João Pedro Senra Pimenta da Gama

CIBERCRIMINALIDADE ORGANIZADA: OS MODELOS DE ORGANIZAÇÃO EM REDE E O CIBERCRIMINOSO

Mestrado em Criminologia

Dissertação sob orientação do
Prof. Doutor **André Lamas Leite**

Maio 2021

RESUMO

A presente tese teve por objetivo propor um modelo explicativo da cibercriminalidade organizada baseado no conceito de organização em rede e apontar a tendência futura dos organismos cibercriminosos em assumirem um desenvolvimento descentralizado das suas células. Sugere a emergência de um perfil de cibercriminoso cujo referencial normativo é constituído pelos valores do empreendedorismo. No seio do ciberespaço ergue-se uma criminalidade organizada pautada pela autonomia técnica e organizativa dos ciberdelinquentes, tendencialmente desgarrados da organização piramidal e do modelo burocrático que marcaria décadas de crime organizado. A sedimentação de um perfil de cibercriminoso inovador, criativo e intelectualmente capaz inculca na centralidade crescente assumida pelos atores periféricos no desenvolvimento das células criminais, bem como na tendência para organizações descentralizadas de reduzida escala. Doravante, a tendência será a formação de pequenas agremiações criminosas compostas por delinquentes recrutados em função do guião criminal e das suas mais-valias técnicas – os *facilitators.* O núcleo duro tenderá a reduzir e o processo de descentralização e dispersão horizontal das relações tenderá a sedimentar-se e a substituir o padrão hierarquizado dos modelos burocratizados: emerge no seio das organizações aquilo a que chamamos de *swarmização.* Recorrendo à tipologia estabelecida por McGuire (2012) e alicerçados nas considerações sociológicas de Whyte (1951), Mayo (1933) e Pareto (1910), sugerimos um modelo explicativo e um padrão de crescimento dotado de utilidade analítica para futuros estudos empíricos.

Palavras-chave: cibercriminoso; crime organizado; *swarmização*; organização em rede; empreendedorismo.

ABSTRACT

The purpose of this paper aims at showing a self-explanatory model for organized cybercrime based on network organization and pointing to the future trend of cybercrime organizations assuming a decentralized cellular development. Suggests the rising of a cybercrime profile whose reference sits on entrepreneurship values. In cyberspace innermost arises an organized criminality under the technical autonomy ofcyber criminality, tending to stray away from the pyramidal organization and from the bureaucratic model which would set the trend in decades of organized crime. Setting an innovative cybercrime profile, creative and intellectually fitted, reveals the growing centrality performed by the peripheral actors in the development of cellular crime, as well as setting the trend for decentralized small scale organizations. From now on the trend will be the small scale criminal organizations formed by offenders recruited according to a criminal guidance and technical know-how- the facilitators. The inner core will reduce itself and the decentralization process as well as the network horizontal spreading will grow steady and gradually replacing the hierarchical pattern of bureaucratic models: it emerges from within the organizations what could be called as the swarming. According to the typology established by McGuire (2012) and grounded in the sociological meanings of Whyte (1951), Mayo (1933) and Pareto (1910) we suggest an explanatory model and a growing and bold pattern for future empirical studies.

Key-words: cybercriminal; organized crime; swarming; network organization; entrepreneurship.

ÍNDICE

Capítulo I- Introdução

A presente tese divide-se em seis capítulos, cuja arrumação poderá ser agrupada em dois grandes objetivos: a revisão de literatura sobre o cibercrime e a resposta às questões de investigação.

O segundo capítulo resume o estado da arte do fenómeno do cibercrime engavetado em três grandes esferas: o cibercrime e o espaço digital, a que corresponde o ponto 2.1; a política criminal e os diferentes discursos que torneiam o fenómeno da cibercriminalidade, a que corresponde o ponto 2.2, e o perfil do cibercriminoso, a que corresponde o ponto 2.3.

O terceiro capítulo corresponde à exposição metodológica. Divide-se em dois pontos. O ponto 3.1 indica os objetivos do estudo e o ponto 3.2 resume a estrutura dos capítulos subsequentes.

Nos capítulos quarto e quinto, o objetivo será expor, em função dos objetivos delineados, alguns conceitos chave e considerações teóricas e empíricas pertinentes para a resposta às questões lançadas no ponto 3.1.

Mais concretamente, assumem centralidade na exposição destes dois capítulos a tipologia estabelecida por McGuire (2012) e o conceito de cibercriminoso empreendedor retirado dos estudos de Neves *et al.* (2015).

O capítulo quarto remete para o desenvolvimento da temática do cibercrime organizado, cujo desenvolvimento se completa com considerações teóricas acerca do crime organizado e de trabalhos sociológicos no âmbito das organizações.

O capítulo quinto parte da assunção das semelhanças entre o perfil dos criminosos de colarinho branco e os cibercriminosos sugerida por Sherizen (1990) para elaborar uma proposta explicativa do perfil do cibercriminoso, cujo referencial normativo aponta para os valores do empreendedorismo enquadráveis no criminoso de colarinho branco empreendedor teorizado por Neves *et al.* (2015).

O capítulo sexto parte do conceito de modelo de organização em rede (Gameiro, 2008) estabelecido no ponto 6.1 para a resposta às questões de investigações delimitadas no ponto 3.1.

CAPÍTULO II - Revisão de literatura

2.1- O cibercrime e o espaço digital

As sociedades atuais caraterizam-se pela abundância de redes informacionais. O fluxo de conexões apresenta-se de tal modo avassalador que um dos principais desafios da contemporaneidade passará inevitavelmente pela regulação das múltiplas e variadas esferas de poder, que emergem do enorme leito comunicacional que pauta a sociedade em rede. Os Estados, cada vez mais dependentes entre si, correm atrás da fluidez das ligações, perseguindo com a pauta da regulamentação os fenómenos socioculturais e socioeconómicos que se renovam e transformam de forma cada vez mais contagiosa. Como refere Byung-Chul Han (2019), a comunicação digital assume a forma não só de espectro, mas também de vírus. É contagiosa, porque se produz imediatamente no plano emocional ou afetivo.

O Direito, enquanto reduto que estabelece as normatividades, multiplica-se em instrumentos transnacionais. Prescinde do seu elemento centrípeto, perseguindo as regulamentações laterais das relações.

Os instrumentos normativos buscam adaptar-se constantemente às novas dinâmicas sociais, bem como às pré-existentes de contornos modificados e a todas que na borda da legitimidade porventura poderiam ganhar consistência se em si não encontrassem poder dissuasor bastante (Tatarinova *et al.*, 2016).

A emergência dos modernos fenómenos regulatórios impõe novos desafios à Criminologia enquanto parte integrante do chamado Direito Penal Total e disciplina autónoma que busca a compreensão das múltiplas formas de organizações dos espaços delinquenciais.

A cibercriminalidade, enquanto realidade sociocriminal emergente e em constante reconstrução, impõe ao investigador a tarefa cada vez mais exigente de construção de um metadiscurso crítico e introspetivo, capaz de criticamente avaliar os métodos, os conceitos e as teorias a partir das quais compreende os fenómenos (Agra, 2005).

A internet, espaço no seio do qual emerge a cibercriminalidade, trata-se de um fenómeno relativamente recente: a sua exploração comercial data apenas da década de Oitenta da passada centúria. Mais recente ainda será o fenómeno do chamado *Big Data*, com o aumento no volume

de dados e sofisticação das estruturas de armazenamento da informação a erguer o véu dos mecanismos societais cada vez mais assentes no controlo, vigilância e disciplina (Garland, 2001).

O antropológico espaço físico que sempre caraterizou a vivência humana transmuta-se paulatinamente num palco secundário das vivências, fruto da emergência exasperada do mundo digital (Byung-Chul Han, 2020).

A tendência de criação de redes cada vez mais alargadas de contactos pessoais no espaço digital reflete-se no crescimento proporcional da suscetibilidade à vitimação (Taivo, 2015). O imperativo da digitalização que marca o processo crescente de transformação tecnológica das estruturas comunicativas herdadas do século XX integra o núcleo das políticas públicas nacionais e transnacionais, com cobertura por vezes insuficiente do Direito Penal.

Das suas brechas renasce o crime sob novas vestes (Sutherland, 2018). Da Convenção sobre o Cibercrime do Conselho da Europa, realizada em 23 de novembro de 2001, em Budapeste, destacamos as seguintes diretrizes: ligação das tecnologias de informação a todos os aspetos da atividade mundana; promoção de medidas técnicas de proteção de sistemas de informática relacionadas com medidas jurídicas de prevenção e dissuasão da delinquência e respeito pelos direitos humanos na sociedade de informação.

Como forma de crescimento económico, integração e modernização das economias de mercado e mitigação das desigualdades socioculturais (Santos, 2018), a digitalização impõe mudanças profundas ao nível micro e macro. A crescente expansão dos mercados *online*, bem como a prestações de serviços administrativos *online* conduziram muitos governos a criarem linhas de telefone e espaços *online* de denúncia de mecanismos fraudulentos cometidos no ciberespaço (Sutherland, 2018).

Com o imperativo da digitalização surge a atomização das vítimas. Um estudo realizado pela Norton (Symantec) revela que 65% dos utilizadores da internet já experienciou algum tipo de vitimação fruto da cibercriminalidade: na análise estatística, os dados revelam que a China com 83% lidera o *ranking*, seguida do Brasil/Índia e dos Estados Unidos com 76% e 73%, respetivamente.

Tatarinova (2016) concluiu que as atividades de *download* e *online gaming* apresentam os índices mais elevados de vitimação. No caso de disseminação de *malware* ou congeminação de esquemas fraudulentos no ciberespaço, entre os quais se destacam o *phishing*, o *carding*, o *spam* acaba por ser o primeiro ponto de contacto (Alazab & Broadhurst, 2015).

As transformações no espaço digital, apesar de refletirem uma dinâmica própria que deverá ser estudada autonomamente, com as suas leis e mecanismos (D. S. Wall, 2008), não deixa de demonstrar em maior ou menor grau as particularidades do meio social em que se insere, bem como o enquadramento psicossocial dos atores que o protagonizam (Walker & Bakopoulo´s, 2005).

O cibercrime, como ausente do espaço físico, carateriza-se pelo anonimato, escalabilidade e acesso global (Santos, 2015).

A heterogeneidade dos cibercrimes, que do ponto de vista legal se reflete na ampla variedade de tipos de ilícitos que podem ser considerados incluídos no conceito, coloca iguais dificuldades quanto à sua definição.

A definição de cibercrime comporta dificuldades inerentes à sua natureza fluída e transnacional: dificuldades que emergem do facto de quebrar com as barreiras dos espaços nacionais, e por isso alargar a sua definição à concorrência de várias esferas jurídico-políticas (L. F. Taritova, 2015); e dificuldades que resultam da heterogeneidade de bens jurídicos tutelados (Faria Costa, 1998).

