***RANSOMWARE* E CIBERCRIMINOLOGIA:** Desafios criminológicos que se descortinam no século XXI, ainda em movimento

Avante
REVISTA ACADÊMICA DA POLÍCIA CIVIL DE MINAS GERAIS

Frederico Henrique Moreira Nascimento
https://lattes.cnpq.br/7212267097642182 - https://orcid.org/0009-0006-9358-6793
fredericonascimento013@gmail.com
Polícia Civil de Minas Gerais – PCMG, Belo Horizonte, MG, Brasil

RESUMO
Ransomware é uma técnica criminal que vem ganhando cada vez mais espaço no mundo digitalizado e dependente economicamente da informação e da informática. Diversos são os casos globalmente conhecidos que causaram consequências devastadoras a empresas, nações e indivíduos. Assim, este trabalho aborda o tema a partir dos óculos da Criminologia e especificamente da Cibercriminologia, com o intuito de demonstrar o grau de complexidade do fenômeno e o quanto isso impacta o estudo do crime e as limitações explicativas das teorias criminológicas, bem como a capacidade de elas serem aplicadas no entendimento do fenômeno. A metodologia utilizada foi a revisão transdisciplinar da bibliografia, que trata dos temas da Segurança da Informação, Criminologia e Direito. O alto grau de complexidade do fenômeno trabalhado impõe sérias dificuldades àqueles que se dedicam a compreender as questões criminais. Por isso, defende-se a integração dos conhecimentos da Informática e da Criminologia para melhor se adequar a um dos principais crimes de informação da atualidade, o *ransomware*. Concluiu-se que as teorias criminológicas convencionais podem explicar essa forma de criminalidade com algumas restrições. Para tanto, as Teorias da Transição Espacial, no âmbito da Cibercriminologia, e as da Desinibição *On-line*, no cenário da Psicologia, são capazes de preencher tais lacunas e responder adequadamente às discutidas limitações.

Palavras-chave: Cibercriminologia; *Ransomware;* Crimes Cibernéticos; Controle Social; Perfil Criminal.

RANSOMWARE AND CYBERCRIMINOLOGY: Criminological challenges that emerge in the 21st century, still in motion

ABSTRACT
Ransomware is a criminal technique that is gaining more and more space in the digitalized world that is economically dependent on information and computing. There are several globally known cases that have caused devastating consequences for companies, nations and individuals. Thus, this work approaches the topic from the perspective of Criminology and specifically Cybercriminology. In order to demonstrate the degree of complexity of the phenomenon and how much this impacts the study of crime, the explanatory limitations of criminological theories, as well as their ability to be applied to understanding the phenomenon. The methodology used was the transdisciplinary review of the bibliography that deals with the topics of Information Security, Criminology and Law. The high degree of complexity of the phenomenon discussed imposes serious difficulties on those who dedicate themselves to understanding criminal issues. Therefore, we advocate the integration of IT and Criminology knowledge to better adapt to one of today's main information crimes, ransomware. The results were that conventional criminological theories can explain this form of crime with some restrictions. To this end, the Theories of Spatial Transition, within the scope of Cybercriminology, and Online Disinhibition, within the context of Psychology, are capable of filling such gaps and adequately responding to the discussed limitations.

Keywords: Cybercriminology; Ransomware; Cybercrimes; Social Control; Criminal Profile.

DOI: https://doi.org/10.70365/2764-0779.2024.94

Recebido em: 02/09/2024.
Aceito em: 09/10/2024.

1 INTRODUÇÃO

Ransomware é a conduta de algum cibercriminoso que visa obter acesso indevido a dispositivos informáticos, mormente redes de computadores contendo dados corporativos, e, com isso, por meio de criptografia dos dados digitais, impedir o acesso do legítimo proprietário aos seus recursos informáticos. A particularidade dessa conduta criminosa é que, para liberar o acesso novamente aos dados, o extorsionário exige do lesado pagamento de valores financeiros, normalmente em criptomoedas (Liska; Gallo, 2017; Pimentel; Cabrera; Forte, 2021; Ditz; Minetti, 2023).

O fenômeno em tela também é conhe*cido* como sequestro digital, sequestro de dados ou extorsão criptográfica. Segundo Ditz e Minetti (2023), um dos primeiros casos conhecidos data do ano de 2005, mas, foi a partir de 2008, com o advento da moeda digital *Bitcoin*, que os sequestros digitais se alastraram de maneira mais contundente pelo mundo, dada a dificuldade em se rastrear o uso de tal moeda, o que passou a causar danos econômicos e políticos cada vez mais severos. Tal situação, portanto, exige trazer esse tema para as discussões criminológicas e esclarecer os impactos dessa nova forma de criminalidade para as ciências que se dedicam ao estudo do crime.

Com base nisso, erigiu-se o seguinte problema central: "como a digitalização socioeconômica, já desenvolvida no século XXI, e o surgimento das práticas de sequestro digital (*ransomware*) fomentam novos desafios para a Criminologia?", tendo em vista a hipótese de que o advento massivo da digitalização e dos sequestros digitais impõem significativas limitações explicativas e interpretativas às teorias criminológicas já estabelecidas, uma vez que o fenômeno sociotécnico aqui em evidência impacta, de forma direta, a desenvoltura de condutas desviantes disruptivas e não previstas pela Criminologia tradicional.

Diante disso, sob a perspectiva da Cibercriminologia de Jaishankar (2007), o objetivo geral estabelecido é confrontar o advento dos sequestros digitais (*ransomware*) com os objetos de análise da Criminologia (o crime, o criminoso, o controle social e a vítima) e seus pilares teóricos. Além disso, os objetivos específicos se constituem em abordar o sequestro digital (*ransomware*), apontando e elencando as dificuldades que as teorias criminológicas enfrentam quando aplicadas no entendimento e na explicação dos sequestros digitais; e demonstrar a Cibercriminologia como saber específico capaz de preencher satisfatoriamente as lacunas interpretativas da Criminologia quanto às especificidades do *ransomware*.

A metodologia utilizada neste texto adotou revisão interdisciplinar. A linha de pesquisa seguiu os princípios da Cibercriminologia, conforme preconizado por autores como Jaishankar (2007) e Arroyo (2020), que enfatizam a necessidade de uma análise criminológica especializada para compreender os crimes cibernéticos, dadas as complexidades do ciberespaço. Além disso, foram incorporados elementos da Segurança da Informação, conforme discutido por Pimentel, Cabrera e Forte (2021) e Liska e Gallo (2017), para entender aspectos técnicos do *ransomware*. Os desdobramentos da pesquisa também contemplaram abordagens da Criminologia tradicional e da Psicologia, à luz das teorias da Transição Espacial e da Desinibição *On-line*, conforme apontado por Lucena (2012) e Llinares (2012). A análise transdisciplinar, a integração de conhecimentos da informática e da tecnologia da informação e as discussões sobre a globalização e a criminalidade foram alinhadas com as propostas de Jaishankar (2007) e Carrapiço (2005). Essa abordagem metodológica permitiu uma análise abrangente do *ransomware*, considerando seus aspectos criminológicos, técnicos, jurídicos, econômicos e sociais a fim de responder ao problema central do texto.

O tema se justifica na medida em que o *ransomware* se apresenta como uma das maiores ameaças à segurança da informação e, portanto, à integridade física e patrimonial das empresas e pessoas, além de se configurar como uma grave ameaça também à privacidade. Ademais, ele ganha relevância ainda por ter como um dos seus efeitos a restrição ou bloqueio a bens e serviços, muitos deles essenciais ao próprio exercício da cidadania – sobretudo quando ataca dados oriundos de instituições públicas governamentais.

Importante também é o fato de que o fenômeno possibilita ganhos extraordinários aos delinquentes cibernéticos. Isso porque não permite às vítimas muitas escolhas, a não ser pagar pela extorsão; uma vez que os dados são, na maioria das vezes, essenciais à sobrevivência de uma empresa, tendo o mesmo valor que o próprio dinheiro. Assim, o sequestro digital não só prejudica gravemente as corporações, como pode ocasionar diversos riscos sociais: desde impedir o tráfego de veículos, aeronaves, embarcações marítimas até a fustigação do fornecimento de água, energia, alimentos e combustíveis.

