2022
FLUXO CONTÍNUO
Ed. 37 - Vol. 1. Págs. 512-527

JNT - FACIT BUSINESS AND TECHNOLOGY JOURNAL ISSN: 2526-4281 - QUALIS B1

A ASCENSÃO DOS CRIMES CIBERNÉTICOS NO CONTEXTO CONTEMPORÂNEO

THE RISE OF CYBER CRIME IN THE CONTEMPORARY CONTEXT

Rogério da Costa MARTINS FILHO
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: rogeriocostacostacosta698@gmail.com

Roniel Bispo LEITE
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: ronielbleite@gmail.com

Pollyanna Marinho Medeiros CEREWUTA
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: pollyanna.cerewuta@unitpac.edu.br

RESUMO

Este estudo analisa o crescimento dos ataques cibernéticos no mundo contemporâneo, algo que tem ganhado cada vez mais ênfase nos últimos tempos, tendo em vista que isso se tornara um dos principais problemas de segurança no mundo virtual da atualidade. O objetivo é compreender o atual contexto deste problema e analisar como tudo isso se desenvolveu até o quadro atual. O estudo foi desenvolvido com base metodológica, esmiuçando os pormenores dessa conjuntura. A contemporaneidade trouxe inúmeras inovações e transformações no âmbito social, político, econômico e cultural, basicamente se vive em outra era nos dias de hoje, um mundo completamente diferente do que era cinquenta anos atrás, o advento da revolução técnico-científico foi um dos pilares que proporcionou essa revolução. O mundo virtual está intrinsecamente ligado ao convívio social das pessoas e das instituições, entretanto nem tudo é benéfico, pois há algo muito crescente nesse virtual, os crimes cibernéticos. Esses ilícitos estão crescendo demasiadamente nos últimos tempos, de modo que este cenário está se tornando um grande problema de segurança, algo que os governos, instituições e companhias deverão se centrar nos próximos anos para tentar mitigar ao máximo os danos e prejuízos nesse novo contexto de ataques cibernéticos.

Palavras-Chave: Revolução. Crimes Cibernéticos. Governo. Internet.

ABSTRACT

This study analyzes the growth of cyber attacks in the contemporary world, something that has gained more and more emphasis in recent times, given that it has become one of the main security problems in today's virtual world. The objective is to understand the current context of this problem and analyze how it all developed to the current situation. The study was developed on a methodological basis, detailing the details of this situation. Contemporaneity has brought countless innovations and transformations in the social, political, economic and cultural spheres, basically we live in another era these days, a completely different world from what it was fifty years ago, the advent of the technical-scientific revolution was one of the pillars that provided this revolution. The virtual world is intrinsically linked to the social life of people and institutions, however not everything is

beneficial, as there is something very growing in this virtual world, cyber crimes. These illicit acts are growing excessively in recent times, so this scenario is becoming a major security problem, something that governments, institutions and companies will have to focus on in the coming years to try to mitigate as much as possible the damages and losses in this new context of cyber attacks.

Keywords: Revolution. Cyber Crimes. Government. Internet.

INTRODUÇÃO

Este estudo analisa o crescimento dos ataques cibernéticos no mundo contemporâneo, algo que tem ganhado cada vez mais ênfase nos últimos tempos, tendo em vista que isso se tornara um dos principais problemas de segurança no mundo virtual da atualidade.

O processo informático é um dos elementos que ganharam uma relevância substancial no atual cenário de globalização tecnológica. A estruturação da maioria dos setores da sociedade teve que convergir para esta nova realidade, todavia, o processo de adaptação ainda traz sérios desafios e obstáculos que precisam ser enfrentados e vencidos em face desta nova adequação.

A área digital está intrinsecamente inserida na maioria dos grandes centros e localidades. A necessidade de acoplar e organizar dados, o processo de automação que já substituiu o físico em muitas esferas, a busca por mão de obra para preencher e desempenhar atividades que estão surgindo em face deste cenário em constante mudança, com isso, o crime organizado também se adaptou com essas novas mudanças.

Os delitos cibernéticos constituem a frente mais moderna do crime organizado, área que se alavancou nas últimas duas décadas devido à introdução em larga da internet e a expansão dos serviços de mídia. As organizações criminosas aperfeiçoaram suas táticas e trabalham com táticas cirúrgicas para obter a máxima de rentabilidade de suas atividades ilícitas.

O objetivo é compreender o atual contexto deste problema e analisar como tudo isso se desenvolveu até o quadro atual. A contemporaneidade trouxe inúmeras inovações e transformações no âmbito social, político, econômico e cultural, basicamente se vive em outra era nos dias de hoje, um mundo completamente diferente do que era cinquenta anos

atrás, o advento da revolução técnico-científico foi um dos pilares que proporcionou essa revolução.