De acordo com Stephanie Perrin (2005), o cibercrime avoca a si diferentes fenomenologias:

i)- criminalidade no ciberespaço

ii)- utilização fraudulenta de sistemas informáticos, de redes e dados informáticos

iii)- infrações criminais

iv)- atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de rede e dados informáticos

v)- cibercriminalidade

vi)- incriminação desses comportamentos

Partindo da definição do cibercrime como *the use of electronic communication for criminal and transgressive activities that involve the internet and web-based information and communication tecnologies,* observamos que a estrutura da definição coloca a tónica no facto de ser utilizada comunicação eletrónica para o crime e para atividades transgressoras na internet: a definição circula a instituição da ação de um sujeito no espaço: parte do instrumento como forma de significação (Barbai, 2013).

Os comportamentos cibercriminais são muito diferenciados entre si. Podemos falar de invasão de computadores, fraude, furto de propriedade intelectual, assédio sexual, etc. (Amador, 2013). Por isso mesmo, julgamos que a melhor forma de homogeneização de práticas tão diversas será enfatizar o recurso aos meios tecnológicos como elemento distintivo que permite separar entre crimes cometidos no ciberespaço (mais comumente designados como crimes *online*) e crimes cometidos no espaço físico (também designados de crimes *offline*).

Porém, apesar da homogeneização alcançada pela via do instrumento tecnológico, sabemos que as realidades criminológicas diferem bastante se falarmos de crimes cometidos contra bens eminentemente patrimoniais, como é o caso do *phishing* ou da propagação de *malware*, ou delitos cometidos contra bens eminentemente pessoais, como é o caso do *sexting*, do *cyberstalking* ou do assédio sexual.

2.2 - Política-criminal e o cibercrime: diferentes discursos

Abrimos esta secção com uma citação de Castells (1991, p. 288-289), proferida por Klaus Sessar (2009, p. 597):

Aquilo a que primariamente as novas políticas preventivas se dirigem já não é aos indivíduos, mas aos fatores, às correlações estatísticas de elementos heterogéneos. Desconstroem o sujeito no concreto da intervenção e reconstroem a combinação de fatores responsável pela produção do risco. O seu objetivo primeiro não é confrontar uma situação perigosa concreta, mas antecipar todas as formas possíveis de irrupção do perigo (…) Para se ser suspeito já não é necessário manifestar sintomas de anormalidade, basta exibir uma qualquer das caraterísticas que os especialistas responsáveis pela definição da política preventiva tenham constituído como factor de risco.

A cultura do medo (Furedi, 2005) dotou os governados de um pré-compreensão acerca dos fenómenos sociais altamente condicionados por perceções sociais do crime baseadas essencialmente no medo e na sensação de desordem (Santos, 2018). O nível de insegurança racionalmente percebido e projetado em diferentes situações e a resposta emocional à possibilidade de serem vítimas de uma atividade criminosa constituem o medo nas suas componentes racionais e emocionais (Santos, 2018). Citando Ulrich Beck (2007, p. 30), na sua obra "*Sociedade de Risco Mundial: em busca da segurança perdida", o medo determina o sentimento existencial. A prioridade máxima na escala de valores é atribuída à segurança, que suplanta a liberdade e a igualdade. Verifica-se um agravamento das leis, um "totalitarismo da defesa contra os perigos" aparentemente razoável.*

Ao passo que nos crimes *offline* o medo conduz ao evitamento de situações potencialmente perigosas no dito espaço físico, no caso da cibercriminalidade o medo refletese na autoexclusão do ciberespaço, com impactos significativos na saúde, autonomia e bemestar (Poiares, 2019).

A autoexclusão torna-se especialmente preocupante nas faixas etárias mais avançadas (Susana Santos, 2018). De acordo com o *World Population Prospects: the 2017 Revision*, o número de pessoas com idade acima dos 60 anos vai duplicar em 2050 e triplicar em 2100,

passando dos 962 milhões em 2017 a 2.1 mil milhões em 2050 e a 3.1 mil milhões 2100 (Poiares, 2019), o que deixa antever enormes desafios pedagógicos às políticas públicas na área da prevenção da exclusão do digital (Santos, 2018).

Ao nível das políticas públicas de fomento da cibersegurança, podemos distinguir três grandes instrumentos: os voluntários, que passam essencialmente pelos mercados privados, as organizações voluntárias e a família/comunidade; os instrumentos combinados, como a pedagogia (por meio de campanhas de consciencialização e ciberhigiene), os subsídios e os impostos; ou os chamados instrumentos compulsórios, que passam pela regulação e provisionamento direto (Santos, 2018).

Quanto às ações de mitigação de cibercrimes, estas podem passar por:

- *Ações de prevenção,* que sustentam a redução do risco com medidas que reduzam a frequência e/ou a magnitude dos ataques (p. ex... *firewalls*[1], ferramentas antivírus, encriptação etc.);

- *Ações de resposta*, que implicam um controlo do risco com o objetivo de redução da frequência e/ou magnitude das perdas (p. ex., processos de *Disaster Recovery*, sistemas de *failover* e *backups* frequentes);

- *Ações de aprendizagem,* que avaliam o risco e permitem aprender sobre a frequência e/ou magnitude das perdas (p. ex.,. sistemas IDS configurados com base em dados estatísticos, análise/auditorias de *logs*, scans/auditorias de sistema, *aprendizagem bayesiana* com dados de amostras pós-auditorias).

A cultura do medo fabrica contextos criminais que acabam por prejudicar a racionalidade científica das políticas criminais. Wall (2008) aponta a discrepância entre a elevada publicidade conferida ao cibercrime nos *media* e o baixo número de casos reportados nas instâncias formais de controlo.

O autor avança com três causas explicativas: a fabricação de narrativas por parte dos *media*, que acaba por criar e reforçar o sentimento de ameaça iminente; a ineficácia policial no combate à cibercriminalidade e o desconhecimento de particularidades do fenómeno

[1] Um firewall trata-se de um software que permite a passagem seletiva do fluxo de informação entre uma rede interna e a rede pública, assim como a neutralização das tentativas de penetração abusiva nas redes privadas.

cibercriminal que, segundo o autor, poderá conduzir a uma má filtragem da informação por parte dos meios de comunicação social.

Tal como demonstrado por Bryan Wynne, muitas vezes o conhecimento público dos riscos não é, obviamente, um conhecimento de peritos, mas sim de leigos ao qual foi negado reconhecimento social (Beck, 2007). Citando Beck (2007, p. 170), *sublinha-se que o conhecimento (de leigos e peritos) acera dos riscos globais não é, de modo algum inequívoco. Refere-se a acontecimentos futuros, ainda não ocorridos, portanto, utiliza afirmações que não podem ser confirmadas nem refutadas atualmente. Por conseguinte, os críticos chamam repetidamente a atenção para discrepâncias entre o nível de conhecimento real e a dramaturgia pública dos perigos e das crises.*

Numa perspetiva construtivista social, descrita por Ulrich Beck (2007) a propósito da construção das diferentes narrativas em torno da ameaça ecológica mundial, a formação de uma opinião pública mundial consciente dos perigos do cibercrime não resulta inteiramente da globalidade dos problemas (diagnosticados pelas Ciências Sociais, e em especial pela Criminologia), mas sim de coligações discursivas transnacionais que colocam os riscos do cibercrime na agenda pública.

Sutherland (2018) chama à atenção para a necessidade de o combate ao cibercrime incluir as agências privadas. O autor refere que, por vezes, interesses comerciais por parte das agências privadas acabam por impedir um combate mais contundente.

O mesmo autor, na sua descrição de diferentes estratégias nacionais de combate à cibercriminalidade, refere a urgência no estabelecimento de parcerias de cooperação entre governos, empresas e universidades.

O estudioso aponta a relutância de muitas empresas no fornecimento de informação a instâncias governamentais como um dos entraves para a criação de redes eficazes de combate à cibercriminalidade, sugerindo o aproveitamento de mecanismos de *governance* de outras áreas, já devidamente sedimentados, para as políticas da cibersegurança.

Torna-se cada vez mais difícil instituir mecanismos de *criminal compliance* eficazes no seio das próprias empresas. Busato (2018) aponta a crescente subalternização do poder político ao poder económico, cuja dependência dificulta a criação de mecanismos autorregulatórios de prevenção da cibercriminalidade.

Um estudo realizado pelo Max-Planck-Institut aponta que mais de 80% dos delitos socioeconómicos são cometidos através de empresas (Busato, 2018).

Busato (2018), sugerindo Beck na sua obra póstuma *The Metamorphosis of the world: How climate change is transforming our concept of the world*, refere que a profusão da criminalidade organizada pelas empresas alterou o modelo criminológico do crime grave. A mutação sugerida por Beck (2016), refere Busato (2018), passa pelo predomínio de crimes cujos efeitos se produzem de modo massivo, atingindo grandes grupos de pessoas, cometidos por várias pessoas, sucessiva ou cumulativamente, com recurso a uma planificação decorrente da organização de atividades empresariais.

Por isso mesmo, e como afirma Sutherland (2018), a digitalização do crime tem de ser acompanhada pela digitalização do sistema de justiça, caso contrário os meios de investigação ao dispor nunca conseguirão acompanhar a capacidade de reinvenção que a utilização das novas tecnologias possibilita às redes criminais organizadas. Citando o autor (2018, p. 9), *while the digitalization of crime is proceeding apace, the digitalization of criminal justice systems is lagging behind. As with defence, it requires transformation of the system and reskilling of the work force, including judges and prosecutors. In order to remain trusted and to police by consent, it is necessary for police officers to be fully engaged in a digital world.*

Ora, a OTAN aponta precisamente a capacidade de afetar um conjunto de alvos alargado como uma das cinco razões pelas quais os ataques no ciberespaço podem constituir-se como uma forma viável de cometimento de ataques terroristas (Amador, 2014)

É feitiço (ou talvez não) que as políticas em torno da cibersegurança hajam começado em 2003 nos EUA na Administração Bush com a constituição da *National Strategy to Secure Cyberspace* (Sutherland, 2018), momento histórico-político fértil para cavalgadas securitárias. Por isso mesmo, a objetividade dos discursos poderá ter ficado comprometida desde a sua raiz.

As diferentes construções sociais da realidade em torno de um fenómeno social, ensina Beck (2007, p. 174), distinguem-se de acordo com os níveis de "realidade" que possuem: quanto mais próximas das instituições e quanto mais integradas nas mesmas (no sentido de institucionalização de práticas sociais), tanto mais poderosas, tanto mais próximas das decisões e das ações – e tanto mais "reais" se tornam ou parecem ser. O autor sugere que, *o "em si" da realidade, na dinâmica da sociedade de risco mundial, que dissolve tudo em decisões, surge a partir de estruturas de ação, de rotinas- inveteradas- de decisão e de trabalho, nas quais os modelos de perceção são "concretizados" ou transformados (...) deste modo, a aparência de*

construção é destruída, de forma (mais ou menos) refletida e poderosa, e cria-se a aparência do "em si".

A construção discursiva em torno das ameaças iminentes, e à escala global, produzida pelos *mass media*, legitima uma atuação por parte dos Estados no sentido de minimizar os perigos, devolvendo a segurança perdida aos cidadãos. O que em primeiro lugar fora burilado cuidadosamente na esfera comunicativa para ser consumido em massa, – muitas vezes contruído para vender , de modo a satisfazer a urgência do lucro económico e os problemas de financiamento com o qual se defrontam a maioria dos meios de comunicação tradicional –, e cuja estética teatral do relato jornalístico passa pela ênfase dos aspetos catastróficos, que reforçam os perigos do cibercrime e as ameaças pendentes que assolam a sociedade civil, rapidamente passa para a esfera institucional como insegurança percebida.