Outro ponto a se pôr em evidência é o uso de anonimato por meio das criptomoedas usadas na chantagem e na extorsão contra as vítimas, dificultando sobremaneira a persecução penal. Ainda se pode apontar a falta de estudos criminológicos abordando o tema em riste, o que deixa uma lacuna altamente relevante para que se construam meios de controle social formal e

informal. Além disso, estudos nessa área podem abrir caminhos para a discussão de políticas públicas a fim de minorar o avanço desse tipo de criminalidade.

2 FUNDAMENTAÇÃO TEÓRICA E ENQUADRAMENTO DO *RANSOMWARE*

Como referencial teórico, expõe-se que, primeiramente a partir da literatura jurídica, autores como Vianna e Machado (2013) traçam os crimes cibernéticos em dois vieses. O primeiro é conhecido como crime cibernético próprio, em que a conduta delinquencial atenta diretamente contra os sistemas informáticos, enquanto, num segundo plano, os impróprios são aqueles crimes que já existem sem os meios informáticos, mas tão somente se valendo deles para a sua consecução. Nesse sentido, o *ransomware* é a conduta de alguém invadir um sistema informático remotamente e, por meio de criptografia, tornar indisponíveis os recursos informáticos da vítima, exigindo dela, para o restabelecimento da disponibilidade dos seus dados, o pagamento normalmente feito em criptomoedas (Liska; Gallo, 2017).

Discussão importante levantada é a natureza jurídica do *ransomware* e a possibilidade de enquadramento dessa conduta no ordenamento jurídico brasileiro, especificamente no Código Penal. Apesar de ser conhecida como sequestro de dados, a conduta se encaixa no crime de extorsão e não no de extorsão mediante sequestro, persistindo a problemática de se a conduta é equivalente ao crime de invasão de dispositivo[1] (Gomes; Nunes; Wilmers, 2020).

Já criminólogos, especialmente os que se dedicam à Cibercriminologia, Arroyo (2020), Llinares (2012), Lucena (2012), Favero e Favero (2021) e Gama (2021), apontam para uma maior complexidade que vai muito além das definições jurídicas, delineando a cibercriminalidade a partir das motivações políticas, econômicas e sociais (relações interpessoais) dentro de um contexto histórico, técnico, econômico e cultural próprio.

Para essa corrente, existe uma clara dificuldade das teorias criminológicas tradicionais em explicar, de maneira profícua, o fenômeno em riste. Em decorrência disso, surgiram as teorias da Transição Espacial, no âmbito da Cibercriminologia, e a teoria da Desinibição *On-line*, no âmbito da Psicologia. Ponto muito caro aqui é a tentativa de trazer à tona a construção de um perfil criminológico do desviante digital e as inerentes dificuldades dessa empreitada (Lucena, 2012; Arroyo, 2020; Gama, 2021).

Tendo em mente o avanço abrupto dos crimes informáticos, Jaishankar (2007) fundou a Cibercriminologia, preocupando-se em não a separar da

[1] Crime de Invasão de Dispositivo, tipificado no artigo 154-A do Código Penal Brasileiro.

Criminologia ao criar conceitualmente uma criminologia especializada. Jaishankar (2007) justifica tal necessidade de especialização criminológica ao constatar que os postulados da Criminologia convencional serviriam muito pouco a uma análise mais aprofundada dos crimes cibernéticos, visto que estes trazem desafios específicos relacionados a um novo ambiente: o ciberespaço.

Para o mesmo autor, ao falar de cibercrime, uma abordagem satisfatória do crime, do criminoso, da vítima e do controle social só é possível quando se integra de maneira multidisciplinar os conhecimentos da Criminologia e da Informática, formatando, desse modo, o método da Cibercriminologia. Obviamente, tal abordagem não rompe com a Criminologia, mas sim identifica as limitações das teorias estabelecidas e propõe adicionar os conhecimentos da informática a uma nova capacidade analítica do método empírico, interdisciplinar e indutivo da Criminologia.

Empiricamente, a Cibercriminologia identifica o ciberespaço como uma fronteira que se impõe de maneira fática às diversas disciplinas que se dedicam ao fenômeno criminal, configurando, desse modo, uma demanda metodológica e acadêmica por entendimentos mais aprofundados a respeito do crime digital (Jaishankar, 2007). Como explicam Favero e Favero (2021), é uma abordagem sociológica da utilização violenta e/ou criminosa das tecnologias informáticas. Com isso, o estudo criminológico se baseia em como os meios cibernéticos influenciam e são influenciados ao mesmo tempo no crime, na vítima, no criminoso e nos controles sociais.

É nesse método da Cibercriminologia que Lucena (2012), Arroyo (2020), Llinares (2012) e Luna e Labrin (2017) demonstram que o novo espaço de criminalidade, a internet, permite o surgimento de condutas desviantes inovadoras e novos perfis criminais – orientados à tecnologia, que transitam assimetricamente entre o mundo *on-line* e *off-line*. A Cibercriminologia é uma subárea da Criminologia que busca estudar os objetos de análise do fenômeno criminal a partir dos meios tecnológicos que o caracterizam como *locus* contínuo de desvios e vitimizações. Isso a partir de visões críticas das tentativas de caracterização de perfis criminais e do impacto da digitalização para as relações sociais (Jaishankar, 2007).

Já em outra seara, a abordagem da literatura do campo da Segurança da Informação, apresentada em Pimentel, Cabrera e Forte (2021), Liska e Gallo (2017), a respeito do *ransomware*, foca nos aspectos técnicos da criptografia ou do bloqueio de dados. Ademais, ela busca demonstrar a evolução desse tipo de crime em correlação com o próprio desenvolvimento computacional, assim como objetiva traçar aspectos operacionais-corporativos para evitar ou

responder a um ataque desse tipo. Cerca-se, além disso, o uso de criptomoedas (baseada na tecnologia *blockchain*) como forma de anonimato dos extorsionários e uma das características mais marcantes desse tipo de crime.

Em mais um campo de análise, aborda-se o aspecto econômico-valorativo da informação por autores como Goodman (2015), Glenny (2011) e Bisso et al (2019), isto é, a informação como principal ativo do sistema econômico e a dependência cada vez mais acentuada da sociedade em geral dos dados e da tecnologia informática, e o quanto isso afeta o fator criminal atualmente.

Aqui também se enquadra a literatura que caracteriza esse fenômeno sociotécnico a partir de uma relação de desigualdade entre o criminoso cibernético e a vítima, no sentido de que esta quase sempre possui menos conhecimento da própria tecnologia que usa do que aquele (Lucena, 2012; Kunrath, 2014). Mais ainda: a vítima, sob essa perspectiva, tem experimentado uma revolução tecnológica e todos os seus benefícios, sem, no entanto, possuir consciência adequada dos riscos que envolvem a rede mundial de computadores (Clarke; Knake, 2015; Henriques, 2016).

Há ainda a abordagem que confronta globalização e criminalidade, sobretudo o novo tipo de globalização fomentado pela internet e suas tecnologias e como elas modificam sobremaneira a configuração da ordem mundial, e, assim, excitam crimes que se valem da Nova Economia dos dados e da ubiquidade, transformando não só as estruturas sociais, econômicas e políticas, mas também a criminalidade de caráter transnacional (Carrapiço, 2005). Além disso, a literatura demonstra como uma das principais ferramentas do Estado Moderno, a territorialidade, possui nenhuma ou pouca relevância na prevenção ou repressão à criminalidade cibernética (Santos, 2014; Gama, 2021; Luna; Labrin, 2017).

Inicialmente, abordar-se-á o tema quanto à possibilidade de compreensões devidamente aprofundadas e ancoradas nos postulados da Criminologia, conforme o tópico a seguir.

2.1 Criminologia e Ciberdelinquência: limitações e possibilidades de entendimento

Para Llinares (2012), existem debates doutrinários quanto ao fato de o cibercrime ser algo totalmente novo. Nesse caso, as teorias criminológicas não seriam capazes de explicar sua essência ou se o fenômeno criminal em tela é tão somente um tipo especial de delitos, e, dessa maneira, é estruturalmente igual aos crimes e às condutas do meio físico tradicional. No meio disso, aponta-

se uma posição intermediária, defendida pelo referido autor, de que o cibercrime compartilha de todos os elementos definidores do conceito de crime. Todavia, tal teoria trabalha o delito informático com suas novas peculiaridades originadas do meio cibernético, e, portanto, suas explicações, prevenção e repressão são diretamente influenciadas pelo próprio meio em que o cibercrime ocorre.