A metodologia utilizada nesta pesquisa foi a bibliográfica documental, utilizando-se de leis, revistas científicas, livros, doutrinas jurídicas ou multidisciplinares, para a elucidação do que está sendo proposto. O método utilizado foi o dedutivo, visto que parte de uma premissa geral e abrangente para uma mais específica, tendo em visto que os ataques criminosos cibernéticos abarcam um vasto quadro, todavia, relatório irá se concentrar nos crimes digitais praticados contra empresas. Em se tratando da análise dos dados, optou-se pela qualitativa, pois busca um olhar devidamente cirúrgico e mais criteriosos acerca do que está sendo proposto, trazendo uma elucidação mais objetiva a respeito do tema.

Diante deste pequeno esboço, a finalidade deste acervo é demonstrar que há um perigo iminente e de alta periculosidade em um futuro próximo. O caminho que a humanidade está percorrendo no tocante ao processo digital e tecnológico é irreversível, de modo que precisamos nos adequar e tentar criar métodos mais precisos para garantir a seguridade da sociedade.

Para compreender o mundo virtual iniciou-se a discussão demonstrando como está intrinsecamente ligado ao convívio social das pessoas e das instituições, entretanto nem tudo é benéfico, pois há algo muito crescente nesse ambiente virtual, os crimes cibernéticos. Em seguida, a bordagem segue analisando esses ilícitos que estão crescendo demasiadamente nos últimos tempos, de modo que este cenário está se tornando um grande problema de segurança, algo que os governos, instituições e companhias deverão se centrar nos próximos anos para tentar mitigar ao máximo os danos e prejuízos nesse novo contexto de ataques cibernéticos, compondo esta a aboragem final do tema.

O SURGIMENTO E DESENVOLVIMENTO DA INTERNET

O advento da internet foi um dos fenômenos mais revolucionários da humanidade, algo que surgiu relativamente há pouco tempo – pouco mais de três décadas – e que não apenas se adaptou e se espalhou pelo sistema global de serviços, como hoje constitui a principal ferramenta de conexão entre os indivíduos da maioria das sociedades do mundo. O aparato tecnológico que desde meados do século passado apresentou uma constante, rápida e expressiva expansão ajudou definitivamente na consolidação desse meio digital (internet).

Não há consenso acerca de sua data exata de criação, visto que os Estados Unidos – principal fiador das pesquisas precursoras que levaram ao surgimento da internet como a conhecemos hoje – fez pesados investimentos através de seus órgãos institucionais a partir da década de 1960 com o intento de criar uma rede sólida e infalível de computadores, além do fato de já existir também projetos em parceria com países desenvolvidos (França, Inglaterra) nessa época para tal finalidade.

Acredita-se que o seu surgimento exato ocorreu em algum momento em meados da década de 1980, depois começou rapidamente a se espalhar, sendo que a partir da década de 1990 ocorreu um crescimento vertiginoso de seus serviços, o que consequentemente facilitou sua disseminação massiva. Hoje este instrumento está circunscrito no aspecto da vida moderna, sendo algo indissociável do cotidiano da maioria das pessoas, uma vez que está em praticamente todos os setores do cotidiano (trabalho, educação, relações interpessoais, viagens, negócios).

Uma de suas principais características é que a internet é uma ferramenta que não possui uma governança centralizada, isso foi decisivo para que vários serviços fossem acoplados para dentro de suas redes ao longo do tempo. Mensagens instantâneas, fóruns de discussão, redes sociais, tudo isso só foi possível por conta dessa maleabilidade.

A famosa World Wide Web (www) é o principal sistema de interligação de arquivos e dados da internet, um programa que foi criado pelo CERN (Organização Europeia para a Investigação Nuclear). Esse sistema auxilia a introdução, o carregamento e a compatibilização da maioria dos dados atualmente.

Estima-se que a acessibilidade da internet está introduzida em todos os continentes, sendo as áreas mais desenvolvidas (EUA, Europa, Japão, Coreia do Sul) os locais onde ocorre não apenas um maior uso, mas também um trabalho tecnológico muito mais aprimorado.

É de se esperar que os serviços desse meio sejam muito mais abundantes e disponíveis em países desenvolvidos – não apenas pelo óbvio fato de que são mais ricos e tem serviços públicos de qualidade melhores do que os subdesenvolvidos, mas também porque fazem investimentos muito mais pesados em ciência e tecnologia, além de estarem avançados na pesquisa de ponto como a robótico e nanotecnologia.