Deste modo, a construção de políticas públicas de matriz mais securitária (ou de pendor menos liberal, como preferirmos), encontra na insegurança socialmente construída a legitimidade da sua constituição, validando, as mais das vezes, fortes restrições ao nível dos direitos fundamentais – que em matéria de cibercriminalidade acabam por se refletir nas menores exigência probatórias ao nível do Direito Processual material e numa menor proteção em matéria de proteção de dados pessoais (Sutherland, 2018).

Neste sentido, os princípios de autonomia, poder de decisão, escuta do sábio pelo político, e comunicabilidade devem servir de bússola na orientação das políticas criminais e no combate ao famigerado "populismo penal" (Agra, 2012).

2.3 - Cibercriminosos

A investigação acerca da personalidade distingue essencialmente dois momentos: o estudo da personalidade no momento da passagem ao ato e a formação da personalidade do delinquente, e o estudo dos fatores do seu desenvolvimento (Agra, 2010).

Na esteira do pensamento de R. Gassin, e enquadrado num movimento mais amplo apelidado de "positivismo psicológico", o estudo com enfoque no delinquente parte de um esquema causal que relaciona a noção de perigosidade com a noção de personalidade.

Este ramo da Criminologia, que mais tarde viria a entroncar no chamado "neopositivismo criminológico", coloca o enfoque metodológico nos traços ou caraterísticas biológicas, psicopatológicas, psicossociais ou num conjunto de um conjunto de traços estruturados (o chamado conceito do "nó central da personalidade criminal" de J. Pinatel) (Agra, 2010).

À abordagem unifatorial do positivismo, cuja premissa assenta na ideia de que o fenómeno criminal resulta essencialmente de uma observação psicológica, a abordagem multifatorial viria a acrescentar que a explicação psicológica não se limita à causalidade positivista.

Numa crítica ao positivismo clássico, na obra *Entre a Droga e o Crime*, Cândido da Agra (2008, p. 65) explica: *o estudo sobre os modos de explicação científica em geral, revelamnos, numa perspectiva muito panorâmica, que a história da ciência se deslocou de formas elementares e simples de explicação (que mais não eram que simples descrição) para formas actuais caraterizadas pela complexidade. A explicação causal, que prevê relações diretas entre dois fenómenos, de tipo A -B, ou, às mesmas causas sucedem os mesmos efeitos, é um dos exemplos de explicação simples, quase confinado à caraterização de relações físicas fortemente determinísticas. Poucos serão os fenómenos que estarão ligados de maneira estritamente causal, mesmo na natureza.*

No estudo da ligação da cibercriminalidade com a dita criminalidade "terrestre", no que concerne à carreira criminal dos delinquentes, Sanford Sherizen (1990) avança com dois tipos de cibercriminosos. O autor sugere que um tipo de cibercriminosos tende a avançar dos crimes tradicionais para o cibercrime, ao passo que o outro tipo comete vários tipos de cibercrimes.

A interação entre transgressor e vítima revela-se de difícil estudo, dada a dificuldade de incluir nos estudos empíricos os ofensores (Jaishankar, 2018). Mcguire e Dowling (2013) apontam para uma interação entre agressores e vítimas muito distinta dos padrões convencionais do crime *offline*.

Roderic Broadhurst *et al.* (2014) sugerem que, apesar das motivações no cibercrime serem bastante heterogéneas, evidências empíricas demonstram que a motivação dominante nos cibercriminosos é o lucro financeiro. Os autores fornecem um conjunto de exemplos variados de cibercrimes de contornos mediáticos, indicando um amplo conjunto de motivações muito díspares entre si.

No esqueleto dos retratos traçados pelos autores saltam à vista motivações bastante heterogéneas, que passam desde a simples vontade de competir com outros cibercriminosos, até motivações ideológicas.

O perfil típico do cibercriminoso, extraído de estudos sobre a tipologia e características dos ciberdelinquentes concluiu, segundo os dados do Sistema Estatístico de Criminalidade (SEC) do Gabinete de Coordenação e Estudos da Secretaria de Estado de Segurança (Paya Santos, Cremades Guisado & Delgado Morán, 2017), que 76% dos detidos e condenados por crimes cometidos no ciberespaço são homens, cujos delitos passam essencialmente por crimes sexuais e interferência em dados do sistema, sendo que nos casos de delitos de falsificação informática e fraude informática se regista uma menor participação destes.

O estudo realizado revela que se trata essencialmente de uma criminalidade jovem, maioritariamente masculina e com um certo grau de conhecimentos: 76% dos ciberdelinquentes são homens com as idades compreendidas entre os 14 anos (8%) e os 50 anos (11%), sendo que a idade média corresponde a 35 anos.

Segundo Sergio Cámara Arroyo (2020), um cruzamento deste levantamento com outras investigações indica que se trata de uma carreira criminal que tende a iniciar na juventude, em redor dos 11/12 anos de idade.

O perfil jovem do ciberdelinquente apresenta-se como produto inacabado de uma geração de adolescentes com um nível de conhecimentos tecnológicos muito acima dos padrões médios das gerações precedentes, frequentemente autodidatas e com o romantismo das gerações de *hackers* que deixaram o rasto saudosista da cultura *cyberpunk* (Wall, 2008).

Apesar do imaginário da figura do *hacker* solitário, cuja primeira onda de representações sociais se pautou por elevados níveis de moralidade – que viriam a decrescer ao longo das

gerações subsequente (Wall, 2008) –, a sua figura, apesar de cada vez mais distante da grossa fatia da cibercriminalidade, acabara por absorver a população mais jovem na busca de reconhecimento e fama.

Neste campo, teorias de cariz mais sociológico, com enfoque na cultura de valores dominante, poderiam servir de base a futuros estudos explicativos das causas do percurso delinquente juvenil prematuro; pensamos essencialmente na teoria de Sutherland, segundo a qual o comportamento é aprendido ao longo de trocas interpessoais (Cusson, 2006).

A imitação e o comportamento desviante, no caso da ciberdelinquência precoce, surgem essencialmente por meio da socialização primária (Berger & Luckmann, 2010). Os processos de socialização primária refletem o estádio crucial de construção da identidade – enquanto relação dialética entre a identificação dos outros e a autoidentificação – e o momento a partir do qual o indivíduo é introduzido ao mundo objetivo da sociedade (Berger & Luckmann, 2010).

Um perfil criminal iniciado em tão tenra idade deixa antever na relação triangular sociedade-identidade-realidade padrões normativos interiorizados marcados pelo esvaziamento ético da maioria dos comportamentos desviantes cometidos no ciberespaço.

A fluidez da interseção no ciberespaço, marcado pela alternância entre comportamentos desviantes como *cyberstalking*, *sexting*, e delitos contra a propriedade intelectual, o reforço desses comportamentos por parte dos grupos primários como a família e grupos de pares, a incapacidade de percecionar de forma líquida os efeitos nocivos da atividade delinquente e a possibilidade de recorrer ao anonimato como forma de garantir maior segurança contribuem decisivamente para uma falta de consciência da danosidade social e individual dos atos cometidos no espaço digital.

Fanjul Fernandez & ESERP Business School (2018) concluíram, no seu estudo acerca da ciberdelinquência, que os ciberdelinquentes devem ser diferenciados pelo nível de *expertise* no manuseamento das tecnologias de informação. Os autores distinguem os delinquentes entre aqueles que apresentam uma grande facilidade de manuseamento e se revelam amplos conhecedores dos sistemas de redes, daqueles cujos conhecimentos e habilidades se apresentam como rudimentares ou suficientes.

Os investigadores concluem que os níveis de especialização apresentados assumem impacto primordial no tipo de crimes cometidos no ciberespaço: enquanto os primeiros procuram a aquisição de conhecimentos específicos, muitas vezes tendo como simples motivação o desafio intelectual de conseguir *hackear* um sistema de alta segurança, os segundos

são movidos essencialmente pela obtenção de lucro económico, a vingança pessoal ou a busca de prazer sexual.

Roderic Broadhurst *et al.* (2014) referem no seu estudo acerca da natureza dos grupos envolvidos no cibercrime um conjunto de exemplos de ciberdelinquentes altamente especializados cujo perfil, quanto à competência técnica, enquadra-se no primeiro tipo descrito por Fanjul Fernandez (2018).

Os casos de Edward Pearson, que furtou 8 mil milhões de identidades, 200. 000 contas PayPal e 2700 números de cartão de multibanco e de Aaron Swartz, um programador e associado na Universidade de Harvard que fora condenado em 2011 pela descarga de 4 mil milhões de artigos académicos da base de dados do Massachussets Institute of Technology (MIT), parecem enquadrar-se no primeiro retrato definido por Fanjul Fernandez (2018): após investigações, conclui-se que em ambos os casos o lucro nunca fora o móbil central da atividade criminosa; viera a provar-se que o acesso ilegítimo a bases de dados e o roubo de identidade surgira de motivações ideológicas ou fruto do mero desafio intelectual.

Sergio Cámara Arroyo (2018), na leitura que faz dos dois tipos de perfis técnicos descritos nos parágrafos antecedentes, distingue ambos os perfis na relação da atividade criminosa com o objetivo prosseguido: o primeiro tipo, o perfil mais especializado e com um conhecimento mais aprofundado das novas tecnologias , tende a valorizar o aspeto virtual do próprio ataque para lá da prossecução do objetivo criminoso, ao passo que o segundo secundariza o processo e as suas especificidades virtuais, determinado somente pelo alcance do objetivo criminoso.

O aspeto cultural poderá em parte revelar-se uma determinante útil no estudo da cibercriminalidade. A maior parte dos estudos realizados sobre o perfil do cibercriminoso fazem coincidir o perfil do cibercriminoso com o género masculino. Outros autores (Miró Llinares 2012; Fanjul Fernández *et al*., 2018) agrupam o perfil dos cibercriminosos baseados na tipologia do delito cometido. Neste seguimento, definem o cibercriminoso baseado no tipo de delito cometido, agrupando em três tipos:

- O *cibercriminoso económico*, que tem como principal motivação a obtenção de lucro económico, alcançado diretamente através do ataque, ou indiretamente nos casos em que o ganho surge de uma recompensa paga pelos grupos organizados a quem prestou os serviços (Sérgio CámaraArroyo, 2018); neste grupo, o perfil divide-se entre aqueles que trabalham nas

instituições ou empresas vítimas da infração (os chamados *insiders),* e os que não pertencem às organizações;

- O *cibercriminoso político*, cujo perfil se enquadra na categoria do *cyberhate* e do *hacktivismo* (MiróLlinares, 2011);
- O *cibercriminoso social*, enquanto categoria bastante heterogénea e difusa, cujo bem jurídico protegido não é económico nem político e que incluem os *cyberstalker*, *cyberbuller*, *groomers*,etc. (MiróLlinares, 2011).

A presença de traços patológicos neste tipo de delinquência não é tão frequente como na maior parte da delinquência tradicional. Porém, o traço psicopatológico mais frequente neste tipo de criminoso é a paranoia, causada pelo medo constante da detenção (Sergio Cámara Arroyo, 2018). Cremos que a ténue distinção entre o *online* e o *offline* favorece o constante estado de alerta a que os criminosos do ciberespaço estão submetidos, em comparação com os criminosos ditos "tradicionais".