O estudo da Cibercriminologia, ramo específico da própria Criminologia, tem sua origem, segundo Arroyo (2020), em Jaishankar (2007), o qual cunhou, pela primeira vez, o termo em riste. Para Arroyo (2020), a Cibercriminologia estuda as condutas desviantes e os crimes não só a partir do meio em que elas ocorrem, mas também busca delinear aspectos do perfil do delinquente cibernético, das vítimas e, ainda, busca categorizar as diferentes condutas a partir de um meio sociotécnico.

A Criminologia, tanto a nível empírico quanto teórico, tardiamente se debruçou sobre as influências que as tecnologias emergentes produziram na sociedade e no fator criminal. Como resultado disso, grande parte dos trabalhos nesse campo de estudo tem partido das teorias tradicionais conhecidas como totais ou gerais, em que se acredita que elas possam ser capazes de explicar a origem de todos os fenômenos criminais (Arroyo, 2020). Dentro desse aparato, a Cibercriminologia surge como área de pesquisa necessária ao aplicar conhecimentos da Ciência da Computação e da Criminologia, conjuntamente com o objetivo de explicar e analisar os crimes que se desenvolvem por meio da Rede Mundial de Computadores (Jaishankar, 2007).

Nessa esteira, para Vianna e Machado (2013, p. 37 e 38), a Teoria da Associação Diferencial, criada por Sutherland para explicar os crimes de colarinho branco, e, além disso, analisar como a conduta criminal é resultante de processos de aprendizagem em contextos de associações diferenciais, adapta-se eficazmente ao criminoso informático. Dado que, especialmente esse tipo de crime, mais do que qualquer outro, necessita ser aprendido antes de ser posto em prática. Esse aprendizado se dá pelo contato do criminoso com o meio cibernético, inundado de técnicas criminais facilmente encontráveis. Exemplo disso são os manuais dedicados a pedófilos na *Dark Web*, com vários ensinamentos (Moreira, 2019). Reforçando esse ponto, numa operação da Polícia Civil de Minas Gerais, um médico foi alvo de busca e apreensão, e, em seu computador, foi encontrado um manual para pedófilos,

com detalhes instrutórios sobre como encontrar crianças, como seduzi-las e outros ensinamentos[2].

Todavia, conforme asseveram os mesmos autores: o referido aprendizado supera a questão meramente técnica, para fazer com que o indivíduo seja influenciado por uma específica subcultura, que os autores caracterizam como *cyberpunk*. Subcultura essa que valoriza a capacidade do criminoso em cometer atos audazes, a exemplo de invasões de *sites* importantes dos governos, configurando, dessa forma, uma possibilidade de aplicação da Teoria da Subcultura, forjada por Cohen (1955), à criminalidade digital, que pode ser delineada a partir de valores e normas específicas de grupos ciberdelinquentes.

Então, pode-se dizer que há uma junção dessas duas teorias. Tendo em mente que, enquanto o criminoso aprende técnicas informáticas criminosas, ao mesmo tempo, passa a se identificar com valores e normas próprias de grupos cibernéticos desviantes. Portanto, é necessário mais do que o conhecimento técnico, pois este deve vir acompanhado de um contorno de subcultura de grupos informáticos criminosos que exercitam o desvio como valor, ou seja, o criminoso digital soma conhecimento técnico e identificação com valores desviantes (Vianna; Machado, 2013).

Para Gama (2021), existem similaridades entre o criminoso de colarinho branco, explicado pela Teoria da Associação Diferencial, e o criminoso informático, notadamente na dimensão de valores e motivações. Tendo em vista que, nos dois tipos citados, ambos os infratores podem se caracterizar pelo ânimo empreendedor, bem como pela utilização do recurso fraudulento, em contexto econômico e, geralmente, sem utilização de violência, é possível identificar similitudes entre o crime de colarinho branco e suas teorias explicativas e o cibercriminoso de caráter empreendedor.

Em uma percepção mais inovadora e específica, Lucena (2012) assevera que, com a emergência da internet, novos comportamentos e novas maneiras de relações sociais vieram à tona. Isso implica diretamente em condutas desviantes e/ou criminosas, demandando um entendimento específico do criminoso informático sob o prisma psicossocial, pois o desviante em questão se encontra em grupos com subculturas próprias.

Favero e Favero (2021) trazem, em seus estudos, uma teoria gestada dentro do método da Cibercriminologia, chamada Teoria da Transição Espacial. Nela são tratados os novos aspectos da tecnologia informática de

[2] Disponível em https://www.bbc.com/portuguese/brasil-47825687. Acesso em: 14 out.2024.

interconexão de redes e seus impactos na criminalidade. Segundo os autores citados, a teoria pressupõe que existe uma transição de condutas do ciberdelinquente frente às dinâmicas do mundo *off-line* e *on-line*. Esse conceito debate o ciberdelinquente como uma pessoa que, no mundo *off-line,* pode ser altamente conformista, mas que, no espaço *on-line*, é desviante, o que também vai ao encontro do que ensina Lucena (2012).

Uma das grandes limitações da Criminologia é que, tradicionalmente, ela vem buscando entender como os aspectos socioeconômicos de exclusão se configuram como forças motrizes para a delinquência. No entanto, esse aparato teórico vigente pouco ou nada se aplicaria ao criminoso informático, uma vez que se pressupõe que esse delinquente seja integrante de um grupo com características bem distintas do criminoso marginalizado convencional (Arroyo, 2020; Jaishankar, 2007).

Essa é uma categoria de desviantes até então bem pouco conhecida, pois o crime informático demanda dos seus autores conhecimentos técnicos que pressupõem um nível intelectual, pelo menos, razoável, uma vez que a ausência de conhecimentos específicos mínimos impede a participação do sujeito na cibercriminalidade. De maneira geral, trata-se de um indivíduo que não é tolhido dos produtos resultantes do sistema social e político em que vive (Arroyo, 2020).

Em conformidade com isso, Lucena (2012) esclarece que os sujeitos ativos desse tipo de criminalidade são, em geral, pessoas de bons relacionamentos com outros indivíduos no mundo *off-line*, surgindo das camadas médias e altas da sociedade e, portanto, não marginalizados[3] e com acesso à educação formal, renda, emprego e informação de qualidade. São sujeitos com grandes habilidades, conhecimentos informáticos e com níveis significativos de qualificação profissional. Gama (2021) caracteriza isso como a triangulação de competências profissionais, inteligência e criatividade.

Destaca-se ainda que a maioria desses indivíduos desviantes informáticos não são criminalmente versáteis, uma vez que praticam – via de regra – somente delitos no âmbito cibernético, corroborando a tese central da Teoria da Transição Espacial (Lucena, 2012). No entanto, Arroyo (2020) assinala que, em razão do próprio desenvolvimento massivo das tecnologias da informação, o cibercrime tem ficado cada vez mais acessível aos usuários comuns da internet, inclusive aqueles que possuem conhecimentos técnicos corriqueiros,

[3] Para Vianna e Machado (2013), a marginalização do criminoso informático ocorre na dimensão intelectual, devido a essa característica de possuir inteligência acima da média.

assim dificultando sobremaneira a construção de um perfil do criminoso informático.

Para esse mesmo autor, devido ao extremo dinamismo do mundo cibernético, um perfil rígido da ciberdelinquência é impossível diante da própria natureza técnica do fenômeno, existindo ainda a possibilidade de aqueles sujeitos desviantes com maior capacidade técnica (experientes desenvolvedores de códigos, por exemplo) abrirem janelas de oportunidade para os menos qualificados e inexperientes. Isso faz com que o perfil do criminoso digital seja significativamente heterogêneo frente às competências informáticas, o que leva, para as teorias criminológicas, uma importante problemática a ser enfrentada.

Nessa mesma esteira, Henriques (2016, p. 34) aponta que, antigamente (antes de a internet se transformar em *mass media*[4]), o crime cibernético era dado a poucos indivíduos e a grupos com elevada *expertise* informática, sobretudo aqueles com conhecimentos superiores em programação. Todavia, atualmente, é extremamente facilitado a qualquer pessoa com conhecimentos comuns de tecnologia angariar ferramentas maliciosas, aprender a explorar vulnerabilidades técnicas e humanas e a obter acesso não autorizado – e criminoso – a sistemas informáticos, com algumas horas ou dias de pesquisa e dedicação. Ainda dentro desse cenário, destaca-se o fato de que, enquanto os ataques cibernéticos têm ganhado maior complexidade e consequências devastadoras, o nível de conhecimento técnico para operacionalizá-los é cada vez menor.