No contexto nacional, a internet foi introduzida no final da década de 1980, mais precisamente por uma parceria entre docentes e acadêmicos das universidades paulista e carioca com o mesmo intuito que foi introduzida pelas universidades americanas: construir

uma conexão entre rede de computadores e dados com a finalidade de conectar instituições. Pode-se dizer que esse foi um período de alvorecer, visto que foi nessa época em que os computadores começavam a ser comercializados e disponibilizados em uma escala maior, além do fato de terem se tornado uma ferramenta um pouco mais acessível.

A disseminação só ocorreu a partir dos anos 2000, nesse período a internet era na modalidade discada – isto é, conectada à linha de aparelho telefone – e o uso de computadores pessoais começou a se espalhar, apesar do fato de ser um país atrasado do ponto de vista tecnológico, o uso desses instrumentos foi sendo gradualmente introduzido até ganhar certa relevância, o que decididamente ajudou na consolidação desse meio virtual no país.

A inclusão digital basicamente foi conquistada atualmente, visto que mais de 80 % da população já possui acesso aos serviços de internet. O Brasil ainda não é um país de primeiro mundo, e do ponto de vista da tecnologia digital ainda precisa se desenvolver bastante (vide os países mais desenvolvidos), entretanto já possuímos sistemas de distribuição de serviços dessa seara, que se estende por todo o país. Através da disponibilização de fibras ópticas e da mais recente tecnologia 5G, pode-se afirmar cabalmente que essa é uma realidade que veio para todos, de modo que o único desafio para um futuro próximo é apenas aprimorar mais esse contexto para que ele possa alcançar ainda mais indivíduos.

A Internet e a Globalização

O trabalho manual sempre permeou a história da humanidade – grande parte dos trabalhos ainda são braçais ou manuais até os dias de hoje – e as relações de serviço e demanda na maior parte do tempo também seguiam essa lógica, entretanto isso mudou consideravelmente com o degringolar dos acontecimentos nos últimos duzentos anos.

A maior parte dos eventos históricos que trazem mudanças drásticas e rompimentos de paradigmas ocorre de maneira gradual ou paulatina, no tocante ao que foi dito no final do parágrafo anterior, o primeiro deles foi a Revolução Industrial, esse acontecimento decretou o fim do monopólio da manufatura nas relações trabalhistas e a introdução das máquinas no cenário social, político e econômico do mundo ocidental. Após isso, uma sucessão de eventos – sejam eles históricos ou políticos – contribuiu decisivamente para jogar a humanidade em uma reta de crescente desenvolvimento científico e tecnológico.

Um exemplo cirúrgico é o fato de que as guerras – que se olhadas de uma perspectiva estratégica – foram precisamente decisivas na evolução de ferramentas e aparatos com a finalidade de aprimorar ainda mais os setores científicos e de pesquisa dos países diretamente envolvidos em conflitos. A própria internet, como explicitado neste acervo anteriormente, foi germinada no período da Guerra Fria pelos EUA e seus aliados ocidentais.

É sabido que geralmente é o governo que financia (através de investimentos robustos e consideráveis) várias pesquisas e projetos de caráter científico, muitas das vezes assumindo o risco pelo empreendimento, visto que nem sempre se obtém o resultado desejável.

Diante disso, pode-se afirmar conclusivamente que o advento do mundo virtual não foi obra da aleatoriedade ou do acaso, muito menos um fato isolado ou um evento fortuito que ganhou projeções inesperadas, e sim uma ocorrência dentro de um ambiente totalmente propício para o surgimento de algo assim desse calibre.

Muitos estudiosos alegam que a globalização começou há muito tempo, mas precisamente no início das Grandes Navegações, momento em que as nações soberanas da Europa se lançaram em aventuras para desbravá-lo o território ultramarino. O resultado foi a descoberta do novo mundo (América) e o subsequente processo de colonização que perdurou por séculos, uma relação bilateral entre metrópole e colônia em que havia um constante fluxo de trocas. Esse fato foi o momento embrionário daquilo que seria o principal fenômeno que caracterizaria as relações não apenas entre estados e organizações, mas principalmente entre indivíduos.

As barreiras físicas propriamente ditas ainda existem, entretanto do ponto de vista de uma lógica comercial, cultural e economia, elas já há muito tempo superada. O mundo desfruta de uma economia sólida, robusta e abrangente (apesar das constantes crises periódicas), algo que nunca aconteceu na história humana, além da quase infinito disponibilidade de serviços e os meios de transporte (especialmente o aéreo) que podem fazer conexões entre cadeias de produção, produtos e pessoas ao redor de todo o globo em um tempo relativamente curto.