CAPÍTULO III - Caraterização do estudo

3.1- Objetivos (gerais e específicos)

Pretendemos com o presente estudo explorar as dinâmicas organizacionais do cibercrime, argumentando que o recurso ao modelo de organização em rede é aquele que melhor se adequa ao estudo da cibercriminalidade organizada e que o processo de desenvolvimento das redes do cibercrime organizado tenderá a assumir um esquema organizativo marcado pela dispersão e descentralização dos seus componentes – tendência que, partindo da tipologia estabelecida por Mcguire (2012), apelidamos de *swarmização*.

A presente tese segue a linha do estudo taxonómico efetuado por Mcguire (2012), cuja classificação retomamos no capítulo conclusivo com o objetivo de propor um modelo de interpretação das dinâmicas organizacionais dos grupos cibercriminosos que possa servir de modelo para futuras investigações empíricas.

Com o modelo de organização em rede pretendemos argumentar, partindo da tipologia estabelecida por Mcguire (2012), que as redes organizadas cujas atividades se pautam maioritariamente pela atividade *online* tenderão a assumir a estrutura organizacional típica dos *swarms* – organismos criminosos dispersos que se desenvolvem de forma descentralizada e flexível.

Sintetizando, o nosso estudo pretende sugerir a existência de uma tendência para a organização em rede do cibercrime organizado, em contraste com o modelo piramidal de topo para a base (Agra, 2018), cujas dinâmicas organizacionais refletem o desenvolvimento de "nós para nós" em relação lateralizadas e com uma tendência crescente para o esboroar das relações hierárquicas.

Aquilo a que chamamos na síntese conclusiva de *swarmização*, enquanto tendência para os organismos que operam maioritariamente no espaço *online* assumirem a composição organizacional típica dos grupos apelidados por Mcguire (2012) de *swarms,* projeta o desenvolvimento futuro em moldes semelhantes de outras redes de cibercrime organizado (tais

como os *hubs* (assumindo a terminologia proposta por Mcguire, 2012). Falamos de um padrão de expansão que indicia a *swarmização* futura de outras redes de cibercrime organizado.

O processo de *swarmização* a que fazemos alusão reflete a composição orgânica avançada em estudos empíricos (Leukfeldt *et al*., 2016), cujo retrato aponta para a emergência de novos atores periféricos no mundo da cibercriminalidade.

Com o modelo de organização em rede emerge o perfil do cibercriminoso empreendedor (Cruz *et al*., 2015), numa relação de bicondicionalização.

A semelhança apontada pela literatura entre o criminoso de colarinho branco e o cibercriminoso (Sherizen, 1990) remete para o estudo de um perfil do cibercriminoso como indivíduo autónomo da organização, cuja mentalidade inovadora – fruto das suas competências técnicas e do seu perfil intelectual tendencialmente sofisticado (Fanjul Fernandez, 2018) – sugere uma tendência para procurar ligações criminais laterais que lhe permitam potenciar os seus ganhos financeiros. Enquadra-se, na tipologia de Miró Llinares (2012) e Fanjul Fernández *et al.* (2018), no perfil de cibercriminoso económico (referenciado no capítulo precedente).

Com o modelo de organização proposto e numa relação dialética de recíproca influência, cremos que o cibercriminoso inserido no cibercrime organizado deverá ser assemelhado ao criminoso de colarinho branco empreendedor, dada a sofisticação do seu guião criminoso, a sua sofisticação técnica e o guião criminoso altamente complexificado.

Deste modo, pretendemos propor um modelo explicativo baseado nos seguintes vértices:

i) os modelos de organização em rede apresentam-se como o referencial teórico mais adequado para a compreensão das dinâmicas organizativas da cibercriminalidade organizada, ao invés do modelo piramidal e tendencialmente burocrático;

ii) a tendência futura das organizações criminosas que operam no ciberespaço será assumirem um esquema organizativo disperso e descentralizado, cujo modelo de distribuição assume o esquema figurativo dos *swarms* (segundo a tipologia elaborada por Mcguire, 2012);

iii) o esquema de organização em rede é produto e produtor de um ciberdelinquente cujo referencial normativo assenta nos valores do empreendedorismo.

3.2- Estrutura da tese

Após a revisão de literatura efetuada no capítulo segundo, segue-se uma apresentação dos conteúdos chave que servirão de base para os objetivos de investigação. O capítulo quarto servirá uma breve exposição de algumas teorias da sociologia das organizações (ponto 4.1), seguida de uma incursão pelas teorias de crime organizado (ponto 4.2) e cibercrime organizado (ponto 4.3). A exposição das duas últimas temáticas (pontos 4.2 e 4.3) baseia-se essencialmente numa revisão de literatura adequado ao objetivo do nosso estudo. O capítulo quinto assenta numa proposta explicativa do cibercriminoso empreendedor com base nas semelhanças entre o cibercriminoso e criminoso de colarinho branco cujo perfil cremos ser produto e produtor de um processo de *swarmização* dos organismos criminosos.

No capítulo sexto, mais concretamente no ponto 6.2, desenvolveremos os três objetivos referenciados, não sem antes proceder a uma breve exposição dos conceitos de organização em rede (a que corresponde o ponto 6.1). Para facilitar o encadeamento da síntese conclusiva com a exposição dos modelos de organização em rede, optámos pelo enquadramento conceptual destes no capítulo da síntese conclusiva. Finalizaremos com uma breve conclusão a que corresponde o ponto 6.3.

Julgamos indispensável uma breve passagem por dois pontos laterais de elevada importância para os objetivos do nosso estudo: a abordagem teórica do crime organizado e a referência sociológicas de natureza teórica acerca das Organizações.

Quanto ao primeiro, duvidámos se seria adequado incorporar no capítulo quarto ou se uma breve referência conceptual no capítulo de revisão de literatura seria suficiente. Optámos pela sua integração no capítulo quarto por uma razão de coerência sistemática.

A referência às teorias criminológicas do crime organizado justifica, pela semelhança do objeto, o seu emparelhamento com as abordagens empíricas do cibercrime organizado. Permite-se desta forma uma melhor incursão sobre a temática geral das organizações criminosas, completando as abordagens do cibercrime organizado com considerações gerais acerca da criminalidade organizada que julgamos enriquecerem a compreensão do leitor.

A inclusão de algumas considerações da Sociologia das Organizações do ponto 4.1 justifica-se em função de três objetivos:

i) Integrar na explicação do processo de *swarmização* dos organismos criminosos uma lente teórica que relaciona o desenvolvimento das dinâmicas organizacionais com as alterações tecnológicas oriundas do ciberespaço e que servem de pano de fundo à sua atuação;

ii) Evidenciar a ancoragem das transformações nas organizações num plano sociocultural que sugere um perfil do cibercriminoso altamente influenciado pelos valores pós-modernistas; iii) Relacionar o pano de fundo sociocultural com o processo de *swarmização e* o perfil do cibercriminoso empreendedor.

Por isso mesmo, a referência a Weber e Elton Mayo no capítulo conclusivo impõe a breve incursão do ponto 4.1.

CAPÍTULO IV - O crime organizado e o cibercrime organizado

4.1.- A Sociologia das Organizações

Na história do pensamento sociológico a ideia de organização tem-se revelado um tema profícuo, ponto de partida e chegada para muitas das reflexões acerca do Homem e da sua relação com o Social.

A abordagem inicial ao fenómeno, de um ponto de vista sociológico, foi feita por Marx e Engels, que consideravam todo o tipo de organizações sociais e económicas iminência direta do estado das forças produtivas, presente ao nível da infraestrutura.

Para Marx, o conflito interno de forças presente nas organizações apenas poderá ser compreendido por meio da análise do conflito macro presente na sociedade, que se expresso nos antagonismos entre o valor da força de trabalho e o valor da propriedade privada (Aron, 1970).

No seguimento da visão marxista das organizações, Durkheim introduz a noção de divisão do trabalho como fonte geradora de solidariedade e maior integração social. A nova divisão do trabalho pauta a solidariedade orgânica presente na sociedade moderna. O autor chama a atenção para o facto de as modernas configurações do trabalho, - caraterizadas pela hierarquia, especialização e dependência funcional – serem fontes geradores de tensões sociais (aquilo a que o autor denomina de anomia). Deste modo, a anomia deverá ser combatida pela introdução e reforço de novos valores morais, de forma a permitir que a nova configuração individualista do ser humano na sociedade seja acompanhada de uma rede de valores que permita a sua total integração no seio da solidariedade orgânica. A procura coletiva de individualização desenvolve uma moral numa historicidade que é essencialmente cultural (Norbert Elias, 1980).

O tema das organizações fora posteriormente desenvolvido mais intensamente por Max Weber. O autor, alicerçado na ideia de poder enquanto probabilidade de um ator, numa relação social, estar em posição de impor o seu desejo (Henriques, 2014), endereça o tema das organizações por meio dos conceitos de autoridade carismática, tradição e normas legais.

A burocracia moderna pressupõe a hierarquização dos relacionamentos, compatibilizados por atividades quase mecânicas dos membros das organizações, e que obedecem a comandos piramidais rigidamente definidos.

A especialização em Weber surge como resultado direto do processo de burocratização do real, que permite a dominação por meio da integração dos conflitos internos, e que revela a natureza impessoal das relações enquanto mecanismos de intersubjetividade que fortalecem o valor normativo da meritocracia.

No contexto da dominação burocrática, verifica-se uma constante tensão entre a descentralização nas estruturas, enquanto modelo organizacional associado a uma maior democraticidade, e o modelo de cariz mais autocrático, capaz de uma governação autónoma face a condicionalismos socioculturais externos, e que se carateriza essencialmente por organismos centralizados, com chefias reforçadas e relações hierárquicas bem definidas (Henriques, 2014).

Para Weber, de forma resumida, o tipo ideal, – enquanto síntese ideal que norteia a análise empírica, mas que com ela se não confunde – de dominação burocrática contém em si quatro elementos distintivos: 1) - estrutura hierárquica da autoridade; 2) – especialização; 3) - recrutamento com base em conhecimentos técnicos; 4) - relações impessoais.

Weber, referindo-se várias vezes ao seu conceito de tipo ideal, ressalva o facto de o tipo ideal ser apenas um referencial analítico, que não poderá dispensar a construção de modelos com base nas particularidades empíricas do objeto de estudo (Manheim, 1966/1940).
Citando Henriques (2014, p.17):

(..) admitimos que o tipo ideal de Weber possa, no entanto, evoluir e incluir outras caraterísticas que, ao nível da sociedade se revelem, por força da evolução da própria sociedade. A título de exemplo, a globalização de mercados e comunicações dos últimos vinte a trinta anos coloca questões relativas a uma lógica de relação de serviço que abrange todas as organizações de serviços ou industriais, com vista ao usufruto adequado pelos clientes. Esta "servicilização" pode ser entendida como uma caraterística a incluir no tipo ideal, o que não impede que, empiricamente, o como e até a própria existência da caraterística.

A relação entre o meio social, produtor de normas e valores externas à organização da estrutura, e a organização foi objeto de amplo debate pelos autores clássicos. Num contexto de

análise que tinha como pano de fundo a ampla obra de Weber, Robert Michels estudou os partidos políticos enquanto forças organizativas que, segundo o autor, tendem naturalmente para a composição oligárquica.

