceiros através: a) da introdução, da alteração, da eliminação ou da suspensão de dados informáticos; ou b) de qualquer intervenção no funcionamento de um sistema informático. Damásio de Jesus e de José Antônio Milagre, os quais afirmam não ter um único tipo penal claro no ordenamento jurídico brasileiro para fazer frente a tal conduta[125]. Essa declaração merece reparos.

Os núcleos são os seguintes: introduzir, alterar, eliminar ou suprimir dados informáticos. Caso o dano resulte de invasão, impõe-se o art. 154-A do Código Penal; caso haja dano somente, então o crime será de dano, nos termos do art. 163 do Código Penal. Introduzir e alterar

---

123 Por lesionar outros bens jurídico-penais como a fé pública, será em tese considerada crime cibernético misto: Falsidade ideológica Art. 299 - Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante: Pena - reclusão, de um a cinco anos, e multa, se o documento é público, e reclusão de um a três anos, e multa, de quinhentos mil réis a cinco contos de réis, se o documento é particular. Parágrafo único - Se o agente é funcionário público, e comete o crime prevalecendo-se do cargo, ou se a falsificação ou alteração é de assentamento de registro civil, aumenta-se a pena de sexta parte.

124 Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.

125 JESUS, Damásio de; MILAGRE, José Antônio. Manual de crimes informáticos, São Paulo, Saraiva, 2016, p. 45.

dados, mais uma vez, podem amoldar-se ou ao art. art. 299 do Código Penal, no caso de dados privados; ou ao tipo penal do art. 313-A do Código Penal, no âmbito da Administração Pública.

A respeito de dar-se origem à perda de bens a terceiros através de qualquer intervenção no funcionamento de um sistema informática, o que merece reparo é a própria redação da Convenção. Trata-se de um pretendido tipo penal extremamente aberto, de modo que pode ser perpetrado de inúmeras maneiras. Imagine-se o caso de alguém que, invadindo o sistema de um banco, destrua dados relacionados à conta de um correntista, fazendo-o perder muito dinheiro. Nesse caso, pode-se enxergar, em tese, a aplicação do art. 154, § 2º, do Código Penal[126].

A única ressalva que deve ser feita é que a Convenção de Budapeste exige uma perda de bens de terceiros. Isso pode ou não ocorrer no caso concreto, e, ocorrendo, certamente acarretará aumento de pena por permitir valorar negativamente uma das circunstâncias judiciais do art. 59 do Código Penal: as consequências do crime. Caso o Brasil, todavia, realmente queira especificar a conduta esmiuçadamente tal qual fez a Convenção, então, realmente, necessita-se de um novo tipo penal.

Finalmente, desta feita se relacionando com um dos crimes cibernéticos impróprios mais preocupantes, a Convenção traz, em seu art. 9º, disposição acerca do dever de os Estados criminalizarem condutas relacionadas com pornografia infantil e sistemas informáticos:

> Artigo 9º - Infracções relacionadas com pornografia infantil

---

[126] Revelando uma pena extremamente irrisória se comparada ao possível prejuízo: 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. (...)§ 2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

1.Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, as seguintes condutas, quando cometidas de forma intencional e ilegítima:
a) Produzir pornografia infantil com o objectivo da sua difusão através de um sistema informático;
b) Oferecer ou disponibilizar pornografia infantil através de um sistema informático; c) Difundir ou transmitir pornografia infantil através de um sistema informático;
d) Obter pornografia infantil através de um sistema informático para si próprio ou para terceiros;
e) Possuir pornografia infantil num sistema informático ou num meio de armazenamento de dados informáticos.
2. Para efeitos do n.º 1, a expressão "pornografia infantil" inclui qualquer material pornográfico que represente visualmente:
a) Um menor envolvido num comportamento sexualmente explícito;
b) Uma pessoa que aparente ser menor envolvida num comportamento sexualmente explícito;
c) Imagens realísticas que representem um menor envolvido num comportamento sexualmente explícito;
3. Para efeitos do n.º 2, a expressão "menor" inclui qualquer pessoa com idade inferior a 18 anos. Uma Parte, pode, no entanto, exigir um limite de idade inferior, que não será menos que 16 anos.

> 4. Cada Parte pode reservar-se o direito de não aplicar, no todo ou em parte, o disposto nos n.ºs 1, alínea d), e., 2, alíneas b) e c).