Essa mudança facilitou a inclusão de grupos que outrora eram completamente excluídos do processo produtivo em uma economia complexa e diversificada. As redes sociais também foram outra grande invenção do início deste século que engatilhavam a passos curtos, entretanto conseguiram conquistar um espaço poderosíssimo no meio social

– remodelando completamente as relações de interações pessoais. Essas ferramentas junto com a indústria cinematográfica são responsáveis pela diversificação cultural de hoje.

Um dado importante que precisa ser analisado é o fato de que quanto mais um produto é acessível, mais rentável e poderoso ele se torna, visto que sob esta visão, a quantidade é uma variável muito mais determinante para o sucesso de um produto do que propriamente outros fatores. Esse conceito pode ser perfeitamente aplicado com a internet, mas diante disso há uma pequena ressalva: só isso não explica a magnitude e o poder que essa ferramenta detém nos dias de hoje.

Raquel Recuero (2014), explica detalhadamente que o fenômeno virtual se tornou importante e indispensável pelo fato de podermos acompanhar tudo de perto, mesmo estando distante fisicamente, como uma eleição presidencial ou até desastres ambientais.

A recente pandemia é o exemplo mais cirúrgico da importância que o meio digital possui atualmente, além de explicitar a magnitude e a proporção desse instrumento na vida moderna da sociedade. O vírus invisível e microscópico obrigou a maioria das sociedades mundo afora a adotarem medidas restritivas (distanciamento social, home office, lockdown, fechamentos de estabelecimentos) com o intuito de conter uma disseminação que parecia completamente desenfreada.

Uma boa parte dos serviços tiveram que ser acoplados ao meio digital, uma vez que o trabalho físico estava comprometido – é claro que essa situação não foi geral, visto que grande parte dos trabalhos não são passíveis de serem transferidos para esta plataforma, especialmente em países pobres – em face do possível contágio.

Pode-se dizer que isso foi um verdadeiro experimento, uma vez que nunca antes algo assim tinha sido tentado em larga escala, o tipo de situação que só ocorre em decorrência do imponderável, que acordo com Nassim Taleb (2007) nada mais é do que um fato de força muitíssimo maior e inesperado, e seu relativo sucesso só foi possível graças a internet e seus meandros que não apenas foram os alicerces que sustentaram essa situação, mas também uma ferramenta que ainda pode alçar conquistas muito mais promissoras.

O CONTEXTO VIRTUAL E A INSEGURANÇA DA REDE

O processo informático se apoderou da estrutura de serviços do mundo contemporâneo, a evolução tecnológica é um fenômeno irreversível, de modo que a partir deste momento em diante, esse quadro só tende a se aprofundar ainda mais. Os

smartphones (celulares digitais) que foram introduzidos gradualmente no mercado de consumo no início da década passada, hoje são as ferramentas tecnológicas mais difundidas e acessíveis de nosso período moderno.

A relação entre organizações, grupos, Estados, entidades, comunidades e principalmente pessoas na atualidade segue uma lógica digital, em que o virtual está intimamente ligado ao convívio dos indivíduos, sendo um elemento que não pode mais ser dissociado de nosso meio.

O famoso autor e historiador israelense Yuval Noah Harari (2015), em seu best-seller internacional, Sapiens (2015), afirma que se vive uma terceira revolução industrial, e que ao contrário das últimas duas, esta é peculiar pelo fato de que independe da vontade humana, isto é, é um fenômeno imprevisível, em que os humanos podem obter inovações e conquistas que certamente podem trazer melhorias consideráveis para a vida coletiva, entretanto ninguém pode afirmar categoricamente para onde todo esse processo levará, sendo que esse futuro pode ser tanto algo benéfico como maléfico, visto que as mudanças estão ocorrendo em um ritmo acelerado e os seus efeitos, no médio e longo prazo, ainda são difíceis de calcular.

Entretanto, não é válido dizer que todo esse conhecimento e evolução trouxeram apenas benesses, pois essa afirmação certamente é equivocada. Muitas foram as transformações que ocorreram no último século, especialmente nos últimos cinquenta anos, porém essa nova realidade tornou a coletividade muito mais vulnerável, e um exemplo cirúrgico de nosso contexto virtual são os ataques cibernéticos, que já configuram um grande problema de segurança para a sociedade, e certamente será o principal desafio que as autoridades e a política deverão se encarregar nas próximas décadas para resguardar a integridade e a proteção de indivíduos e organizações.

O Cibercrime

A área digital está intrinsecamente inserida ao grandes centros e localidades. A necessidade de acoplar e organizar dados, o próprio processo de automação que já substituiu o físico em muitas esferas, a busca por mão de obra para preencher e desempenhar atividades que estão surgindo em face do cenário em constante mudança, além do próprio modelo do ambiente empresarial que transferiu sua operacionalidade para este novo meio. Esses e outros fatores ajudam a explicar a importância vital que a seara

virtual adquiriu na funcionalidade e operação trabalhistas no mundo de hoje; todavia, o crime organizado também se adaptou com essas novas mudanças.