A radical funcionalização da existência, que remete o indivíduo para as amarras da organização revela, muitas vezes, processos desviantes no seio dos quais as subjetividades chocam com a racionalidade das organizações. Por isso mesmo, desde cedo os trabalhos sociológicos incentivaram o questionamento acerca das relações de poder no seio das organizações, centro a partir do qual se pode observar o florescer de significações coletivas ou legitimações como formas de justificar e reforçar a dominação e a coerção (Henriques, 2014).

É precisamente nesse ponto central das relações que melhor observamos noções tais como lealdade, confiança e envolvimento, que emergem de contextos socioinstitucionais amplos para dar significado à intersubjetividade organizacional, e que por sua vez influenciam esses mesmos contextos macro.

Fayol (1949), ao contrário de Marx, alargou o seu objeto de estudo das organizações no contexto de processos produtivos para as funções administrativas e de gestão, estabelecendo os princípios básicos aplicáveis a todas as organizações. Segundo Fayol (1949) os princípios a serem aplicados são: a unidade de controlo; a especialização; e a delegação limitada (Henriques, 2014).

Partindo da ideia de Pareto, de que os equilíbrios nos grupos sociais se revelam frutos de ajustamento a processos de desequilíbrio resultantes de mudanças sociotécnicas, Mayo assumiu papel de destaque na evolução da teoria das organizações a partir da teoria da gestão científica do trabalho. Para Mayo, a organização interna emerge da relação tensional entre a formalidade das regras e a informalidade das interações (Henriques, 2014).

No contexto das organizações, as investigações empíricas focaram-se na integração grupal, constituindo a organização formal a variável externa. Para Mayo, as regras internas da organização encontram-se numa relação dialética com os valores que os indivíduos trazem consigo; a harmonia e a cooperação surgem no ponto ótimo de interseção entre ambas, que permite integrar as condicionantes normativas externas nos objetivos coletivos internos.

Posteriormente, viria a Escola de Chicago atribuir maior destaque aos fatores sociais externos à organização. A importância atribuída por autores como Whyte (1951) às mudanças sociais e tecnológicas externas enquanto determinantes da cultura grupal veio a salientar a

importância de analisar o comportamento numa perspetiva cada vez mais holística (Henriques, 2014).

O papel atribuído à observação processual, preocupada com a observação e análise da integração das mudanças na relação com a base tecnológica e com as caraterísticas dos indivíduos, viria a caraterizar grande parte dos estudos efetuados pela Escola de Chicago no campo das organizações. Citando Henriques (2014, p. 20-21):

Whyte, depois dos anos de 1940, utilizou entrevistas para pesquisar todas as forças que influenciam o comportamento nas organizações e refere os comportamentos individuais como resultado de situação imposta pela estrutura da organização, em que esta influência e é influenciada pela tecnologia, e em que várias disciplinas (economia, contabilidade de custos) são chamadas a dar contributo.

4.2.- O crime organizado

A generalização da forma económica do mercado, no contexto atual da sociedade em rede, funciona como princípio de inteligibilidade, princípio de explicação das relações sociais e dos comportamentos individuais.

Significa que a análise em termos de economia de mercado, de oferta e de procura, vai servir de esquema que se pode aplicar a domínio não económicos.

Graças a este esquema de análise, a esta grelha de inteligibilidade, vai poder-se fazer aparecer em processos não económicos, em relações não económicas, em comportamentos não económicos, certo número de relações inteligíveis que não se apresentariam como tais - uma espécie de análise economista do não económico, disse-o Foucault (1979), na lição de 21 de março de 1979, a propósito da introdução à abordagem do *homo poenalis* e dos mecanismos economicistas das penas esboçados nos finais do século XVIII e inícios do século XIX.

Certamente não a pensar no crime organizado enquanto forma de organização empresarial das atividades criminosas, Foucault ensaia, com a fecundidade que lhe é caraterística, um conjunto de pensamentos pertinentes para fenómenos que, em parte, ultrapassam a literalidade dos seus enunciados.

A Convenção de Palermo refere que para ser considerado crime organizado exige-se uma composição mínima de três membros (Leal, 2018). Excetuam-se, no caso da legislação portuguesa, os tipos construídos antes de 2004, constituindo exemplo paradigmático as associações criminosas previstas na legislação do combate ao tráfico de droga, bem como as organizações terroristas, que exigem apenas um mínimo de dois membros (Leal, 2018).

De acordo com a definição proposta pela União Europeia , *a Criminal Organization means a structured association, established over a period of time, of 2 or more persons, acting in a concerted manner with a view to committing offences which are punishable by deprivation of liberty or a detention order (...) whether such offences are an end in themselves or a means of obtaining material benefits and, where appropriate, of improperly influencing the operation of public authorities* (Carrapiço, 2005 p.178).

No caso de cibercriminalidade organizada, alguns autores sugerem que a mobilização de vários *bots*[2] por um único servidor poderá ser considerado crime organizado (Chang, 2012).

Consideramos, em nosso juízo, que os conceitos jurídicos devem estar em constante atualização, sob pena de se cristalizarem em universos concetuais afastados das realidades socio criminais complexas e em constante mutação.

Cândido da Agra (2018) enquadra o crime organizado na ideia de um modelo de organização hierárquico, composto número de pessoas elevado desde o topo até à base, cujas atividades económicas implicam relações contínuas entre pessoas e em que o sucesso envolve, em alguma medida, um certo grau de corrupção ou intimidação dos agentes do controlo social formal.

No seguimento da sua reflexão acerca do crime organizado propõe uma taxonomia baseada nos ensinamentos de Marcus Felson (2002), erigindo os conceitos de "cadeias de informação" e "rede ilícita" como parte integrante do núcleo essencial explicativo do fenómeno do crime organizado.

De acordo com Kleemans (2014), existem diferentes teorias explicativas do crime organizado. O autor atribui especial destaque a três:

i)- a *allien conspiracy model*, que considera o modelo de crime organizado uma conspiração de grupos exteriores às sociedades democráticas abertas;

ii)- o *modelo burocrático*, que afirma a similitude dos modelos de organização à formalidade das burocracias (ver referências a Weber no capítulo precedente);

iii)- e o *modelo tipicamente empresarial*, que assume os criminosos como verdadeiros empresários do crime, indivíduos calculistas e que operam de forma muito similar às empresas de mercados legais.

O primeiro modelo, denominado *allien conspiracy model*, é um produto teórico historicamente atribuído às estruturas policiais da sociedade americana dos meados do século

[2] A palavra *bot* é utilizada como diminuto de robot, também conhecido como internet *bot* ou *web robot*.

XX, elaborado no decurso do debate público acerca do domínio da sociedade por parte de grupos italo-americanos da máfia.

Este modelo explicativo assume o crime organizado como o resultado importado de grupos externos à sociedade: as contingências históricas do modelo remetiam a causa do surgimento do crime organizado para as vagas de imigração de cidadãos italianos dos finais dos anos noventa e inícios dos anos 2000 (Kleemans, 2014).

O modelo conspirativo proposto complementa-se frequentemente com outros fatores explicativos, tais como algumas das caraterísticas do modo de organização burocrático e a prevalência de elevada homogeneidade étnica enquanto fator justificativo da coesão dos organismos criminosos (Kleeman, 2014).

A variante conspirativa, apesar de arrogar para si a natureza analítica de uma teoria criminológica explicativa do fenómeno do crime organizado, acaba por assumir um cariz marcadamente ideológico; de pendor essencialmente político, este padrão explicativo, julgamos nós, poderá, se a ele recorrermos frequentemente para explicar o fenómeno da criminalidade organizada, desaguar num discurso político próximo do conceito de inimigo formulado por Carl Schmitt (1963), e que em termos normativos veio a originar construções jurídicas a que se atribui o desígnio de "Direito Penal do Inimigo".

O segundo tipo sugerido por Kleemans (2014) é o modelo burocrático. Com origem nas confissões proferidas pelos membros da máfia, particularmente desenvolvido por Cressey (1969) no seu livro "Theft of the nation", a estrutura organizacional dos grupos criminosos é frequentemente assemelhada às estruturas caraterísticas das organizações burocráticas (Kleemans, 2014).

Podemos, segundo este modelo, definir a organização criminosa com recurso a cinco caraterísticas: a existência de uma organização piramidal, em contraste com as organizações em rede, na qual as estruturas de poder de desenvolvem de forma vertical ; a presença de uma distribuição hierárquica estrita dos seus membros ; a clara divisão de tarefas, que atribui maior impessoalidade às relações entre os seus membros ; a presença de códigos de conduta vincados, formalmente definidos e o reforço desses mesmos códigos por meio de sanções externas e internas.

Kleemans (2014), na sua crítica à explicação baseada na burocracia, considera que em muitos tipos de crime o modelo de organização burocrática acaba por ser a exceção e não a regra.

Da nossa parte, julgamos ser a cibercriminalidade organizada um caso em que organização hierárquica constitui a exceção e não a regra - para mais, justificaremos no último capítulo.

Alguns autores, a que Kleemans (2014) faz referência, tais como Paoli (2003), consideram que grupos como a máfia devem ser vistos mais como sociedades de fraternidade, com os seus rituais de iniciação, do que propriamente grupos que se regem pelo modelo de organização burocrática.

O terceiro modelo explicativo parte da similitude entre as formas de organização empresariais das atividades legais com as estruturas organizativas das células criminosas. Segundo este modelo, os membros das organizações são vistos como normativos e racionais: verdadeiros empresários do crime orientados para o cálculo económico do custo-benefício (Kleemans, 2014).

Neste sentido, boa parte das explicações destes fenómenos reconduzem-se a taxonomias derivadas da Economia e da Gestão, salientando com especial acuidade as caraterísticas pessoais dos empreendedores do crime (Neves, 2020)

Não obstante, alguns autores apontam falhas na transposição baseada no modelo empresarial para os crimes organizados, fruto das particularidades do mercado ilegal. Para autores como Reuter (1983), referido por Kleemans (2014), constrangimentos do mercado ilegal tais como a probabilidade de membros dos grupos serem presos, bem como contrariedades típicas das atividades criminosas – que constantemente necessitam de ajustar os seus calendários às estratégias mais eficazes de escapar às malhas dos controlos sociais formais e informais –, acabam por revelar-se caraterísticas típicas do mundo do crime que impedem a analogia com o mundo empresarial. Apesar de sabermos, com Agra (2018), que no caso do crime organizado os controlos sociais informais acabam por ser menos eficientes, constrangimentos desse tipo não deixam de ser equacionados por esta redes criminosas.

Deste modo, Reuter (1983), citado por Kleemans (2014), prevê uma durabilidade reduzida destas organizações criminosas, concluindo que o modelo empresarial mais adequado para sobreviver à incerteza dos mercados ilegais serão organizações em pequena escala, algo que no caso da cibercriminalidade organizada vem sendo corroborado por alguns autores (ver Leal, 2018 referido no ponto seguinte).

Como teoria explicativa Kleemans (2014) sugere ainda teorias tais como a chamada *protection theory* e a explicação baseada na integração social dos membros como causa da

criação de amplas redes sociais de contactos que favorecem a emergência do chamado crime organizado.