O Brasil não só tipifica as condutas nesse artigo mencionadas, como também vai além. Por exemplo, a conduta objeto de criminalização no art. 9º, "a", da Convenção, estabelece um fim específico para a ação de produzir pornografia infantil: o de difundi-la através de sistema informático. O Brasil, no Estatuto da Criança e do Adolescente (Lei 8.069/90[127]), criminaliza a conduta com diversos núcleos do tipo, sem exigir elemento subjetivo do injusto, o que aumenta a proteção dos bens jurídicos das crianças e dos adolescentes frente aos crimes (não apenas cibernéticos):

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. § 1 o Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena. § 2 o Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime: (Redação dada pela Lei nº 11.829, de 2008) I – no

[127] BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Lei Nº 8.069, de 13 de julho de 1990**. Brasília, DF, 13 jul. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 29 out. 2020.

> exercício de cargo ou função pública ou a pretexto de exercê-la; II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou (Redação dada pela Lei nº 11.829, de 2008) III – prevalecendo-se de relações de parentesco consangüíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento.

E, tratando especificamente do caráter cibernético envolvendo essas ações, o ECA aprofunda-se, tipificando, além das condutas previstas na Convenção (art. 241-A e 241-B), a que diz respeito a montagens simulando a participação de crianças e adolescentes em cena de sexo explícito ou pornográfica:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
> § 1 o Nas mesmas penas incorre quem:
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;

II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.

§ 2 o As condutas tipificadas nos incisos I e II do § 1 o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.

Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§ 1 o A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.

§ 2 o Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:

I – agente público no exercício de suas funções;

II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;

> III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.
> § 3 o As pessoas referidas no § 2 o deste artigo deverão manter sob sigilo o material ilícito referido.
> Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual:
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
> Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo.

Há mais uma coisa a ser analisada nessas comparações: a CPI, quando de sua feitura, concluiu ser necessário um novo tipo penal criminalizando a conduta conhecida como *revenge porn*, ou pornografia de vingança – que consiste na divulgação sem autorização da vítima de cenas de sexo, nudez ou pornografia em que ela apareça. Isso foi resolvido com

o advento da Lei 13.718/18[128], a qual insere no Código Penal o seguinte tipo, referente a um crime cibernético impróprio:

> Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia:
> Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.

A partir dessa análise, pode-se concluir que a legislação penal do Brasil não é deficiente frente ao problema dos crimes cibernéticos: dispomos de tipos penais aptos a enquadrar a maioria das condutas que a Convenção de Budapeste prevê. Entretanto, algumas melhorias podem ser feitas: a primeira parte da já mencionada dificuldade de aplicação do art. 154-A, cuja solução já foi apontada. A segunda diz respeito à

---

128 BRASIL. Lei nº 13.718, de 25 de setembro de 2018. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). **Lei Nº 13.718, de 24 de setembro de 2018**. Brasília, DF, 24 set. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm. Acesso em: 30 out. 2020.

criminalização da posse de dispositivos concebidos essencialmente para permitir crimes cibernéticos. A terceira é revelada pela ínfima pena aplicável a uma invasão de sistema que gere prejuízo financeiro (cf. nota de rodapé nº126). Nesse caso, haveria de se discutir a possibilidade de uma sanção mais gravosa, em virtude da possibilidade extremamente danosa desse crime – imaginando, por exemplo, que um correntista (ou mesmo o próprio banco, num caso mais extremo) perca todas as suas economias.

4. CONSIDERAÇÕES FINAIS

Estamos atravessando um momento em que novos problemas põem em xeque nossas certezas antigas. Por ainda não aceitar novas soluções, a sociedade aparenta viver um momento niilista de desilusão e raiva. Adota-se generalizadamente uma postura de pânico ante a consciência da mudança que se vive. É a postura errada[129].

Segundo o já tão citado professor Harari, não se deve adotar uma postura de pânico, mas uma postura de perplexidade. Segundo o autor, o pânico é uma forma de prepotência: deriva da pretensiosa sensação de que se sabe para onde o mundo está caminhando – ladeira abaixo. A verdade é que não sabemos. A aceitação da ignorância é o primeiro passo para superá-la. O segundo é buscar respostas. Nesse sentido, buscou o presente trabalho abordar, no âmbito do Direito Penal, implicações advindas do momento histórico que embala o mundo: a Quarta Revolução Industrial.