Desse modo, pode-se caracterizar o ciberdelinquente além do conhecimento técnico, pois estudos empíricos clarificam que uma carreira cibercriminosa bem-sucedida exige ao indivíduo desviante espírito inovador e criativo. Soma-se a isso capacidades de criação de redes de ataques de alta tecnologia, como requisito fundamental de agentes criminosos atuantes no cibercrime organizado. Dessa maneira, esse criminoso deve ser capaz de reinventar-se frente aos desafios contextuais da contemporaneidade, o que quer dizer também adaptabilidade, assunção de riscos, foco no ganho financeiro e identificação de oportunidades (Gama, 2021).

Para Lucena (2012), o conceito de desinibição *on-line*, desenvolvido pelo psicólogo Jonh Suler, também se torna importante para entender a

[4] O termo significa mídias de comunicação de massa, isto é, aqueles meios de comunicação que visam atingir um número indeterminado e cada vez maior de pessoas. Cronologicamente, pode-se dizer que o primeiro desses meios foi o jornal (mídia escrita), passando pelo rádio e pela televisão, e finalmente chegando à internet (Miguel, 2001).

delinquência digital, pressupondo que as pessoas se sentem mais desinibidas para se comunicarem no meio cibernético, uma vez que a internet possibilita assincronismo, ubiquidade, anonimato e a inexistência de repressores sociais que só existem no mundo físico do indivíduo. Dessa maneira, o desviante cibernético estaria agindo a partir da inexistência dos controles sociais tradicionais, dado que a internet rompeu até mesmo com a eficácia desses controles, fazendo com que as pessoas tenham comportamentos distintos em ambos os espaços (Llinares 2012).

Ao conjugar os esforços analíticos de Lucena (2012), Llinares (2012), Gama (2021) e Arroyo (2020), pode-se depreender que a Transição Espacial está diretamente ligada aos efeitos materiais de mudança que as tecnologias informáticas produzem de maneira disruptiva, configurando um entorno de gênese criminal, sociologicamente compreendido. Por outro lado, a Desinibição *On-line* estaria mais ligada ao aspecto psicológico do indivíduo desviante, uma vez que a internet possibilitaria uma espécie de amplo anonimato e fantasia ao seu usuário, em que vítimas e autores não se tocam fisicamente, o que profundamente a percepção dos consumidores criminosos da rede em relação ao desvio e à conformidade social.

Arroyo (2020) explica que a Teoria da Transição Espacial identifica um indivíduo que sofre eficazmente os efeitos do controle social no espaço físico e, por outro lado, tem propensão para cometer crimes no espaço cibernético, que ele não cometeria no espaço *off-line*, muito devido a sua condição social. Um segundo fator seria que a flexibilidade de identidade dos meios digitais, junto ao anonimato, impediria mecanismos de dissuasão. Mais ainda: a dinâmica cibernética entre espaço e tempo favorece a capacidade do cibercriminoso de se evadir da aplicação da lei. Por conta disso, internet é uma tecnologia que favorece o recrutamento e o associativismo criminal, bem como a difusão de técnicas criminais. Além disso, o conflito entre as normas e valores do espaço físico com as normas e valores do ciberespaço podem ser causa geradora de delitos.

É preciso, todavia, chamar atenção no sentido de que a Teoria da Transição Espacial não propugna que haja uma ruptura entre os dois espaços tratados. O que se traz como cerne da questão é a capacidade de os indivíduos mudarem suas condutas quando estão em contato com a Rede Mundial de Computadores, podendo o criminoso informático valorar a conformidade em diversos setores de sua vida no mundo *off-line* e, ao mesmo tempo, praticar desvios e se identificar com valores desviantes no mundo *on-line*.

Arroyo (2020) traz que são inerentes à internet ameaças e riscos que podem se transformar em condutas criminais. Isso tudo a partir das características principais dessa tecnologia: alcance mundial da internet, desterritorialização, subcultura criminal no ciberespaço e possibilidade de interações remotas entre atacantes e vítimas. Para além disso, é possível citar ainda o custo financeiro e operacional mínimo de manipulação de dados e programas, automatização de condutas criminais via *softwares*, caráter exponencial do cibercrime (uma conduta pode atingir simultaneamente diversas vítimas), limitação estrutural dos controles sociais e ciclo de inovação de técnicas e procedimentos a serviço do crime, marcadamente disruptivo. Nesse contexto, a informação se transforma em um bem altamente valioso (tanto em mercados legais quanto ilegais).

Frente a essa questão, Clarke e Knake (2015) apresentam a internet como vocacionada a propagar facilmente tráfego malicioso, direcionado a invadir computadores e demais dispositivos. Isso ocorre, segundo os autores, justamente porque a internet não possui, no limite, ninguém para comandá-la e não há uma fiscalização de tráfego por parte dos provedores de conexão devido a questões de privacidade e por tornar a rede mais lenta e o serviço mais caro financeiramente.

Reitera-se, portanto, que é nesse sentido que Jaishankar (2007) patrocina a mandatória integração dos conhecimentos da Criminologia com os conhecimentos da Informática, defendendo que essas duas áreas, apesar de possuírem linguagens aparentemente conflitivas, devem romper com as suas tradicionais resistências isolacionistas e se englobarem no entendimento do fenômeno cibercriminoso, pois esse é o viés metodológico adequado que abarcará a demanda cada vez mais emergente da Cibercriminologia.

Dessa feita, no próximo tópico, propõe-se uma análise do fenômeno aqui em exame, levando em consideração as suas atuais características sociais e os impactos dele decorrentes, como uma específica forma criminal.

2.2 A Sequestrável Era dos Dados: *ransomware* como nova forma de criminalidade

Segundo Liska e Gallo (2017), o termo *ransomware* se origina de duas palavras nativas do idioma inglês, em que *ransom* significa pagamento ou resgate e *ware* vem da palavra *software*, especificamente de *malware*, *software* malicioso (*malicious software*). Para o Centro de Estudos, Resposta e

Tratamento de Incidentes de Segurança no Brasil, CERTbr[5], existem dois tipos de ataque *ransomware*, o do tipo *crypto* e o do tipo *locker*: o primeiro age criptografando os dados, e o acesso a eles só acontece após a liberação da chave de decodificação por parte do cibercriminoso, ao receber o pagamento da extorsão, geralmente em criptomoedas. Já o *locker* impede o acesso ao dispositivo em que os dados e as informações estão armazenados e também exige um pagamento.

Em 1989, um biólogo da universidade de Harvard, Joseph Frank Popp, desenvolveu um vírus, denominado AIDS, que tornava os dados contidos em computadores indisponíveis para seus usuários finais e exigia um pagamento para o desbloqueio dos dados. Durante a extorsão, a vítima era obrigada a enviar o dinheiro para uma caixa postal no Panamá. No entanto, o FBI logo chegou à autoria do crime e prendeu o criador da primeira ferramenta de sequestro digital (*ransomware*) da história (Pimentel; Cabrera; Forte, 2021; Liska; Galo, 2017).

Diante da facilidade com que a Polícia Federal norte-americana conseguiu identificar e prender o autor da extorsão digital, esse modelo não apresentou nenhum registro em qualquer parte do mundo que se saiba até 2005. No entanto, no limiar do século XXI, o sequestro digital, conhecido como *ransomware*, só se viu aumentar ano após ano, causando preocupações latentes em todo globo terrestre.

Um dos fatores que levou a esse aumento está diretamente ligado ao desenvolvimento de esquemas mais robustos de criptografia, ciência ou técnica que estudam maneiras de codificar e decodificar mensagens, além de mais disponibilidade de métodos avançados desse campo do saber. Também o desenvolvimento computacional fomentou de maneira exponencial a capacidade criptográfica via *software* (Liska; Gallo, 2017).

É importante destacar que os ataques *ransomware* vêm ganhando cada vez mais sofisticação técnica. Prova disso é que, desde 2008, esse tipo de criminalidade vem utilizando maciçamente algoritmos de criptografia padrão oriundos da indústria de tecnologia, a exemplo do *Triple Data Encryption Standard (3DES)* e *Advanced Encryption Standard (AES)*. No entanto, nem todos os ataques desse tipo possuem alto grau de maturidade técnica, coexistindo novos atores que tentam se estabelecer nessa indústria criminosa e grupos de cibercriminosos profissionais que já dominam o mercado de extorsão criptográfica (Pimentel; Cabrera; Forte, 2021).

[5] Disponível em https://cartilha.cert.br/*ransomware*/. Acesso em: 19 mar. 2023.