Grande parte dos crimes cibernéticos podem ser divididos em dois tipos: aqueles que visam atacar computadores específicos, que muitas das vezes envolvem vírus e outros tipos de malware e aqueles que usam computadores para cometer outros crimes. A finalidade do ataque aos computadores propriamente ditos é impedir o usuário de usar o seu próprio dispositivo ou que um uma empresa tenha seu sistema de software comprometido e não consiga realizar ou prestar os seus serviços para seus clientes.

Com isso, surgiu um novo tipo de criminalidade, em que seus meios não envolvem violência física como os crimes comuns, porém possuem um vasto alcance e podem causar grandes prejuízos, que são os crimes cibernéticos.

O ataque é um fenômeno que basicamente sempre existiu, desde o surgimento e a propagação em larga escala da internet. Pessoas físicas eram (e ainda são), majoritariamente, as principais vítimas, visto que são notoriamente os alvos mais vulneráveis. As empresas, também, vêm constantemente sendo atacadas, devido o grande retorno econômico que pode advir desta prática ilícita. Ao longo da última década, essa atividade criminosa foi aperfeiçoada, especialmente em face da importância que os meios tecnológico, digitais e de comunicação ganharam na conjuntura social.

Sabrina Brito e Marco DeMello (2021), afirmam que há uma grande vulnerabilidade de nossos sistemas de defesa diante da magnitude e precisão dos ataques cibernéticos que estão sendo perpetrados nos dias de hoje, ou seja, isto nos torna “alvos fáceis”, uma vez que o ramo da segurança cibernética ainda é pouco abundante e ainda não existe uma demanda significativa por este tipo de serviço, o que em sua visão, é uma grande negligência.

Os tipos de investidas mais comuns, são os sequestros virtuais, em que os dados de uma empresa, grupo ou organização são retidos pelo invasor, uma vez retidos esses dados, o criminoso exige uma quantia (dinheiro) para devolvê-los de volta. De acordo com Brito e DeMello (2021), há uma estimativa de US$ 6 trilhões de dólares em prejuízos apenas nos Estados Unidos no passado, evidenciando, assim, que é um terreno substancialmente rentável para a atividade criminosa e bastante fértil.

O tipo de programa que ocasiona esse ataque malicioso é o Malware, uma abreviação de software malicioso, ele tem a finalidade de danificar e comprometer a estrutura e funcionamento de um computador ou dispositivo normal. O programa

secundário de malware aprimorada para ataques de extorsão é o ransomware, muito utilizado em ataques em massa.

Um exemplo cabal foi o ataque do ransomware WannaCry em maio de 2017, quando um malware explorou uma falha em computadores que utilizavam o Microsoft Windows, é estimado que no momento do ataque algo em torno de 230 mil computadores foram atacados em mais de 150 países, os usuários ficaram sem seus arquivos e receberam uma mensagem exigindo o pagamento de bitcoins para terem seus dados restituídos. Calcula-se que o ataque acarretou prejuízos no montante de US$ 4 bilhões ao redor do mundo.

Há vários tipos de ataques cibernéticos, como a fraude de identidades, quando documentos pessoais são roubados e usados contra a vontade de seus reais detentores, é um tipo de investida usado principalmente contra particulares, além de ser uma das modalidades prediletas de criminosos que atuam em grupos especializados de assalto e roubo. Todos os anos, especialmente nas grandes capitais, são registrados milhares de ocorrências de uso não autorizado de dados, roubos e furtos de documentos pessoais – principalmente cartões.

Um meio bastante engenhoso que os criminosos usam é o uso dos sites ‘’phishing’’, isso ocorre quando sites maliciosos se disfarçam de legítimos e usam as informações que obtém para fraudar dados e documentos, dado a falta de cuidado e instrução na hora do manejo de suas informações pessoais no território da internet, é uma maneira bastante fácil de cooptar indevidamente esses dados.

Há também a extorsão cibernética, que visa pedir uma recompensa para prevenir um ataque iminente, mais um dos muitos artifícios usados por hackers para extorquir dinheiro de pessoas físicas e jurídicas.

Já a Cryptojacking é uma atividade mais recente, que se envereda pelo sistema de criptomoedas, em que hackers fazem uso e manejo desse dinheiro digital para praticar crimes. Existe também a espionagem cibernética, afinal é sempre importante ressaltar que esse tipo de ação (não necessariamente um ataque) geralmente é perpetrada por nações, em especial as grandes potências (EUA, Rússia, China, Europa Ocidental), visto que ocorre uma verdadeira guerra cibernética entre estes entes nos dias de hoje, pois a informação e os segredos de Estado são definitivamente uma moeda preciosíssima no mundo moderno.