Diferentemente das Revoluções que a sucederam, a Quarta Revolução Industrial se diferencia por seu ritmo extraordinariamente acelerado, sua amplitude e sua profundidade, muito em razão da quantidade e qualidade das novas tecnologias, as quais se inter-relacionam de modo incrível, originando a hiperconexão das pessoas e das coisas.

Apesar das mudanças, mantém-se o Direito como elemento essencial de pacificação, sendo o Direito Penal seu desdobramento mais

---

[129] HARARI, Yuval Noah. 21 lições para o século 21, São Paulo, Companhia das Letras, 2018, p. 37-38.

enérgico, o qual, tendo superado momentos obscuros de uso de força desmedida, vive uma constante tensão, consistente na função de proteção de bens jurídicos e garantia do réu frente a possíveis arbitrariedades – revestindo-se de enorme importância, nesse contexto, o princípio da exclusiva proteção de bens jurídicos.

Buscou-se abordar o conceito de bem jurídico-penal, em análise da obra de Cláudio Brandão, fazendo sua retrospectiva história, desde antes de sua concepção, com Feuerbach, passando por seu teórico inicial, Birnbaum, e pelo positivismo de Binding, até a noção que se tem hoje, derivada do neokantismo, chegando-se à conclusão de que bem jurídico o conteúdo material do crime, traduzido no valor tutelado pelo direito.

Em momento posterior, tratou-se do princípio da exclusiva proteção de bens jurídicos, analisando-se a obra de Santiago Mir Puig, que entende duas serem as condições necessárias para um bem jurídico ser considerado um bem jurídico-penal: a) revestir-se de suficiente importância social; e b) necessitar de proteção pelo Direito Penal – ainda discorrendo brevemente sobre a fragmentariedade do Direito Penal.

Depois, buscou-se abordar o conceito de expansionismo penal, formulado por Jesús-Maria Silva Sánchez, condenando o uso do direito penal como mera solução simples a problemas complexos – ou como legislação simbólica, nos dizeres de Marcelo Neves. Apontou-se que se trata, na verdade, de uma expansão razoável a proteção, pelo Direito Penal, da tecnologia da informação, em virtude da hiperconexão e seu crescimento no contexto da Indústria 4.0, de fertilidade para a prática de crimes cibernéticos.

Numa síntese entre Quarta Revolução Industrial e Direito Penal, chegou-se à conclusão de que a tecnologia da informação é um bem jurídico-penal, sendo passível das consequências que isso implica e revelando-se numa dinâmica já existente há algum tempo, mas que tem se desenvolvido especialmente nos últimos tempos: a da criminalidade cibernética.

Passou-se a tratar, finalmente, dos crimes cibernéticos, apontando inicialmente a dificuldade terminológica em virtude de cada autor denominá-lo diferentemente dos demais, optando-se pelo termo crime cibernético (ou aqueles correlatos).

Em seguida, buscou conceituar esses crimes cibernéticos, chegando-se à conclusão de ser um fato típico, ilícito e culpável cometido contra a ou por meio da tecnologia da informação, o que implicou a tipologia feita em seguida, que os distinguiu em crimes cibernéticos próprios (ou puros), impróprios (ou impuros) e mistos.

Depois, abordaram-se os crimes cibernéticos próprios no ordenamento jurídico brasileiro, que estão previstos nos seguintes dispositivos: art. 154-A do Código Penal; 266 do Código Penal; art. 10 da Lei 9.296/96; e arts. 313-A e 313-B do Código Penal.

Em um momento posterior, buscou o presente trabalho abordar algumas questões normalmente discutidas no âmbito do estudo dos crimes cibernéticos: técnicas e condutas criminosas, lugar do crime e autoria. Quanto às primeiras, observou-se não ser profícuo tipificar técnicas cibernéticas, visto que elas estão em constante mudança e aperfeiçoamento; na verdade, devem-se tipificar as condutas (que abrangem ou não as técnicas, mas não se reduzem a elas). Quanto ao lugar do crime, demonstrou-se que, por nosso Código Penal adotar a teoria da ubiquidade, não se reveste de maior problemática a questão, visto que será considerado local do crime onde ele for praticado ou onde ele produzir (ou dever produzir) seu resultado.