Ainda segundo Liska e Gallo (2017), a disponibilidade global de criptomoedas, como o *Bitcoin*, operadas de maneira completamente descentralizada e em pseudoanonimato, favorece a prática de *ransomware*. Pois, ao contrário do que aconteceu com o vírus AIDS, o rastreio das transações de criptomoedas, apesar de ser possível, é extremamente trabalhoso e complexo. Além disso, um extorsionário digital experimentado é capaz de se valer do próprio sistema da moeda, para ser usada em mercados comuns, antes mesmo de ser rastreado.

Em 2017, a prática de *ransomware* se tornou globalmente conhecida, em razão do famoso *ransomware Wanna Cry*, que sequestrou milhares de computadores em todo o mundo, trazendo à tona o quanto a rede mundial de computadores apresenta fragilidades, além do fato de que a dependência informática da Sociedade do Conhecimento aumenta a vulnerabilidade em níveis alarmantes (Silva; Teixeira, 2019).

Para Liska e Gallo (2017), o *ransomware* é cada vez mais comum porque é um método criminoso altamente eficaz, sobretudo em seu aspecto de ganho financeiro e a dificuldade de identificação de seus perpetradores. Antes mesmo da eclosão do famoso *Wanna Cry*, Goodman (2015) já falava do futuro do crime tendo como cerne o criminoso de informação, isto é, aquele sujeito que se vale das informações dispostas em banco de dados e na internet em geral, sendo elas expostas pelo próprio usuário ou por meio de invasões de dispositivos.

A informação assim também se torna um elemento primordial para a criminalidade em geral e um alvo crucial para o ciberdelinquente. No caso de um ataque *ransomware*, a extorsão se justifica pelo fato de que os dados e as informações cada vez mais dispostas em bancos de dados digitais são, em muitos casos, o elemento fundamental para a sobrevivência de uma organização, seja ela pública, seja privada (Goodman, 2015; Glenny, 2011).

Assim como os sequestradores de outrora, que extorquiam famílias ricas e abastadas ao manter sob cárcere privado os seus entes queridos, uma extorsão de um *ransonwarer* busca não deixar escolhas para a vítima, pois perder os dados pode comprometer todas as suas operações e negócios. Valores monetários e financeiros caminham de mãos dadas com os dados (Morais, 2021). Não à toa, Jesus e Milagre (2013) defendem que a informação seja elencada como um bem jurídico de relevância penal. Todavia, eles apontam também que há uma dissonância entre o Código Penal e Processual da Era do Rádio (década de 1940) e os crimes informáticos, no sentido de que aquele não é capaz de combater eficazmente os delitos digitais.

Desse contexto, surge a necessidade de recortar o *ransomware* a partir do entendimento de autores que se dedicam ao estudo de crimes cibernéticos. Com isso, o próximo tópico tenta esclarecer o problema de maneira mais específica.

2.3 O ransomware sob o necessário crivo da Cibercriminologia

O fenômeno aqui estudado, para além das concepções jurídicas de crime próprio ou impróprio e das abordagens técnicas da Segurança da Informação, é categorizado se destacando dentro do alargado espectro do cibercrime. Conforme aponta Llinares (2012), essa classificação, de cunho criminológico, centra-se em três grandes categorias, a partir dos sujeitos que realizam os delitos cibernéticos e os seus objetivos, a saber: o cibercrime de caráter social, o de caráter político e o econômico.

Para esse mesmo autor, na categoria de crimes cibernéticos de cunho social, estão aquelas condutas originadas das próprias relações sociais, em que se podem citar como exemplo os crimes contra a honra em redes sociais e aplicativos de trocas de mensagens, indicando que, nesse recorte, estão aqueles delitos em que o autor tem alguma ligação social com a vítima, que pode ser do tipo amorosa, familiar ou parecidas.

Já no caso do cibercrime político, estão condutas que permeiam as relações geopolíticas, em que os Estados inauguram uma nova era de guerra, a chamada guerra cibernética, ou *netwar*. Nesse caso, majoritariamente, há grupos formados e/ou financiados por Estados-nação na tentativa de realizar ataques contra sistemas informáticos críticos de países rivais (Casalunga, 2020; Clarke; Knake 2015; Greenberg, 2021).

O cibercrime do tipo econômico (aquele orientado pelo ganho patrimonial por parte do criminoso) é o que apresenta a maior parte identificável de infrações cometidas por meio do espaço digital. Nisso, Llinares (2012) aponta que é possível duas subcategorizações: a primeira em sentido estrito e a segunda em sentido mediato, ou instrumental. Entendendo esta última como forma de preparação para a primeira, é possível depreender que as duas estão, portanto, interligadas.

No caso específico da extorsão digital, o *ransomware* se enquadraria conceitualmente no sentido estrito, e uma série de invasões anteriores à extorsão (instrumentais ou mediatas) é necessária para que ele se concretize. Isso acontece, por exemplo, por meio de *spam* – envio automático e em massa de *e-mails* contendo *softwares* maliciosos – e *spyware* – uma espécie de *malware* dedicado a capturar informações de senhas e logins e todas as

atividades que acontecem em um dado dispositivo eventualmente infectado –, bem como outras infecções via *software* ou acesso físico indevido a equipamentos (Llinares, 2012; Liska; Gallo 2017). Além disso, podem-se citar técnicas de engenharia social, que consistem no uso de engano, perfídia, ardil e falsas informações para convencer um usuário de tecnologia a clicar em um *link* infectado ou, até mesmo, fornecer senhas (Henriques, 2016).

Ainda segundo aponta Llinares (2012), essa classificação não deve ser trabalhada de maneira rígida e inflexível, pois, conforme exemplifica, um crime cibernético comumente econômico, tal qual o *ransomware*, pode servir tanto a fins sociais quanto principalmente políticos – geopolíticos. Isso é clarificado em autores como Greenberg (2021) e Clarke e Knake (2015), que afirmam que Estados-nação se valem de *softwares* projetados para cometer crimes em favor de seus objetivos políticos de espionagem ou de desestabilização de nações rivais.

Nessa trilha de entendimento, o *ransomware* é mais do que uma simples delinquência informática ou meramente um crime de cunho patrimonial. Ele é um fenômeno que ocorre dentro e em decorrência da moldura social, histórica, econômica e técnica do século XXI. É interessante notar ainda que, apesar de ser um delito tipicamente patrimonial, ele não só atinge esse tipo de bem, vindo a prejudicar seriamente também a intimidade, a privacidade e, tecnicamente, diversos outros bens jurídicos fundamentais: a vida, a liberdade, o direito de ir e vir, o exercício da cidadania etc. (Linares, 2012).

É um ataque com implicações financeiras latentes e, algumas vezes, irremediáveis, tornando-se uma indústria criminosa exponencialmente lucrativa – na casa dos milhões de dólares em todo o globo terrestre. No ano de 2020, essa prática teve um aumento de 311% e gerou a cifra de 350 milhões de dólares apenas no citado período, segundo ilustra Morais (2021). De acordo com a Interpol (2022), o *ransomware* é considerado uma das principais ameaças globais e está entre os crimes com mais tendência de crescimento nos próximos anos, ao lado do seu congênere *phishing* e da lavagem de dinheiro. Em um mesmo raciocínio, Vaz-Ferreira e Rodrigues (2021) caracterizam os sequestros digitais como ameaças globais que acabam por impor graves dificuldades à persecução criminal, sobretudo às questões afetas à identificação e à autoria dos ataques, em um contexto de obscuridades quanto à nacionalidade, à origem e ao grupo do qual o criminoso faz parte.

Exemplificando o cenário dessa indústria criminosa milionária transnacional, o Município de *Lake City* na Flórida – EUA – se viu obrigado a pagar a quantia de 460 mil dólares em Bitcoin. *Riviera Beach*, também na

Flórida, desembolsou 600 mil dólares. Ambos os ataques ocorreram em 2019. Já em 2021, a empresa Colonial Pipeline, detentora da maior rede de oleodutos dos EUA, pagou 5 milhões de dólares. No Brasil, em 2020, o Superior Tribunal de Justiça (STJ) viu seus sistemas informáticos inacessíveis, assim como o Tribunal de Justiça do Rio Grande do Sul, após ataques do tipo r*ansomware*. Todo esse cenário, por exemplo, fez com que os EUA considerassem esse tipo de criminalidade como uma questão de segurança nacional (Vaz-Ferreira; Rodrigues, 2021).