Já a finalidade de usar computadores para cometer outras ilicitudes já é algo mais abrangente, pois o número de atividades ilícitas que são perpetradas no submundo da

internet para alcançar essa finalidade é muito maior. Violação de direitos autorais, venda de artigos ou objetos ilegais online, produção, venda ou incitação da pornografia infantil, apologia e incitação a crimes contra a vida, violência contra mulheres, xenofobia, intolerância religiosa, maus-tratos contra animais, grupos neonazistas e outras vertentes declaradamente racistas, tudo isto são alguns dos exemplos que podem ser citados para explicitar o tamanho da abrangência desses tipos de criminalidade neste setor.

A legislação Brasileira e o Combate aos Crimes Virtuais

O cenário no Brasil ainda é muito conturbado, por um lado o país tem uma legislação para lidar com a proteção e privacidade de dados pessoais, que é a LGPD (Lei Geral de Proteção de Dados Pessoais), que é a lei mais recente e atualizada, além de possuir outros dispositivos esparsos na Constituição Federal e no Código Penal.

A Lei Geral de Proteção de Dados Pessoais adentrou no ordenamento jurídico para garantir e assegurar a proteção de dados pessoais pelas empresas, sendo que outorgou a empresas alguns princípios para que possa garantir a segurança dos dados, princípios estes que são o da Confiabilidade, para garantir que as pessoas não sejam expostas a riscos; integridade, para garantir que os dados estão corretos e atualizados; e a disponibilidade, que garante que os dados estarão disponíveis para acesso, conforme diz Jorge Alexandre Fagundes (2020).

A popularmente denominada LGPD versa sobre a coleta de dados na internet de provedores e seus usuários, o principal pilar que define a lei é que essa coleta deve ser sempre feita com o consentimento do usuário, além de ter como objetivo a função de resguardar as informações pessoais do indivíduo, para que elas não sejam utilizadas por terceiros e para finalidades diversas sem o consentimento do usuário.

A LGPD busca gerenciar os riscos e falhas para que os responsáveis pelo gerenciamento de banco de dados pessoais elaborem regras para a gestão, cumprindo medidas de segurança e notificar imediatamente a ANPD (Autoridade Nacional de Proteção de Dados) e as pessoas diretamente envolvidas (BARBOSA, 2020).

A fiscalização ficará sob responsabilidade da Autoridade Nacional de Proteção de Dados (ANPD). O órgão federal é responsável por implantar e fiscalizar se as empresas estão cumprindo os protocolos de segurança da LGPD, desse modo, o órgão também fica com a responsabilidade de editar regulamentos e procedimentos que serão adotados em processamento de dados.

Há também regras específicas para garantir a privacidade dos titulares dos dados, e ainda o artigo 52 da lei, asseguram multas de até 2% da renda da pessoa jurídica, estabelecendo um teto máximo de até 50 milhões de reais por infração (SANTOS, 2020).

A figura do Marco Civil da Internet, Lei n° 12.965/2014, que de uma maneira mais esparsa, tentou fazer da internet um ambiente menos desgovernado, uma lei que foi elaborada através de um debate virtual com participação popular, aborda questões como retenção de dados, a função social da internet, liberdade de expressão e responsabilidade civil de provedores.

Entretanto também é importante frisar que o ambiente virtual brasileiro ainda é muito conturbado, em face dos novos problemas que surgem e da maneira como lidamos com eles, de modo que é necessário um empenho maior, não apenas do governo em tentar não necessariamente regular, mas adequar para conferir uma proteção maior aos seus cidadãos, elaborando esse quadro juntamente com os indivíduos e companhias.

A ideia do Marco Civil surgiu a partir da concepção do professor Ronaldo Lemos, expressa em artigo publicado em 22 de maio de 2007. No primeiro semestre de 2008, o professor da Faculdade de Comunicação da UFBA André Lemos e o sociólogo e então professor da Fundação Cásper Líbero Sérgio Amadeu iniciaram um abaixo-assinado que foi circulado dentro das redes de pesquisadores de cibercultura (ABCiber). Segundo Amadeu, a ideia inicial era expressar para o Senado a opinião dos intelectuais. Então o ativista e publicitário João Caribé criou uma petição online, que atingiu 100 mil assinaturas em menos de um mês, consolidando assim, a ideia do Marco Civil da Internet.