Questão mais complexa foi a relacionada à autoria dos crimes cibernéticos, mas demonstraram-se, com base em informações do Ministério Público e na Lei 12.965/14, os caminhos a serem percorridos pelas forças de investigação no sentido de encontrar o autor da conduta cibernética criminosa: obter o endereço de IP mediante perícia; com autorização judicial obter, perante os provedores, informações acerca do IP; e, finalmente, também com autorização do Poder Judiciário, proceder às diligências referentes à quebra de sigilo telefônico.

No tópico final, tratou-se de analisar uma possível deficiência na legislação penal brasileira frente aos crimes cibernéticos, tomando-se como parâmetros a Convenção sobre o Cibercrime (Convenção de Budapeste) e a Comissão Parlamentar de Inquérito sobre os Crimes Cibernéticos, no âmbito da Câmara dos Deputados. Chegou-se à conclusão de que não há uma deficiência, de forma geral, na legislação penal brasileira ante os *cybercrimes,* mas apontaram-se aperfeiçoamentos a serem realizados no sentido de melhor proteger o bem jurídico-penal tecnologia da informação.

REFERÊNCIAS

2017 Norton Cyber Security Insights Report. 2017. Disponível em: https://www.nortonlifelock.com/us/en/newsroom/press-kits/ncsir-2017/#:~:text=Uncover%20the%20discrepancies%20behind%20consumers,21%2C000%20consumers%20in%2020%20countries.. Acesso em: 29 out. 2020.

ALI, Aran. Here's what happens every minute on the internet in 2020. 2020. Disponível em: https://www.weforum.org/agenda/2020/09/internet-social-media-downloads-uploads-facebook-twitter-youtube-instagram-tiktok/. Acesso em: 14 out. 2020.

ASÚA, Luis Jiménez de. Principios de derecho penal: la ley y el delito, Buenos Aires, Abeledo-Perrot, 1997.

BITTENCOURT, Cézar Roberto. Tratado de direito penal: parte geral, São Paulo, Saraiva, 2016, 22ª ed.

BRANDÃO, Cláudio. "Bem jurídico e norma penal: a função da antinormatividade na teoria do crime". DELICTAE: Revista de Estudos Interdisciplinares sobre o Delito, v. 3, n. 4, Belo Horizonte, 2018.

BRANDÃO, Cláudio. Teoria jurídica do crime, São Paulo, Atlas, 2015, 4ª ed.

BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. **Decreto Nº 8.771, de 11 de Maio de 2016**. Brasília, DF, 11 maio 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm. Acesso em: 29 out. 2020.

BRASIL. Decreto-Lei nº 1.001, de 21 de outubro de 1969. Código Penal Militar. **Decreto-Lei Nº 1.001, de 21 de outubro de 1969**. Brasília, DF, 21 out. 1969. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del1001.htm. Acesso em: 29 out. 2020.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. **Decreto-Lei Nº 2.848, de 7 de dezembro de 1940**. Rio de Janeiro, RJ, 7 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 29 out. 2020.

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº

1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. **Lei Nº 12.735, de 30 de novembro de 2012**. Brasília, DF, 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 29 out. 2020.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.. **Lei Nº 12.737, de 30 de novembro de 2012**. Brasília, DF, 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm#:~:text=Disp%C3%B5e%20sobre%20a%20tipifica%C3%A7%C3%A3o%20criminal,Art.. Acesso em: 29 out. 2020.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.. **Lei Nº 12.965, de 23 de abril de 2014**. Brasília, DF, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 29 out. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Lei Nº 13.709, de 14 de agosto de 2018.** Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 29 out. 2020

BRASIL. Lei nº 13.718, de 25 de setembro de 2018. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a

liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). **Lei Nº 13.718, de 24 de setembro de 2018**. Brasília, DF, 24 set. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm. Acesso em: 30 out. 2020.

BRASIL. Lei nº 7.716, de 5 de janeiro de 1989. Define os crimes resultantes de preconceito de raça ou de cor.. **Lei Nº 7.716, de 5 de Janeiro de 1989.**. Brasília, DF, 5 jan. 1989. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 29 out. 2020.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Lei Nº 8.069, de 13 de julho de 1990**. Brasília, DF, 13 jul. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 29 out. 2020.

BRASIL. MINISTÉRIO PÚBLICO FEDERAL. Crimes cibernéticos: coletânea de artigos, Brasília, MPF, 2018, 3ª ed.