Segundo Liska e Gallo (2017), os cibercriminosos de hoje estão se concentrando em atacar corporações, para as quais os dados possuem valor significativamente mais elevado, o que nos leva a concluir que o *ransomware* é produto desviante e delinquencial de sociedades globais interdependentes dos dados, fazendo com que o contínuo avanço social e econômico trazido pelas tecnologias globalizantes também seja força motriz de um tipo específico e mais avassalador de extorsão, um novo tipo de sujeito desviante[6] e de novas formas de insegurança pública.

Mais ainda, entra-se na Era da Computação Armada, em que uma quantidade oceânica de *softwares* projetados para cometer crimes – o *crimeware* e especialmente o *ransomware as a service (ransomware* como serviço*)* – é facilmente acessada e adquirida nos caminhos da *Dark Web* e *Deep Web*. Ambientes estes em que se pode vender e comprar de tudo: substâncias das mais diversas, pornografia infantil e programas de computador, bem como o financiamento e o planejamento de ataques terroristas (Goodman, 2015; Glenny, 2011).

O desenvolvimento de novas ferramentas é prontamente percebido e utilizado pelos cibercriminosos que as malversam para seus fins ilegítimos, como foi o caso das já citadas criptomoedas, das tecnologias de criptografia e do aumento do poder computacional. Dito de outro modo, é a tecnologia como aliada do crime (Gomes; Nunes; Wilmers, 2020; Goodman, 2015).

Todas essas considerações levam à inegável complexidade do tema e a diversos dificultadores para sua mitigação atualmente. Com efeito, elencam-se, no próximo tópico, características que impõem agigantadas dificuldades e que merecem, por isso, melhor aprofundamento.

[6] Sobre estudos que se dedicam ao perfil de ciberdelinquentes, consultar Arroyo (2020) e Vianna e Machado (2013).

2.4 Fomentando desafios para a Criminologia convencional: a implosão da territorialidade e o surgimento da criminalidade ubíqua

Para Gama (2021), a eficácia dos objetivos criminosos de operações de *malware* é facilitada e possibilitada operacionalmente pela dispersão territorial que os meios informáticos provêm, o que faz com que vítimas e autores estejam em localidades diferentes e sejam interligados quase que unicamente pelas tecnologias cibernéticas de redes de computadores. A cibercriminalidade claramente alarga-se para além das fronteiras nacionais, identificando e explorando lacunas legais desse horizonte e a desconexão territorial para evadir-se de eventuais detenções, prisões e aplicações da lei.

Um bom exemplo disso é trazido por Goodman (2015). O autor em questão afirma que demonstrações práticas de pesquisadores de segurança da informação provam que é possível para criminosos invadirem um dispositivo que esteja alocado em um automóvel qualquer a 2.500Km de distância, enquanto o carro é dirigido a uma velocidade de 100 Km/h.

Sob o ponto de vista da persecução criminal, o problema da territorialidade se impõe como importante ponto de inflexão quanto a capacidade de os Estados punirem cibercriminosos, tendo em vista que os países possuem legislações e motivações geopolíticas diferentes entre si. Além do fato de que o ciberespaço não pode ser entendido propriamente como um território, mas sim como um fenômeno mundial de fluxo de informações via redes de comunicações (Santos, 2014).

Por outro lado, Luna e Labrin (2017) apontam que o fenômeno da hiperconectividade informática traz consigo a irrelevância do espaço físico, assim como a aniquilação do tempo, ao demonstrarem a perda significativa do valor do território frente ao fenômeno tecnológico em riste.

Outro ponto de muita importância é o surgimento da computação ubíqua, que é a integração naturalizada entre *bits* e o mundo físico. Situação essa que foi acentuada pela internet das coisas (*IoT*), em que passaremos para a hiperconectividade, na qual tudo poderá se conectar à internet – desde geladeiras aos carros, passando pelos trincos das portas e dos postes de iluminação pública. Irresistivelmente, todos os objetos do mundo físico vêm se constituindo em endereços de internet – o IP (Goodman, 2015).

O impacto da computação ubíqua para a (des)territorialidade do cibercrime é, por consequência, altamente significativo, porque tal condição indica que o mundo físico tem sido cada vez mais assimilado pelo computador, ou melhor, pelas conexões de redes de computadores. Isso acarreta a fusão de átomos do mundo natural (físico) com *bits* do mundo digital, fazendo com que

seja zerada, praticamente, a distinção entre esses dois mundos (Goodman, 2015; Luna; Labrin, 2017).

É justamente nesse cenário de computação ubíqua que o *ransomware* tem imposto seríssimas dificuldades a toda a sociedade global, e as ferramentas estatais de dissuasão, controle social, prevenção e repressão sequer vislumbram algum horizonte de possibilidade para frear tal ameaça. Isso reflete uma leitura fenomenológica dos crimes digitais (Kunrath, 2014).

Como dito anteriormente, o perfil empreendedor dos cibercriminosos encontra, justamente nesse ambiente sociotécnico, campo fértil para operações de sequestro digital. Tudo isso é possibilitado por avanços cada vez mais notáveis das capacidades informáticas em diversas frentes, como criptografia e computação ubíqua, além de debilidades ou omissão legal dos Estados, investimento abundante nas melhorias das redes de computadores e acentuação exponencial da dependência econômica dos dados digitais (Goodman, 2015; Liska; Gallo, 2017; Pimentel; Cabrera; Forte, 2021).

Pois bem, surge inegavelmente uma nova fronteira aos criminólogos, tão empolgante quanto espinhosa e tortuosa. Uma nova forma de desvio, crime e possível controle social: o sequestro digital, caracterizando-se na órbita da ubiquidade e da digitalização massiva.

Tradicionalmente, o crime sempre esteve ligado a questões territoriais, tanto para a Criminologia quanto para o Direito e demais áreas que a ele dedicam estudo. Acontece que o ciberespaço é definido como um novo domínio, além da terra, ar, mar e espaço, e isso muda radicalmente a concepção de controle social – informal e/ou formal (Gonzales; Santos; Herrera, 2023).

Esse Quinto Domínio, assim chamado pelos militares dedicados à Guerra Cibernética nos EUA, também é tratado por alguns cibercriminólogos como um *locus* de atividade criminosa e um complexo emaranhado de delitos, fazendo surgir o cibercriminoso e a cibervítima em caráter assimétrico quanto ao conhecimento da rede mundial de computadores. Isso ocorre de tal maneira que, enquanto a vítima consome os recursos providos pelas tecnologias, os cibercriminosos dedicam tempo e recursos para identificar vulnerabilidades técnicas e humanas e explorá-las na medida da própria evolução tecnológica. (Kunrath, 2014; Gonzales; Santos; Herrera, 2023).

Uma das principais causas para os controles sociais convencionais, assentados em territorialidade – prisão, investigação, lei penal interna dos Estados, julgamento, processo e condenação – não estarem funcionando assertivamente no controle, na prevenção e na repressão dos crimes

cibernéticos, e, em especial, do *ransomware*, está no fato aqui tão discutido da computação ubíqua, que fomenta a Computação Armada. Em outras palavras: *softwares* desenvolvidos para a prática criminosa permitem que infratores cometam crimes simplesmente por meio de cliques de mouses e não mais por meio de recursos dispendiosos do mundo físico. Dessa forma, a questão territorial, mais uma vez, é completamente irrelevante.

A exemplo, o ciberdelinquente não se vale de uma alavanca para invadir e furtar uma mansão ou uma arma de fogo para rapto de uma pessoa objetivando extorsão. O extorsionário digital se vale de pacotes de zeros e uns tanto para invadir um sistema quanto para extorquir seus proprietários, não importando a distância. Portanto, a informação é, ao mesmo tempo, alvo e instrumento do cibercriminoso. Trata-se de uma engenhosidade completamente diferente, a nível instrumental, dos crimes físicos (Goodman, 2015).

Segundo Kunrath (2014), a peculiaridade intelectual do cibercriminoso faz com que uma política criminal baseada total ou majoritariamente no Direito Penal e Processual Penal não arrefeça ou mitigue o avanço dos crimes de informática. Pelo contrário, essas clássicas ferramentas jurídicas podem causar até mesmo o efeito inverso do que se propõem. Soma-se a isso o fato de que o desenvolvimento tecnológico distribuído globalmente permite que grupos ciberdelinquentes de matizes diversas estabeleçam contatos internacionais, sem o menor esforço e se valendo de mínimos recursos e ferramentas, em consonância com que diz Carrapiço (2005).