A *protection theory* tem as suas raízes históricas no controlo quase total da atividade económica de segmentos específicos de mercado em vastas parcelas territoriais. Os grupos criminosos comportam-se como verdadeiros Estados soberanos nesses territórios, fazendo uso do monopólio da força e da prerrogativa de imposição de impostos para controlar setores de atividade altamente lucrativos. A visão da *protection theory* remete para explicações ligadas às políticas públicas, adaptadas em parte à explicação de fenómenos criminais (Kleemans, 2014).

Segundo esta teoria, a existência de mercados fracos, cuja teia de regulamentação estatal apresenta enormes debilidades, bem como a falta de provisão de bens e recursos por parte das entidades públicas, desemboca na formação de cartéis e monopólios por parte de organizações criminosas, que, tal como as empresas legais homólogas, apresentam grande resiliência e longevidade (Kleemans, 2014).

Críticos desta teoria afirmam que a capacidade das organizações criminosas para explorar as falhas de mercado não podem ser explicadas por razões de ordem económica, pois a capacidade que estas organizações apresentam deve-se essencialmente à possibilidade de utilização da violência e do poder nas comunidades para se imporem ; neste sentido, a interpretação veiculada, de que as organizações criminosas se movimentam como verdadeiras empresas (que cobram no mercado ilegal pelos serviços prestados às comunidades) deve ser olhada com alguma reserva (Kleemans, 2014), pois tende a mitigar algumas diferenças na relação empresas legais/mercado legal e redes criminosas/mercado ilegal.

Para Annelise Anderson (1995), referenciada por Leal (2018), as causas subjacentes ao aparecimento de crime organizado prendem-se essencialmente com a ausência de poder do Estado, o excesso de burocracia estatal e a proibição de determinadas atividades económicas. Citando Leal (2018, p.215):

(…) *a plasticidade do comportamento do crime organizado tende a parasitar as estruturas legítimas existentes na sociedade, aproveitando o funcionamento das atividades e dos sistemas implantados que sustentam a vida social, ora como meio para a concretização do desiderato criminoso, ora para explorar de forma direta os recursos existentes nessas atividades e sistemas, posicionando-se neste último caso de forma predatória.*

A explicação baseada na integração social parte dos vínculos sociais dos membros das redes criminosa como forma de explicar a constituição e alargamento das relações criminosas.

Nesta perspetiva, em parte, devemos analisar as relações dos membros de forma a perceber a sua origem e evolução. Por exemplo, a maior ou menor internacionalização da rede poderá ser explicada pela estrutura de oportunidades sociais de alguns dos seus membros, que permite ou não o estabelecimento de vínculos sociais com membros de outras organizações sediados noutro território.[3]

Não deixamos de salientar que no caso do cibercrime, o recurso a novas tecnologias tem vindo a revelar-se um fator decisivo para o recrutamento de novos membros e estabelecimento de novos vínculos que, cremos nós, em muitos dos casos se revelam essenciais para a sobrevivência da rede estabelecida.

A visão baseada na interação dos membros com o meio ambiente, numa perspetiva adaptativa face às incertezas típicas do mercado ilegal, sugere a existência de laços sociais frágeis e instáveis (Kleemans & van de Bunt, 1999; Kleemans, 2014).

Com uma visão de pendor mais sociológico, a investigação empírica baseia-se essencialmente na compreensão das determinantes sociais e culturais para a compreensão dos ofensores e das dinâmicas organizacionais.

Kleemans e van de Bunt (1999) cunharam o termo "social snowball effect" para descreverem a forma como os delinquentes se envolvem no crime e o modo como as suas carreiras se desenvolvem.

Citando Kleemans (2014, p. 7):

(…) *offenders get in touch with criminal networks through social relations; and – as they go along – their dependency on other´s people´s resources (such as money, knowledge, and contacts) gradually declines; subsequently they choose their own ways: they generate new criminal groups by attracting people from their own social environment, and the story begins all over again.*

[3] No caso da cibercriminalidade organizada, os estudos de Leukfeldt *et al*. (2016) referenciados no ponto seguinte são particularmente reveladores da importância do recurso à estrutura das oportunidades sociais como fator explicativo para a maior capacidade de internacionalização das redes de cibercrime. Para lá remetemos maiores desenvolvimentos.

Autores como David Whittaker e Bruce Hoffman colocam a obtenção de lucro como uma das caraterísticas centrais para distinguir o crime organizado das organizações terroristas (Carrapiço, 2005).

Num enquadramento simplificador da literatura já existente sobre o tema podemos definir os modelos tipo de crime organizado como modelos piramidais ou modelos em rede (Agra, 2018 p. 368). Os primeiros, citando o autor, *estruturam-se em planos que se sucedem, em dinâmica convergente, da base para um topo, do elemento para a totalidade.*

Apesar de compatível com a estrutura hierárquica típica do modelo de organização piramidal, o modelo de organização em rede pauta-se essencialmente pela horizontalidade e maior fluidez nas posições ocupados pelos membros integrantes da rede, quer ao nível dos cargos de poder que ocupam quer das tarefas a executar. Apesar de não mutuamente exclusivos (Agra, 2018), os modelos piramidais e os modelos em rede geram diferentes dinâmicas na organização criminosa.

Pesquisas recentes acerca do crime organizado (Waldeck Cavalcante, 2018; Leukfeldt *et al*., 2016; Leal, 2018) revelam a alta flexibilidade e a capacidade de adaptação dos organismos criminosos, sendo por isso a tendência atual a organização em pequena escala; as organizações atuais procuram evitar grandes estruturas e formalidades como forma eficiente de escapar às malhas da detenção (Leal, 2018). Voltaremos a este ponto com maior detalhe no capítulo conclusivo.

Segundo Lemieux (2003), referido por Gonçalves (2013), podem ser identificados sete papéis no seio de uma rede criminosa: o organizador, figura central da rede e que garante a direção e coordenação da mesma; o isolador, cujo papel passa por isolar o núcleo da rede do perigo e ameaças; o guardião, peça central na garantia da segurança, e auxiliar no processo de recrutamento de novos membros, assegurando todos os rituais de iniciação necessários para a integração segura dos novos recrutas; o extensor, cuja função passa pela expansão através da introdução de novos membros ou por meio do estabelecimento de conexões com outras organizações; o monitor, responsável pela eficiência da rede, e que permite o escoamento da informação até ao núcleo duro da organização, sendo também encarregado de garantir a adaptação face a novas circunstâncias; o *crossover*, que alterna entre instituições legítimas e ilegítimas, com o objetivo de providenciar informação e garantir a proteção; e o comunicador, garante de uma comunicação eficaz entre as diferentes células do organismo criminal.

A tendência para a construção social de redes complexas de crime organizado, que acabam por validar a referência cultural das grandes famílias criminosas ao estilo da Máfia,

apresenta-se como uma crença partilhada sem grande respaldo empírico. À assunção de existência de uma maior organização à conspiração criminosa do que ela realmente tem chamase falácia do crime organizado (Agra, 2018).

No que diz respeito às atividades desenvolvidas, o crime organizado atua essencialmente em seis áreas distintas: o narcotráfico, os crimes financeiros, o tráfico de seres humanos, a ajuda à imigração, os crimes tecnológicos e o tráfico diverso (Carrapiço, 2005). De entre os vários setores, o da droga será de longe a área mais lucrativa, apresentando um lucro estimado de 400 mil milhões de dólares por ano.

As carreiras criminais no crime organizado, numa perspetiva comparativa que procura justificar as diferenças empiricamente comprovadas entre as carreiras dos criminosos integrados nas organizações e as restantes, os autores remetem para três ordens de razão (Kleemans, 2014):

i) a grande importância das relações sociais no crime organizado comparativamente ao crime não organizado;

ii) a natureza transnacional de muitos dos crimes cometido por organizações criminosas, que acaba por afastar alguns perfis de criminosos deste tipo de delitos;

iii) comumente, os crimes inseridos no contexto das organizações revelam maior complexidade em termos logísticos.

A diferença na natureza dos crimes traduz-se numa tendência para os jovens se encontrarem ausentes deste tipo de crimes, o que reflete um perfil de idade mais avançada (Kleemans, 2014).

Numa leitura entrecruzada dos dados recolhidos, no capítulo quinto referimos que a iniciação da ciberdelinquência se dá numa tenra idade (ver as conclusões de Sérgio Camarà Arroyo (2020)).

Porém, e como apontam as razões acima invocadas por Kleemans (2014), cremos que o perfil típico do ciberdelinquente jovem, quanto à faixa etária, não assenta na mesma realidade criminológica que o perfil do ciberdelinquente integrado em redes organizações criminosas.

Acreditamos que, face à revisão de literatura, o ciberdelinquente jovem se pauta por crimes de menor escala, que alterna entre crimes contra a propriedade intelectual e crimes como

o *cyberstalking*, ao contrário do ciberdelinquente inserido em organizações criminosas, cujo guião criminal e a sofisticação dos ataques perpetrados diferem substancialmente (como sugere Kleemans, 2014).

4.3- O cibercrime organizado

O crescimento da criminalidade praticada com recurso a meios informáticos tem vindo a aumentar progressivamente, acompanhando a tendência decrescente nas formas de criminalidade mais grave e violenta (Leal, 2018). Na cibercriminalidade sob a forma de estruturas organizadas destacam-se a burla cometida através de meios informáticos, a burla informática e nas comunicações, o acesso ilegítimo ou indevido, a devassa por meio informático, a falsidade informática e a sabotagem informática (Leal, 2018).

A ausência de constrangimentos, que marcam o crime no espaço físico, permitiu ao cibercrime desenvolver-se com recurso às novas tecnologias, assumindo formas mais fluídas, ao nível organizacional, do que as formas do crime organizado convencional (Brenner, 2002).

A transitoriedade dos membros associados (geralmente identificados como *professional enablers, recruited enablers* e*money mules*) contrasta com a relativa consistência dos membros do núcleo duro, o que parece indicar a existência de diferentes configurações no que toca aos membros das redes, consoante as exigências técnicas e as particularidades do delito cometido (Leukfeldt *et al*., 2014).

Na relação entre o número de membros do núcleo duro e o grau de desenvolvimento tecnológico das redes criminosas, evidências concluem que as redes criminosas de maior subtileza tecnológica conseguem operar eficazmente com um menor número de membros do seu núcleo duro (Leukfeldt *et al*., 2014; Leukfledt *et al*., 2016).

Um estudo realizado por Leukfeldt *et al.* (2016) analisou as dinâmicas organizacionais de 18 casos de cibercriminalidade organizada na área do *phishing*.

Os autores recorrem ao modelo analítico das estruturas das oportunidades sociais (brevemente explicado *supra*) para analisar as capacidades das redes montadas (o *modus operandi*, a utilização de tecnologia, as atividades criminais secundárias, internacionalização dos membros) e a composição das mesmas.

O estudo divide as redes criminosas de acordo com a forma como estas utilizam as novas tecnologias nos ataques de *phishing*. As redes estudadas são dividas nas categorias de *low-tech attacks e high-tech attacks*, consoante as diferenças observadas nos guiões criminais relatados pelas instâncias formais de controlo.