BRASIL. Procuradoria da República no Estado de São Paulo. Ministério Público Federal. **Crimes cibernéticos**: manual prático de investigação, São Paulo, _____, 2006.

BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. Crime cibernético tomou lugar de roubos e furtos na pandemia, diz ministro Humberto Martins. 2020. Disponível em: http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Cri

me-cibernetico-tomou-lugar-de-roubos-e-furtos-na-pandemia--diz-o-ministro-Humberto-Martins.aspx. Acesso em: 23 nov. 2020.

BRITO, Edivaldo. O que é o IP?: descubra para que serve e qual é seu número. Descubra para que serve e qual é seu número. 2013. Disponível em: https://www.techtudo.com.br/artigos/noticia/2013/05/o-que-e-o-ip-descubra-para-o-que-serve-e-qual-e-seu-numero.html. Acesso em: 27 out. 2020.

CÂMARA DOS DEPUTADOS (Brasil). Congresso Nacional. **CPI - Crimes cibernéticos**: comissão parlamentar de inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país.. Brasília: __, 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D%3E+RCP+10/2015. Acesso em: 29 out. 2020.

CARO, Lucía. **Principales delitos cibernéticos del siglo XXI en España**. 2018. Disponível em: https://www.legaltoday.com/practica-juridica/derecho-penal/penal/principales-delitos-ciberneticos-del-siglo-xxi-en-espana-2018-12-28/. Acesso em: 29 out. 2020.

CEROY, Frederico Meinberg. Os conceitos de provedores no Marco Civil da Internet. 2014. Disponível em: https://migalhas.uol.com.br/depeso/211753/os-conceitos-de-provedores-no-marco-civil-da-internet. Acesso em: 28 out. 2020.

CONSELHO DA EUROPA. Tratado nº 185, de 23 de novembro de 2001. **Convenção sobre o cibercrime**. Budapeste, Disponível em: https://www.cicdr.pt/documents/57891/128776/Conven%C3%A7%C3

%A3o+Cibercrime.pdf/3c7fa1b1-b08e-4f66-9553-f4470f502b9c. Acesso em: 29 out. 2020.

CUNHA, Rogério Sanches. **Manual de direito penal**: parte especial, Salvador: Juspodivm, 2017, 9ª ed.

DOW, Sheila. **What's the future of cryptocurrencies?** 2018. Disponível em: https://www.weforum.org/agenda/2018/08/cryptocurrencies-are-useful-but-will-not-save-us. Acesso em: 15 out. 2020.

FERRAZ JÚNIOR, Tércio Sampaio. Introdução ao estudo do direito: técnica, decisão, dominação, São Paulo, Atlas, 2015, 8ª ed.

FRAZIER, Kevin. COVID-19 Shows we need Universal Basic Internet now. 2020. Disponível em: https://www.weforum.org/agenda/2020/05/covid19-coronavirus-united-states-internet-acess-universal-basic/. Acesso em: 15 out. 2020.

GUSMÃO, Paulo Dourado de. Introdução ao estudo do direito, Rio de Janeiro, Forense, 2015, 46ª ed.

Hackers and crackers. 2002. Disponível em: https://www.informit.com/articles/article.aspx?p=30048#:~:text=They%20might%20discover%20holes%20within,remote%20machines%20with%20malicious%20intent.. Acesso em: 22 out. 2020.

HARARI, Yuval Noah. 21 lições para o século 21, São Paulo, Companhia das Letras, 2018.

HARARI, Yuval Noah. **Homo deus**: uma breve história do amanhã, São Paulo, Companhia das Letras, 2016.

HARARI, Yuval Noah. **Sapiens:** Uma breve história da humanidade, Porto Alegre, L&PM, 2017, 29ª ed.

HOBSBAWM, Eric J. A era das revoluções: 1789 – 1848, Rio de Janeiro/São Paulo, Paz e Terra, 2019, 41ª ed.

JACKSON, Reuben. How cybercrime has evolved since the pandemic hit: opportunistic agility is running rampant among hackers and scammers.. Opportunistic agility is running rampant among hackers and scammers.. 2020. Disponível em: https://bigthink.com/technology-innovation/cybercrime-evolved-during-pandemic?rebelltitem=1#rebelltitem1. Acesso em: 15 out. 2020.