Exemplo dessa insignificância territorial é visto no ano de 2017, quando os *ransomwares Not Petya e Wanna Cry*, assim apelidados pela comunidade de segurança cibernética, sequestraram milhares de computadores ao redor do mundo – Europa Central, Leste Europeu, EUA, América Latina e Ásia, causando simultâneos desastres nacionais com impactos internacionais severos: de apagões elétricos até a inoperabilidade de sistemas de governos e hospitais (Greenberg, 2021).

Algumas tentativas de controle do cibercrime a nível internacional e nacional têm surtido pouco efeito para mitigação das ameaças criminais cibernéticas e os danos delas decorrentes. Um exemplo disso é a Convenção sobre o Cibercrime de 2001[7], também conhecida como Convenção de Budapeste, em que se busca uma atuação conjunta e comum dos Estados

[7] Em 12/04/2023, o Brasil passou a ser signatário da Convenção sobre o Cibercrime, conforme Decreto 11.491.

frente à criminalidade digital, além da vigilância de patrulha executada pelas polícias na *Surface Web* e *Deep Web*, a criação de delegacias especializadas, o FBI *Cyber Crimes Program* e a crescente criação de tipos penais voltados para condutas delituosas na rede. Mesmo com os diversos intentos dos Estados de se valerem da tecnologia para conter tal fenômeno, o cenário contemporâneo demonstra que, ainda, a tecnologia informática mais tem facilitado a desenvoltura do crime do que a contido (Carrapiço, 2005).

Jesus e Milagre (2013) chamam a atenção para o surgimento, nesse contexto, dos apelidados paraísos eletrônicos, fazendo uma comparação com os paraísos fiscais, em que criminosos se valem para lavar dinheiro oriundo de atividades ilícitas. O cibercriminoso utiliza esses paraísos eletrônicos, pois neles existem serviços altamente orientados à privacidade que acabam por fomentar o anonimato – ainda que não seja por completo, dado que, nesse caso, não são coletados e armazenados os registros de atividades dos usuários na rede.

Em muitas vezes, é uma ferramenta legítima, sobretudo para indivíduos submetidos a Estados e governos totalitários que violam diuturnamente a vida privada. No entanto, mais uma vez, o cibercriminoso malversa ferramentas legítimas para fins ilegítimos. Para os citados autores, essa questão é uma das principais dificuldades dos Estados em rastrear e identificar cibercriminosos.

Além disso, Vaz-Ferreira e Rodrigues (2021) citam o estudo *Cyber Operations Tracker do Council of Foreign Relations* do ano de 2021, em que é traçada uma estimativa de que, no período compreendido entre 2005 e 2020, 77% de todas as operações maliciosas na Rede Mundial de Computadores tiveram origem no conjunto de países composto por Rússia, China, Irã e Coreia do Norte, caracterizando essas nações como espécies de portos seguros para operações cibercriminosas. Situação essa que fragiliza os tratados internacionais[8] a nível de cooperação jurídica e policial, tal como a Convenção sobre o Cibercrime de 2001, à qual os citados países não aderiram.

Urge diferenciar os conceitos de paraíso eletrônico e porto seguro cibercriminoso. O primeiro diz respeito à vontade legislativa de alguns Estados em não obrigarem empresas que atuam em seu território a coletar dados dos usuários da internet – por questões de posicionamento em prol da privacidade de cidadãos. Por outro lado, o segundo diz respeito a omissões deliberadas e estratégicas, do ponto de vista geopolítico, de Estados que enxergam o espaço cibernético como domínio para vantagens competitivas militares e envolto a

[8] Vaz-Ferreira e Rodrigues (2021) defendem os tratados internacionais como ferramentas centrais no enfrentamento dos cibercrimes.

rivalidades oriundas das relações entre Estados. Além disso, como debatem Clarke e Knake (2015), é comum que cibercriminosos sejam recrutados para atuarem como guerreiros cibernéticos, em nome de interesses obscuros estatais. Ambas as condições impactam na ocorrência da cibercriminalidade transnacional, todavia por caminhos diferentes.

Em concordância ao proposto, Liska e Gallo (2017) acreditam que o anonimato é uma das principais características que fazem o *ransomware* ser tão efetivo, pois é extremamente difícil identificar seus perpetradores, dado que eles se valem eficazmente de operações de segurança, conhecidas no meio como "Opsec", de acordo com o exemplificado em Vieira (2022). Desse modo, impõem-se grandes dificuldades para rastrear e identificar os perpetradores de sequestros digitais.

3 CONCLUSÃO

A partir das discussões aqui trazidas e levantadas, tem-se que as teorias criminológicas não se configuram como totalmente imprestáveis frente ao fenômeno do *ransomware*, nem ao cibercrime de maneira geral. Como discutido, as Teorias da Associação Diferencial e da Subcultura Criminal encontram espaços adequados para se analisar o perfil do ciberdelinquente. No entanto, os dois primeiros arranjos teóricos ainda encontram limitação devido ao surgimento de um novo domínio: o espaço cibernético.

Até mesmo porque não haveria como essas teorias abarcarem tal espaço, pois foram pensadas e forjadas antes de o surgimento do meio cibernético passar a ser dominante e absoluto na vida em sociedade contemporânea. Para tanto, as Teorias da Desinibição *On-line*, no campo da Psicologia, e a Teoria da Transição Espacial, no campo da Criminologia, surgem exatamente da preocupação de seus defensores em entender como o espaço cibernético permite novas formas de criminalidade e condutas, e aqui se pode dizer o *ransomware*.

A grande complexidade enfrentada pela Criminologia tradicional frente aos sequestros digitais reside exatamente na dinâmica assimétrica entre vida *off-line* e *on-line*, em que há transição de condutas. Assim, as teorias macrossociológicas vigentes e convencionais precisam se adequar ao meio cibernético para superar as suas limitações, o que quer dizer que elas são capazes de explicar, ainda que com limitações, o problema analisado.

Restou clarificado que a soma das teorias criminológicas é o meio mais adequado para se entenderem os cibercrimes e suas complexidades. Nisso se inclui o sequestro digital, pois a abordagem isolada de uma teoria, quando se

busca compreender o fenômeno, apresenta inúmeras lacunas. Quanto a isso, a Cibercriminologia, ao integrar os conhecimentos da Informática aos seus objetos de análise, é a subárea da Criminologia mais indicada para tratar a complexidade do tema.

Outro ponto severo de desafio criminológico, um dos mais importantes, é a desterritorialização promovida pelas condutas criminais informáticas, uma vez que foi demonstrado como o crime sempre esteve ligado, mesmo nas acepções teóricas e acadêmicas, em maior ou menor grau, ao território. Os eventos cibernéticos criminais, como fenômenos de uma era continuamente dependente da informática e dos dados, fazem com que a Criminologia toque em uma barreira, uma fronteira metodológica.

Como exemplo, a Subcultura Criminal propõe que o indivíduo se identifica com valores desviantes em contextos de grupos estabelecidos fisicamente no tempo e no espaço – físico ou territorial –, ao passo que o criminoso digital se relaciona em grupos estabelecidos na internet e com pessoas que se valem de *usernames*. Na mesma proporção, a Teoria da Associação Diferencial defende que o crime é aprendido pelo sujeito em contato, evidentemente físico, com outras pessoas desviantes. Todavia, demonstrou-se que essas teorias são aplicáveis quando levam em consideração os preceitos da Cibercriminologia, porque surgem limitações em decorrência das questões de anonimato, flexibilidade de identidades, extrema fluidez de movimentos entre grupos cibernéticos e a origem social e econômica dos ciberdelinquentes que, muitas vezes, advêm das classes não marginalizadas e não excluídas.

Também como resultado, o trabalho insta a participação de diversos pesquisadores frente aos problemas da digitalização e seu impacto no estudo do crime e do controle social, não se pretendendo, com isso, encerrar o tema. Pelo contrário: trata-se de um convite para debates aprofundados dos campos da Segurança Pública, Direito, Informática e Criminologia, a fim de trazer novas abordagens críticas quanto ao entendimento dos crimes cibernéticos.

REFERÊNCIAS

ARROYO, Sergio Cámara. Estudios Criminologicos Contemporáneos: La Cibercriminología y el perfil del ciberdelincuente. **Revista Derecho y Cambio Social,** nº 60, p. 470-512, Peru: Universidad de la Rioja, 2020. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=7524987. Acesso em: 1º maio. 2023.