Os autores sugerem a subdivisão destas categorias em função do maior ou menor contacto com a vítima durante os ataques de *phishing*, relacionando o tipo de ataque (*low-tech attack* ou *high-tech attack)* com o nível de interação com as vítimas. Distinguem quatro guiões criminais típicos na área do *phishing*:

i)- ataques *low-tech* com um elevado nível de interação com as vítimas;

ii)- ataques *low-tech* com um baixo nível de interação com as vítimas;

iii)- ataques *high-tech* com um baixo nível de interação com as vítimas;

iv)- ataques *high-tech* sem qualquer interação entre a vítima e o ofensor.

Os dados recolhidos por Leukfeldt *et al.* (2016) sugerem que o tipo de atividade criminosa secundária varia consoante os laços sociais que os membros do grupo estabelecem com outros membros de subgrupos homólogos.

Assim, a capacidade de expansão das redes criminosas para atividades secundárias depende essencialmente do contacto com outros parceiros criminais associados, que rondam as periferias das redes; estes associados, geralmente apelidados de *brokers*, que acabam por funcionar como elos de ligação entre diferentes redes, são responsáveis pela maior ou menor capacidade de internacionalização das redes criminosas[4].

Os grupos que permanecem constrangidos ao seu meio territorial nacional, de acordo com Leukfeldt *et al.* (2016), identificam-se com os grupos *low-tech*, ao passo que a maior capacidade de internacionalização é associada a uma maior utilização das novas tecnologias. A explicação, segundo os autores do estudo, reside na estrutura de oportunidades sociais, cuja dimensão e potencialidades acaba a depender quase inteiramente do recurso às novas tecnologias. Citando as conclusões, *these condgroup had no access to digital offender convergence setting and was constrained to a local social cluster. Accomplices were recruited through local social contacts and were all living in the Netherlands. All the victims were Dutch too. They also committed all kinds of other crimes to earn easy money. Conversely, the offenders of the first group me teach other at a digital forum. Specific criminal services could*

[4] Por isso mesmo, e como viremos a afirmar na síntese conclusiva do ponto 6.2, os modelos de organização em rede fomentam a internacionalização das redes criminosas. Como tal, cremos revelarem-se os modelos que melhor respondem às necessidades de sobrevivência e multiplicação dos organismos criminosos organizados no ciberespaço. Para mais desenvolvimentos remetemos para o ponto *infra* referenciado.

relatively easily be acquired through the forum: victims were targeted, and accomplices were recruited in foreign countries.

Para determinar o grau de internacionalização das redes criminosas, Leukfeldt *et al.* (2016) identificaram o país a partir do qual os membros operam o ataque, bem como a nacionalidade das vítimas.

As conclusões apontam que as redes criminosas cujos membros operam fora da Holanda, regra geral, identificam-se com redes *high-tech:* apenas uma das sete redes cujos membros não atuam em território holandês recorre a *low-tech attacks*, ao passo que todas as onze redes analisadas compostas exclusivamente por membros que atuam em território holandês operam com recurso a *low-tech attacks.*

Com base nos dados constantes das acusações formais do Ministério Público e nas entrevistas realizadas aos órgãos de polícia criminal, o estudo revela que quatro das redes *lowtech* se encontram envolvidas em tráfico de droga; seis encontram-se envolvidas em atividades fraudulentas ou relacionadas, cinco das quais são *low-tech networks;* e dez das dezassete são compostas por membros que se dedicam a atividades criminais paralelas.

A facilidade de adaptação das estruturas tradicionais do crime organizado ao cibercrime poderá ser um dos fatores explicativos para que muitas das antigas estruturas, que anteriormente operavam no espaço físico, comecem a olhar a cibercriminalidade como a forma natural de expansão dos aparelhos criminosos (Roderic Broadhurst *et a*l., 2014).

Apesar de a maioria do crime organizado no ciberespaço ser composto por grupos de delinquentes com níveis de expertise elevados no manuseamento das tecnologias de comunicação, as estruturas convencionais do crime organizado também absorvem delinquentes com níveis não muito elevados de literacia informática (Roderic Broadhurst *et al*., 2018).

As particularidades do recurso a meios informáticos permite que os indivíduos operem em rede a partir de locais isolados, ou mesmo de forma isolada, mas com ligações a redes mais alargadas (Spapens, 2010).

Lançar amplos ataques de *malware*, ou mesmo recorrer a complexas técnicas de *phishing* e *carding*, não exige necessariamente proximidade física, pelo que a eficácia do projeto é perfeitamente compatível com parcelas dispersas por territórios diversos (Leukfledt *et al*., 2016). Jones (2010), citado por Roderic Broadhurst *et al.* (2016), conclui que mesmo operando no ciberespaço os membros das redes criminosas tendem a pautar-se pela proximidade geográfica.

Na revisão empreendida por McGuire (2012), 50% dos grupos estudados são compostos por 6 ou mais pessoas, ¼ dos grupos têm mais do que 10 indivíduos, e ¼ apresentam um curto tempo de atividade, geralmente inferior a 6 meses de duração. O autor propõe tipos ideais de grupos, organizando uma tipologia taxonómica orientadora (Roderic Broadhurst, *et al.*, 2018). McGuire (2012) elabora três tipologias de grupos organizados, consoante a predominância e o impacto no empreendimento organizacional do crime *online* na sua relação com a atividade *offline*.

Segundo o autor, a primeira tipologia, cuja atividade ronda maioritariamente o *online*, divide-se nos grupos chamados *swarms* e *hubs*.

Os *swarms* são desorganizados, apresentam pequenas cadeias de comando e movem-se, grosso modo, por motivos ideológicos – o grupo *Anonymous* ilustra o subtipo descrito.

Os *hubs*, incluindo-se ainda nos grupos que operam essencialmente no ciberespaço, apresentam uma cadeia de comando mais organizada. Geralmente têm um ponto central organizativo estável, em torno do qual gravitam criminosos associados. Mcguire (2012) reporta que atividades como a distribuição de *scareware* geralmente são cometidas por grupos deste subtipo.

A segunda tipologia é composta por grupos que combinam a atividade *online* com a atividade *offline*. Geralmente associados a tipos de delitos como o *carding*, o subtipo dos *clustered hybrid* apresentam a organização típica dos *hubs*, com a diferença apenas de alternarem entre os crimes *online* e os crimes de rua. O segundo subtipo desta tipologia, os *extended hybrid*, apresenta um nível de coordenação superior à do subtipo mencionado em cima, apesar de se caraterizarem por uma menor centralização; tipicamente são numerosos, compostos por subgrupos e caraterizam-se por uma grande variedade de crimes cometidos.

A terceira tipologia demarca-se das restantes pelo facto de operar essencialmente offline, utilizando a tecnologia online como forma de facilitar o crime de rua (Roderic Broadhurst *et al.*, 2018). Este conjunto pode ser dividido em dois subtipos, os *hierarchies* e os *aggregate groups*, consoante o grau de coesão e organização que apresentam.

Os primeiros tendencialmente identificam-se com os grupos criminais tradicionais, e geralmente transpõem para o ciberespaço muitas das atividades que anteriormente já executavam *online*. Por exemplo, alguns grupos conotados com a máfia, na transposição para o online, passaram a dedicar-se a sítios de pornografia. Os *agreggate groups* são caraterizados pela sua natureza temporária, e atuação sem um claro propósito: por vezes organizam-se de

forma *ad hoc* enquanto grupo no ciberespaço, somente para coordenar crimes que serão cometidos fora do contexto online.

Roderic Broadhurst *et al.* (2018) sugerem que em futuras análises se utilize a grelha elaborada por McGuire (2012).

De referir ainda que, quanto à ligação entre a estrutura organizacional e o tipo de crime, geralmente a complexidade surge mais associada ao cometimento de crimes contra a propriedade, como é o caso da fraude.

CAPÍTULO V - O cibercriminoso empreendedor

5.1 – O cibercriminoso empreendedor – proposta explicativa

Sanford Sherizen (1990) sugere a similitude dos cibercriminosos com os criminosos de colarinho branco, reiterando a falsa crença de que as motivações dos cibercriminosos são bastantes diferentes apenas pelo facto de estes se movimentarem no ciberespaço.

Os estudos relativamente ao criminoso de colarinho branco sugerem que o seu perfil apresenta caraterísticas muito mais próximas dos não-delinquentes do que dos delinquentes que cometem o crime convencional (Cruz, 2012).

O autor indica que, na variável "idade", o criminoso de "colarinho branco" é em média mais velho (tem cerca de 40 anos) do que o criminoso "convencional" (entre 20 e 30 anos); no que respeita ao estatuto social e nível de habilitações, geralmente apresenta um elevado nível de habilitações e um emprego estável, em contraste com o nível relativamente baixo de instrução académica dos criminosos "convencionais. Quanto à inclusão social dos criminosos de colarinho-branco, a integração comunitária é mais elevada do que nos criminosos convencionais (Cruz, 2012).

O perfil do criminoso de colarinho branco, na definição citada por Cruz *et al.* (2015), pressupõe a prática de atos ilícitos ou pouco éticos por pessoas de elevado estatuto sociocultural, algo que se afasta das caraterísticas do cibercriminoso "convencional", cuja revisão empírica não aponta nenhuma relação entre estatuto sociocultural elevado e cibercriminalidade.

Na definição de cibercrime estabelece-se como critério todo o crime cometido com recurso a meios informáticos. Por isso mesmo, facilmente constatamos que muitos dos criminosos de colarinho branco, pela natureza dos crimes cometidos, se enquadram na definição de cibercriminosos, o que poderá indicar que alguma fatia da cibercriminalidade poderá ser explicada com recurso às teorias explicativas do crime de colarinho branco.

Porém, a ligação entre criminosos de colarinho branco e cibercriminosos, para além da sobreposição subjetiva entre ambos já indicada, poderá estabelecer-se na ordem dos valores e das motivações, especialmente se considerarmos que uma parte do cibercrime é cometido de forma organizada no seio de redes criminosas que em parte assumem a estrutura empresarial

como modelo organizativo (Roderic Broadhurst *et al.,* 2018). Algo que se assemelha às formas convencionais assumidas pelo crime de colarinho branco (Busato, 2017).

A orientação das atitudes dos cibercriminosos em função dos valores que caraterizam o empreendedorismo, se partirmos da assunção da similitude dos cibercriminosos com os criminosos de colarinho branco (Sherizen, 1990), poderá em parte explicar alguma da sua atividade cibercriminalidade cometida *a solo*, e boa parte da forma como esta é organizada no seio das organizações – quer sejam elas organizações legítimas com estruturas ilegítimas paralelas, quer sejam organizações criminosas única e exclusivamente criadas para a prática de crimes.

A similitude sugerida passa em primeiro lugar pelas semelhanças entre alguns tipos de cibercrimes e os crimes de colarinho branco. Pensemos por exemplo em todo o tipo de fraudes e meios ardilosos já enunciados, e na definição de Queloz (1999) citada por Cruz (2015). O autor indica seis elementos presentes na definição do criminoso de colarinho branco: ocorre num contexto económico; não utiliza a violência física; exige conhecimentos profissionais específicos nas áreas da economia, comércio, gestão, contabilidade ou finanças; é cometido com o intuito de enriquecimento ou para a resolução de um problema económico; constitui uma violação ou um abuso de confiança.