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

JEVONS, H. Stanley. "The Second Industrial Revolution". The Economic Journal, [s.l.], v. 41, n. 161, Oxford, mar. 1931.

M. CHERIF BASSIOUNI (Itália). Osservatorio Permanente Sulla Criminalità Organizzata (org.). Cybercrime: conferenza internazionale, Milão, Dott. A. Giuffrè, 2004.

Meaning of information technology in English. Disponível em: https://dictionary.cambridge.org/dictionary/english/information-technology. Acesso em: 28 out. 2020.

Meet the Three Industrial Revolutions. Disponível em: https://trailhead.salesforce.com/pt-BR/content/learn/modules/learn-about-the-fourth-industrial-revolution/meet-the-three-industrial-revolutions#:~:text=Beginning%20in%20the%201950s%2C%20the,the%

20Internet%E2%80%94the%20digital%20revolution.. Acesso em: 29 out. 2020.

MEOLA, Andrew. **How smart city technology & the Internet of Things will change our apartments, grids and communities**. 2020. Disponível em: https://www.businessinsider.com/iot-smart-city-technology#:~:text=What%20is%20a%20smart%20city,utilities%20and%20services%2C%20and%20more.. Acesso em: 15 out. 2020.

MOHAJAN, Haradhan Kumar. "The Second Industrial Revolution has Brought Modern Social and Economic Developments". Journal Of Social Science And Humanities, v. 6, Chittagong, jan. 2020. Disponível em: https://www.researchgate.net/publication/338670501_The_Second_Industrial_Revolution_has_Brought_Modern_Social_and_Economic_Developments. Acesso em: 01 abr. 2020.

NEVES, Marcelo. A constitucionalização simbólica, São Paulo, Editora WMF Martins Fontes, 2011, 3ª ed.

O que se sabe sobre a Operação Spoofing e o hacker que interceptou mensagens de autoridades. 2019. Disponível em: https://g1.globo.com/politica/noticia/2019/07/24/o-que-se-sabe-sobre-a-operacao-spoofing-e-os-suspeitos-de-interceptar-mensagens-de-autoridades.ghtml. Acesso em: 29 out. 2020.

OLIVEIRA, Eduardo Cunha. **AS SOLICITAÇÕES DOS REGISTROS DE CONEXÃO (IP) SEM AUTORIZAÇÃO JUDICIAL**. 2019. Disponível em: http://silvavitor.com.br/as-solicitacoes-dos-registros-de-conexao-ip-sem-autorizacao-judicial/. Acesso em: 28 out. 2020.

Operação Spoofing: MPF denuncia sete por crimes envolvendo invasões de celulares de autoridades brasileiras. 2020. Disponível em:

http://www.mpf.mp.br/df/sala-de-imprensa/noticias-df/operacao-spoofing-mpf-denuncia-sete-por-crimes-envolvendo-invasoes-de-celulares-de-autoridades-brasileiras. Acesso em: 29 out. 2020.

OS MISERÁVEIS. Direção de Tom Hooper. Produção de Tim Bevan, Eric Fellner, Debra Hayward e Cameron Mackintosh. Intérpretes: Hugh Jackman. Roteiro: William Nicholson. Música: Claude-Michel Schönberg e Anne Dudley. S.I.: Working Title Films, Cameron Mackintosh Ltd. e Relativity Media, 2012. (158 min.), son., color. Legendado.

P2P. Disponível em: https://techterms.com/definition/p2p#:~:text=Stands%20for%20%22Peer%20to%20Peer,as%20well%20as%20a%20client.. Acesso em: 23 out. 2020.

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

PL 7100/2017. 2017. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2125353. Acesso em: 28 out. 2020.

PRADO, Luís Régis. Curso de direito penal brasileiro: parte geral e parte especial. 14. ed. São Paulo: Editora Revista dos Tribunais, 2015.

PUIG, Santiago Mir. **El derecho penal en el Estado social y democrático de derecho**, Barcelona, Editorial Ariel S.A., 1994.

REALE, Miguel. **Lições preliminares de direito**, São Paulo, Saraiva, 2002, 27ª ed.

REVISTA DE SEGUROS: CNSeg, v. 93, n. 909, Rio de Janeiro, abril-junho, 2019. Disponível em: https://cnseg.org.br/publicacoes/revista-de-seguros-n-909.html. Acesso em: 29 out. 2020.