BISSO, Rodrigo; KREUTZ, Diego; RODRIGUES, Gustavo; PAZ, Giulliano. Vazamentos de Dados: Histórico, Impacto Socioeconômico e as Novas Leis de Proteção de Dados. **Workshop Regional de Segurança da Informação e de Sistemas Computacionais.** WRSeg: 2019. Disponível em: https://sol.sbc.org.br/index.php/errc/article/view/9230. Acesso em: 5 jul. 2023.

CARRAPIÇO, Helena. O Crime Organizado e as Novas Tecnologias: Uma Faca de Dois Gumes. **Revista Nação e Defesa:** 2005. Disponível em: http://hdl.handle.net/10400.26/1156. Acesso em: 1º ago. 2023.

CASALUNGA, Fernando Henrique. **Guerra Híbrida Cibernética: Uma Análise do Conflito Rússia-Ucrânia (2015) sob a perspectiva da tecnologia da informação**. Dissertação de Mestrado. Recife: Universidade Federal de Pernambuco, 2020. Disponível em: https://repositorio.ufpe.br/handle/123456789/37637. Acesso em: 20 jun. 2023.

CLARKE, Richard A; KNAKE, Robert K. **Guerra Cibernética:** a próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro, RJ: Brasport, 2015.

DITZ, Yanina; MINETTI, Gabriela. Detección de Ransomware en Blockchains. **XXV Workshop de Investigadores en Ciencias de la Computación**. Universidad Nacional de La Pampa. Santa Rosa: 2023. Disponível em: https://sedici.unlp.edu.ar/handle/10915/163244. Acesso em: 14 mai. 2024.

FAVERO, Bruno de Oliveira; FAVERO, Altamiro de Oliveira. **Cibercriminologia:** os meios eletrônicos e o policiamento em ambientes digitais. São Paulo: Paco Editorial, 2021.

GAMA, João Pedro Senra Pimenta da. **Cibercriminalidade Organizada:** modelos de organização em rede e o cibercriminoso. Dissertação de mestrado. Porto: Universidade do Porto, 2021. Disponível em: https://repositorio-aberto.up.pt/bitstream/10216/134934/2/483841.pdf. Acesso em: 1º abr. 2023.

GLENNY, Misha. **Mercado Sombrio:** o cibercrime e você; tradução de Augusto Pacheco Calil, Jorge Schlesinger e Luiz A. de Araújo. São Paulo: Companhia das Letras, 2011.

GOODMAN, Marc. **Future Crimes**: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso; tradução de Gerson Yamagami. São Paulo: HSM Editora, 2015.

GOMES, Luiz Eduardo dos Santos Pereira; NUNES, Luana Esteche; WILMERS, Michael Felipe. Natureza Jurídica do Crime de *Ransomware* e a Utilização da Criptomoeda como Meio de Impunidade. **Escola Superior do Ministério Público do Ceará** – ano 12, nº2 / Jul./Dez.2020: Fortaleza: 2020. Disponível em: https://doi.org/10.54275/raesmpce.v12i2.50. Acesso em: 2 abr. 2023.

GONZALES, Vitor Henrique; SANTOS, Claudio Augusto Payá; HERRERA, Bernado Peña. **Estudio Criminológico del Ciberdelicuente y sus Victimas**. Catalunha: Universidade Pablo Olavide, 2023. Disponível em: https://doi.org/10.46661/respublica.8072 . Acesso em: 7 mar. 2023.

GREENBERG, Andy. **Sandworm:** uma nova era na Guerra Cibernética e a caça aos hackers mais perigosos do Kremlin; tradução de Debora Ramires. Rio de Janeiro: Alta Books, 2021.

HENRIQUES, Francisco de Assis Fialho. **A Influência da Engenharia Social no Fator Humano nas Organizações**. Dissertação de Mestrado. Recife: Universidade Federal de Pernambuco, 2016. Disponível em: https://repositorio.ufpe.br/handle/123456789/25353 . Acesso em: 7 mar. 2023.

INTERPOL. **Interpol Global Crime Trend Report**. Disponível em: https://www.interpol.int/content/download/19843/file/INTERPOL%20%20Annual%20Report%202022_EN.pdf. Acesso em: 2 set. 2023.

JAISHANKAR, Karuppannan. Cyber Criminology: Envolving a novel discipline with a new journal. **International Journal of Cyber Criminology**, vol. 1, Jan. 2007. Disponível em: https://www.cybercrimejournal.com/pdf/editorialijcc.pdf. Acesso em: 15 jul. 2023.

JESUS, Damásio Evangelista de; MILAGRE, José Antônio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2013.

KUNRATH, Josefa Cristina Tomaz Martins. **A expansão da Criminalidade no Ciberespaço:** desafios de uma política criminal de prevenção ao cibercrime. Dissertação de mestrado. Salvador: Universidade Federal da Bahia, 2014. Disponível em:http://www.progesp.ufba.br/sites/progesp.ufba.br/files/dissertacao-final-josefa-cristina-tomaz-martins-kunrath-2014.pdf. Acesso em: 15 jul. 2023.

LLINARES, Fernando Miró. **El Cibercrimén: Fenomelogía y crimonología de la delicuencia en el ciberespacio**. Madri: Marcial Pons, 2012. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=4408078. Acesso em: 15 jul. 2023.

LISKA, Allan; GALLO, Timothy. ***Ransomware*:** defendendo-se da extorsão digital; tradução de Lúcia A. Kinoshita. São Paulo: Novatec Editora LTDA, 2017.

LUCENA, Mariana Barrêto Nóbrega. O desvio social na rede mundial de computadores: Aspectos sociológicos e psicológicos dos indivíduos

pertencentes às subculturas criminais da internet. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 17, n. 3128, 24 jan. 2012. Disponível em: https://jus.com.br/artigos/20921. Acesso em: 24 ago. 2023.

LUNA, Julio César García; LABRIN, Daniel Ernesto Peña. Cibercriminalidad e Postmodernidad: la Cibercriminologia como respuesta al escenario contemporâneo. **Revista Pensamiento Penal.** Lima: 2017. Disponível em: https://www.pensamientopenal.com.ar/doctrina/44898-cibercriminalidad-y-posmodernidad-cibercriminologia-respuesta-al-escenario. Acesso em: 25 ago. 2023.

MIGUEL, Luís Felipe. Meios de comunicação de massa e política no Brasil. **Diálogos Latinoamericanos [en linea],** 2001. ISSN: 1600-0110. Disponível em: https://www.redalyc.org/articulo.oa?id=16200302. Acesso em: 3 mar. 2024.

MORAIS, Cézar Henrique Júnior Pontes. **Ransomware:** Segurança da Informação e Prevenção. Goiânia: Pontifícia Universidade Católica de Goiás, 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1619. Acesso em: 1º ago. 2023.

MOREIRA, Marcelo da Silva. **Análise de manuais de pedofilia na Dark Web para prevenção de crimes sexuais contra crianças e adolescentes**. Universidade Federal de Santa Catarina, 2019. Disponível em: https://repositorio.ufsc.br/handle/123456789/214969. Acesso em: 14 out. 2024.

PIMENTEL, José Eduardo de Souza; CABRERA, Diego Antunes; FORTE, Cleberson Eugênio. Ransomware: do surgimento aos ataques as a service. **Congresso de Segurança da Informação**. São Paulo: 2021. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/44. Acesso em: 20 mai. 2023.

SANTOS, Claudomiro Junior de Castro. **Crimes de Informática**. Monografia. Presidente Prudente: Faculdades Integradas Antônio Eufrásio de Toledo, 2014.

SILVA, Felipe Rangel da; TEIXEIRA, Rodrigo Giublin. A Sociedade da Informação e Seus Desafios: a Necessidade de Efetivação de uma Política Pública de Combate ao Ransomware no Brasil. RFD – **Revista da Faculdade de Direito da UERJ**, nº 36, dez.2019. Rio de Janeiro: 2019.Disponível em: https://doi.org/10.12957/rfd.2019.40697. Acesso em: 15 jun. 2023.

VIANNA, Tulio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013.

VAZ-FERREIRA, Luciano; RODRIGUES, Filipe Bach. O Ransomware como ameaça à cibersegurança da gestão pública de dados no Brasil. **Revista Intellector**, n. 35, Rio de Janeiro: 2021. Disponível em: https://doi.org/10.5281/zenodo.5515726. Acesso em: 1º jul. 2023.

VIEIRA, Vinicius. **OPSEC:** Inteligência Cibernética na Prática. São Paulo: Clube de Autores, 2022.