No aspecto da legislação penal houve uma alteração recente com a introdução da Lei 14.155/2021, que majora as penas das atividades criminosas cibernéticas, visto que antes as penas não apenas eram brandas, mas quase sempre eram substituídas por medidas alternativas. “A atual orientação jurisprudencial acaba por estabelecer o império da impunidade em relação a essas fraudes, com grave prejuízo à administração da justiça e à sociedade em geral” (CUNHA, 2021).

A legislação facilitava a prática de crimes desse calibre, visto que a impunidade era certa para com os criminosos. Crimes como furto qualificado e estelionato tiveram uma majoração em suas penas, retirando-se o aspecto da detenção e incluindo a reclusão, além da imputação de multa.

O Brasil era o terceiro país mais afetado por ataques de invasões cibernéticas, era visível e notória a explosão acentuada e absurda de casos, de modo que essa alteração foi constituída com o intento de frear, ainda que de maneira paliativa, esse cenário.

MEDIDAS PARA CONTROLAR OS CRIMES CIBERNÉTICOS

O fim das senhas ou códigos de entrada e o uso ainda mais recorrente de sistemas de dupla identificação e reconhecimento digital, especialmente em softwares de bancos de dados, e-mails, redes sociais podem ser apontadas como um fator de risco que tem contribuído para com um cenário cada vez mais comum de invasões cibernéticas, visto que por ser aparentemente um modelo mais seguro e acessível para os usuários, ainda deixa muitas brechas para ataques.

Um fator que também precisa ser ressaltado é a questão crescente dos robôs de inteligência artificial, eles comprometem o funcionamento normal e adequado de páginas, sites e fóruns, além de serem também uma arma que pode ser usado para a realização de ataques a pessoas ou a grupos e em campanhas de difamação e desinformação, sendo esta última um caso que tem ganhado enorme projeção ultimamente, uma vez o uso desses ataques podem decidir ou comprometer o resultado de uma campanha eleitoral.

Embora o Brasil tenha leis específicas para combater o cibercrime, em muitos casos os criminosos ficam impunes porque determinados comportamentos são imprevistos e esses comportamentos trazem lacunas e explicações que são questionáveis (SANCHES; ANGELO, 2018).

A carência de recursos público para o também é um grande fator que prejudica ao combate aos cibercrimes.

De acordo com Silva, Barreto e Kufa, (2020, p.72), o poder público não está apto para reconhecer a potencialidade delitiva sob o aspecto das novas tecnologias. Uma vez, que a resposta dada pelo aparato policial e judicial está muito aquém do necessário para uma repressão adequada. Isso acaba dificultando a repressão que merece, pois os crimes virtuais são difíceis de distinguir e os recursos disponíveis são escassos.

A falta de qualificação técnica, também se torna um dos fatores primordiais para o grande aumente de ciberataques, já que os sistemas são falhos, e sucessível a ataques e nas investigações, é necessário demonstrar o crime cibernético que se dar por meio da qualificação técnica específica dos profissionais responsáveis, já que a verificação dos

vestígios deixados pelo crime virtual nem sempre estão presentes no local onde o crime foi cometido (BORTOT, 2017, p.20).

Conclui-se que na visão dos gestores e políticos, esses ataques devem ser enxergados como terrorismo – apesar de não existir entre as nações um consenso sobre quais tipos de ataques deveriam ser classificados como terrorismo -, uma vez que as fronteiras entre o dito "ciberespaço" são totalmente inconclusivas. Mas, um ponto que precisa ser dito é que, com certeza, esse debate fluíra ainda mais, tendo em vista o atual contexto, pois assim como a maioria dos problemas, as soluções apenas começam a ser discutidas e concretizadas quando o cenário se agrava.

CONSIDERAÇÕES FINAIS

A segurança cibernética é um instrumento que se faz cada vez mais necessário nos dias de hoje, é algo que de fato fará uma enorme diferença no bem-estar de nossas sociedades em um futuro não tão longínquo assim. Apesar de toda essa importância, ainda é um assunto muito negligenciado, e isso ocorre por diversos fatores, seja porque não há uma visibilidade maior do assunto, seja pelo fato que muitos ainda não se atentaram para a importância que de fato esse tema possui.

Foi explicitado categoricamente neste acervo que os crimes e atividades ilícitas relacionadas ao mundo cibernético não apenas aumentaram consideravelmente nos últimos tempos, mas que irão se tornar o grande foco de criminalidade ainda neste século, uma vez que a coletividade caminha irreversivelmente para o caminho da conexão digital.

O ciberespaço é um território muito amplo, não podendo se fazer uma mensuração devida dele, de modo que é quase impossível exercer um controle sobre este meio, isso não necessariamente é um dilema, mas sim um ponto que precisa ser ressaltado.