ROBERTS, Brian. The Third Industrial Revolution: Implications for Planning Cities and Regions. Disponível em https://www.researchgate.net/publication/275644911_THE_THIRD_INDUSTRIAL_REVOLUTION_Implications_for_Planning_Cities_and_Regions. Acesso em: 06 de abril de 2020.

RUSSEL, Bertrand. História do pensamento ocidental: a aventura dos pré-socráticos a Wittgenstein, Rio de Janeiro, Ediouro, 2001.

SÁNCHEZ, Jesús-Maria Silva. La expansión del derecho penal: aspectos de la política criminal en las sociedades postindustriales, Madrid, Civitas, 2001, 2ª ed.

SCHMITT, Guilherme. Crimes cibernéticos. 2014. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos#:~:text=Da%20Autoria,indevido%20de%20suas%20senhas%20pessoais.. Acesso em: 26 out. 2020.

SCHWAB, Klaus. **A quarta revolução industrial**, São Paulo, Edipro, 2016.

SILVA, Ângelo Roberto Ilha da *et al.* Crimes cibernéticos: racismo, cyberbullying, deep web, pedofilia e pornografia infantojuvenil, infiltração de agentes por meio virtual, obtenção das provas digitais, nova lei antiterrorismo, outros temas, Porto Alegre, Livraria do Advogado, 2018, 2ª ed.

SIQUEIRA, Fernando de. **Conceitos de Tecnologia de Informação**. Disponível em: https://sites.google.com/site/uniplisistemasdeinfogerenciais/aulas/1---conceitos-de-tecnologia-de-informacao. Acesso em: 20 out. 2020.

SOARES, Daniel Menah Cury. **Crimes informáticos:** uma breve resenha e apontamento de complicações. 2019. Disponível em: https://migalhas.uol.com.br/depeso/308978/crimes-informaticos--uma-breve-resenha-e-apontamento-de-complicacoes. Acesso em: 19 out. 2020.

TAVARES, Juarez. Teorias do delito: variações e tendências, São Paulo, Revista dos Tribunais, 1980.

TROLLOPE, Anthony. The Last Chronicles of Barset: The Chronicles of Barsetshire, Oxford, University Press, 2014.

Ukranian who pleaded guilty in hacking scheme gets 30 months in prison. Disponível em: https://www.washingtonpost.com/business/economy/ukranian-who-pleaded-guilty-in-hacking-scheme-gets-30-months-in-prison/2017/05/22/8749ea1e-3efe-11e7-8c25-44d09ff5a4a8_story.html. Acesso em: 26 out. 2020.

UNIÃO EUROPEIA. Regulamento nº 2016/679, de 27 de abril de 2016. **Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 april 2016**. Bruxelas, 27 abr. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 29 out. 2020.

Vendas no e-commerce crescem 145% no 1º semestre e dobram faturamento de lojistas. 2020. Disponível em: https://www.ecommercebrasil.com.br/noticias/vendas-e-commerce-crescem-semestre/. Acesso em: 29 out. 2020.

WELZEL, Hans. Derecho penal: parte general, Buenos Aires, Roque Depalma Editor, 1956.

What are cryptoassets (cryptocurrencies)? Disponível em: https://www.bankofengland.co.uk/knowledgebank/what-are-cryptocurrencies. Acesso em: 15 out. 2020.

WINDER, Davey. **These Hackers Have Made $100 Million And Could Earn $1 Billion By 2025**. 2020. Disponível em: https://www.forbes.com/sites/daveywinder/2020/05/29/these-incredible-100-million-hackers-could-make-1-billion-by-2025-hackerone-bounty-millionaires/?sh=7b02fedd77b8. Acesso em: 29 out. 2020.

ZAFFARONI, Eugênio Raul *et al*. **Derecho penal**: parte general, Buenos Aires: Ediar, 2002, 2ª ed.

ZAMBARDA, Pedro. **Internet das Coisas**: entenda o conceito e o que muda com a tecnologia. entenda o conceito e o que muda com a tecnologia. 2014. Disponível em: https://www.techtudo.com.br/noticias/noticia/2014/08/internet-das-coisas-entenda-o-conceito-e-o-que-muda-com-tecnologia.html. Acesso em: 13 abr. 2020.