O governo deverá, de um modo ou de outro, criar instrumentos de freios e contrapesos com o intuito de neutralizar os aspectos nocivos que permeiam este mundo (crimes, discursos de ódio, invasões, prejuízos econômicos e materiais).

As companhias, principais personagens desse cenário virtual, deverão investir e contribuir no desenvolvimento de uma segurança cibernética mais aprimorada, visto que suas operacionalidades dependem cada vez dos circuitos virtuais de internet.

REFERÊNCIAS

BAPTISTA, Rodrigo. **Lei com penas mais duras contra crimes cibernéticos é sancionada.** Senado, 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contra-crimes-ciberneticos-e-sancionada. Acesso em: 19 de maio de 2022.

BARBOSA, Mateus Israel Alves Cruvinel. A evolução dos crimes cibernéticos e os desafios no combate. Pontifícia Universidade Católica de Goiás, Goiânia, Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/105, 10, 2020.

BORTOT, Jessica Fagundes. Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. **VirtuaJus**, Belo Horizonte, v. 2, n. 2, p.338-362, 1º sem. 2017. ISSN - 1678-3425.

BRITO, Sabrina**.** Marco DeMello: "Estamos na mira dos hackers". **VEJA,** 2021. Disponível em: < https://veja.abril.com.br/tecnologia/marco-demello-estamos-na-mira-dos-hackers/ > Acesso em: 06 de maio de 2022.

DECLOEDT, Cynthia. Ataques cibernéticos com pedidos de resgate atingem pico em outubro. **ESTADÃO**, 2021. Disponível em: < https://economia.estadao.com.br/blogs/coluna-do-broad/ataques-ciberneticos-com-pedidos-de-resgate-atingem-pico-em-outubro/ > Acesso em: 18 nov. 2021.

Escola de Magistrados da Justiça Federal da 3° Região. **Investigação e prova nos crimes cibernéticos.** São Paulo. TRF3, 2017. Disponível em <https://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf> Acesso em: 26 nov. 2021.

FAGUNDES, Jorge Alexandre. **Lei geral de proteção de dados 13.709/18 (LGPD)** está em vigor, e determina que as empresas realizem a adequação. Jus.com.br, 2020. Disponível em: https://jus.com.br/artigos/86423/lei-geral-de-protecao-de-dados-13-709-18-lgpd-esta-em-vigor-e-determina-que-as-empresas-realizem-a-adequacao. Acesso em: 13 de maio de 2022.

HARARI, Yuval Noah. **Sapiens – Uma Breve História da Humanidade.** 1° Edição. Brasil: L&PM, 2 de março de 2015.

HARARI, Yuval Noah. **Homo Deus:** Uma Breve História do Amanhã. 1° Edição. Brasil: Companhia das Letras, 11 de novembro de 2016.

MIRANDA, Vitor. **Crimes Cibernéticos**. Pág. 2,3,5 e 6. 2021. Disponível em < https://docero.com.br/doc/e8nse5n > Acesso em: 06 maio 2022.

SÃO PAULO. Policia Civil SP. **Delitos praticados por meios eletrônicos.** Pág. 4,7 e 9. 2021. Disponível em <https://www.policiacivil.sp.gov.br/portal/imagens/CRIMES%20CIBERN%C3%89TICOS%20-%20PERGUNTAS%20E%20RESPOSTAS%20V2.pdf > Acesso em: 01 de maio. 2022.

RECUERO, Raquel. **Título: Redes Sociais na Internet**. 2° Edição. Brasil: Editora Sulina, 1 de janeiro de 2014.

SANCHES, Ademir Gasques; ANGELO, Ana Elisa. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil**. Disponível em: <https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil/1>. Acesso em: 17 de maio 2022.

SANTOS, Natacha Armstrong. LGPD: Lei geral de proteção de dados pessoais e seus reflexos empresariais. **EVINCI - UniBrasil**, Curitiba, v.5, n.1, p. 142, out. 2019.

SENADOR RODRIGO CUNHA. Senado aprova PL que aumenta as punições para fraudeseletrônicas 2021. Disponivel em:https://www.migalhas.com.br/quentes/345082/senado-aprova-pl-que-aumenta-as-punicoes-para-fraudes-eletronicas.

SILVA, Marcelo Mesquita; BARRETO, Alesandro Gonçalves; KUFA, Karina. **Cibercrimes e seus reflexos no direito brasileiro.** 1ª ed. 2ºtir. Fev/2020 Salvador: Editora JusPODIVM. 2020.

TALEB, Nassim Nicholas. **A lógica do cisne negro**. 19° Edição. Brasil: Best Seller, 16 de julho de 2008.