Cruz *et al.* (2015, p. 553), citando Pickett e Pickett (2002), acrescenta três elementos:

(…) é enganador, pois está associado à mentira, à dissimulação, simulação e à manipulação da verdade; é intencional, ou seja, a fraude não resulta de um simples engano ou negligência, mas existe um propósito de obtenção abusiva de ganhos ou de uma vantagem económica (dolo); normalmente está escondido sob a aparência de legalidade.

Face a esta caraterização do crime de colarinho branco proposta, podemos identificar inúmeros pontos de sobreposição nos guiões criminais do crime de colarinho branco e dos cibercrimes.

Por exemplo, o recurso à fraude está presente em boa parte dos cibercrimes cujo intuito é o lucro financeiro – pensemos por exemplo nos casos de *phishing* e *carding* – ao passo que cibercrimes cuja motivação é essencialmente ideológica (ver descrição do ponto anterior), cometidos pela figura típica do *hacker* ,apresentam tipos de delinquentes cujos conhecimentos

técnicos se revelam muito superiores à média (Roderic Broadhurst *et al*., 2018) – que preenche as caraterísticas referidas por Cruz *et al*. (2015).

Assim se justifica a proposta explicativa de analogia entre criminosos de colarinho branco e cibercriminosos, bem como a breve incursão pela temática do criminoso empreendedor.

No resumo de Cruz *et al.* (2015) acerca dos elementos que caraterizam o empreendedorismo, os autores convocam os trabalhos de Kirrzner, Penrose, Schumpeter e Knight, destacando alguns elementos caraterizadores mais valorizados por cada um dos autores nas diferentes definições que propõem. São eles, respetivamente, o enfoque em ganhos económicos e financeiros; a identificação de oportunidades; a inovação; e a assunção de risco.

A triangulação competências profissionais, inteligência e criatividade faz parte do perfil do criminoso de colarinho branco empreendedor, e faz parte também, pela revisão de literatura efetuada, do perfil de boa parte dos cibercriminosos (Paya Santos, Cremades Guisado & Delgado Morán, 2017; Wall, 2008; Fanjul Fernandez *et al*., 2018; Roderic Broadhurst *et al.*, 2014).

Com base nos estudos observados (ver para este efeito o estudo empírico realizado por Leukfeldt *et al*., 2016), acreditamos que a exigência de um espírito inovador, que permita a criação de redes e ataques *higth-tech*, constitua cada vez mais um requisito para uma carreira bem sucedida no mundo do cibercrime organizado.

A cibercriminalidade cada vez mais se alarga para lá das fronteiras nacionais, aproveitando as lacunas legais e o seu desenraizamento territorial como fator para escapar às malhas da detenção (Leukfeldt *et al*., 2016; Gonçalves, 2013; Amador, 2014). E, para isso, a sobrevivência no cibercrime pressupõe a presença de um espírito inovador e de elevada criatividade, capaz de se reinventar face a diferentes contextos e contrariedades.

Ora, sabemos que os contextos socioculturais influenciam o agir, tanto o agir normativo como o agir desviante (Cusson, 2006). Por isso mesmo, julgamos que exigências de sobrevivência no duro mercado do cibercrime, cada vez mais transnacional e especializado, impõe aos seus atores uma panóplia de mecanismos adaptativos cuja tendência aponta para a semelhança de perfil entre os cibercriminosos e o empresário empreendedor. Julgamos também que a estrutura de valores capitalistas favorece a ancoragem na figura do empresário líder que, por isso mesmo cada vez mais, cremos, inunda o mundo representacional do cibercriminoso.

CAPÍTULO VI - Proposta explicativa

6.1- Os modelos de organização em rede

O recurso ao modelo explicativo de organização rede parte da bicefalia modelos em rede/modelos piramidais proposta por Cândido da Agra (2018) na explicação dos modelos organizacionais do crime organizado citada no capítulo terceiro. Para lá remetemos maiores desenvolvimentos.

Para Mintzberg e Quinn, referidos por Gameiro (2008), o termo "organização em rede" afigura-se uma categoria abrangente a que se recorre para a descrição de uma qualquer forma organizacional que substitui a forma multidimensional como a maneira dominante de estruturar uma empresa moderna.

Na perspetiva destes autores, sugere Gameiro (2008), nas organizações em rede as comunicações periféricas (ou laterais, recorrendo à terminologia do autor) e estruturadas de modo horizontal assumem uma função principal, relegando para segundo plano as comunicações verticais (típicas dos modelos piramidais). Tal dinâmica é visível na figura 1.

Como afirma Gameiro (2008, p. 8), na organização em rede a estrutura formal ficará mais parecida com uma estrutura informal, *onde os colaboradores, em todos os níveis, ignorarão as fronteiras usando a tecnologia de informação para localizar e contactar diretamente os indivíduos cujos conhecimentos ou cooperação necessitam.*

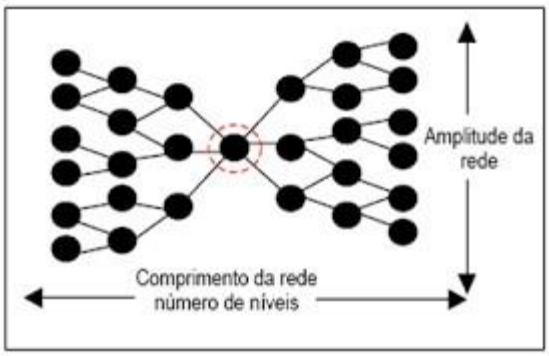

Figura 1- A rede de fornecimento com base no inter-relacionamento de amplitude e comprimento.

Fonte: Gameiro (2008), adaptado de Harland (1999).

A organização em rede pressupõe uma adaptação por parte das empresas a formas de organização cada vez mais globais, com especiais preocupações no estabelecimento de redes de cooperação com entidades externas. Nas relações em rede, como já afirmamos, as ligações interorganizacionais assumem especial destaque.

O modelo de organização em rede, consoante a maior ou menor dispersão centrípeta, poderá assumir a forma modelo de uma teia ou de um raio de sol. Ambos os modelos se diferenciam da estrutura piramidal do topo para a base. Na tabela 1 representamos uma versão adaptada da tabela proposta por Gameiro (2008) que contempla as diferentes especificidades dos dois modelos de organização em rede predominantes no cibercrime organizado[5].

***Tabela 1*- Modelos de organização em rede**

Fonte: Adaptado de Gameiro (2008).

Dimensões	**Teia**	**Raios de Sol**
Definição do nó	Individual	Unidade de Negócios
Local de conhecimento	Nós	Centro e Nós
Modo de ligação	Nós para nós	Centro para nós
Fonte de desenvolvimento	Exponencial	Sintético
Problemas e desafios da administração	- Necessidade de fomentar comunicações sem sobrecarregar o sistema - Gerir a concorrência entre nós	- Necessidade de equilibrar autonomia e controlo - Gerir a sustentabilidade da relação dos nós com o centro
Exemplos	Internet	Grande estúdio de cinema
Exemplos no cibercrime organizado (Mcguire, 2012)	*Swarms*	*Hubs*

[5] A última linha estabelece comparações com a tipologia proposta por McGuire (2012), cuja representação gráfica remete para as figuras 2 e 3 das páginas seguintes. Para maiores desenvolvimentos remetemos para a síntese conclusiva (ponto 6.2).

A tendência de organização em rede encontra reflexo no surgimento de diferentes papeis na estrutura, que fogem ao típico modelo burocrático.

A estrutura dos modelos em rede colide com o tipo ideal do modelo burocrático definido por Weber. O autor afirma como componentes do modelo burocrático, como já referimos no capítulo terceiro, a impessoalidade das relações e a estrutura hierárquica da autoridade. De acordo com Gameiro (2008), os modelos de organização em rede apresentam-se flexíveis e as relações tendencialmente não hierárquicas favorecem uma maior proximidade entre os membros das organizações.

Deste modo, e como já sugerimos no capítulo terceiro, recorrendo à terminologia estabelecida por Kleemans (2014), os modelos de organização em rede, se aplicados às organizações criminosas, não só não conseguem ser explicados pela teoria do modelo burocrático sugerida pelo autor como se revelam nos seus antípodas.

6.2 - Síntese conclusiva – o cibercriminoso empreendedor e os modelos de organização em rede: um processo de "swarmização"

Nesta síntese conclusiva, e face ao levantamento de literatura exposto nas fases precedentes, argumentamos a tendência crescente de descentralização dos grupos organizados do cibercrime.

Consideramos que os estudos até agora realizados (Roderic Broadhurst *et al*, 2018; McGuire, 2012; Kleemans e Van de Bunt, 1999; Kleemans, 2014; Jaishankar, 2018), pela dificuldade de aceder aos ofensores têm-se revelado insuficientes para a elaboração de modelos teóricos suficientemente robustos do ponto de vista empírico.

Porém, as tipologias avançadas na literatura acerca do cibercrime organizado (Roderic Broadhurst *et al*, 2018*;* McGuire, 2012) permitem-nos antever uma tendência de dinâmica organizacional futura que tende para a formação de pequenos aglomerados descentralizados de cibercriminosos organizados em rede (Leukfeldt *et al*., 2014*).*

A necessidade de sobrevivência dos organismos criminosos no ciberespaço, como já viemos afirmando nos capítulos precedentes (Kleemans, 2014), impõe a organização em pequena escala, por meio de células altamente fluídas e perfeitamente ajustáveis às vicissitudes dos constrangimentos legais (Kleemans, 2014).

As dinâmicas do ciberespaço impõem organismos altamente descentralizados, que possam aproveitar as falhar normativas de forma ajustada às necessidades da organização. A análise da literatura acerca do cibercrime veio demonstrar que a dinâmica organizacional da maioria dos organismos cibercriminosos não consegue ser explicada à luz do modelo burocrático (Roderic Broadhurst *et al.*, 2018*;* McGuire, 2012; Kleemans e van de Bunt, 1999; Kleemans, 2014).

Segundo este modelo, como já afirmámos em capítulos precedentes, a organização criminosa é marcada por uma distribuição de tarefas segundo modelos hierarquizados e com uma arrumação de estilo piramidal (Kleemans, 2014)

Consideramos que as organizações que recorrem ao modelo burocrático tenderão a diminuir pois à medida que os crimes se tornam mais complexos e os meios de reação legais mais sofisticados, o processo de estruturação das redes de cibercrime tenderão a apresentar-se flexíveis na estruturação dos papéis assumidos pelos diferentes atores.

As dinâmicas do cibercrime, como apontam diferentes autores (Roderic Broadhurst *et al.*, 2018; Mcguire, 2012; Kleemans e van de Bunt, 1999; Kleemans, 2014; Leukfeldt, 2916), e recorrendo à terminologia estabelecida por Felson (2002), pressupõem conjuntos de cadeias de informação que flutuam entre atores periféricos altamente capazes tecnicamente (Paya Santos, Cremades Guisado & Delgado Morán, 2017; Wall, 2008; Fanjul Fernandez *et al.*, 2018; Roderic Broadhurst *et al*., 2014).

A tendência de complexificação dos crimes informáticos vem acompanhando os crescentes esforços dos Estados em aumentarem a eficiência na sua rede de cibersegurança (Sutherland, 2018).

Deste modo, as dinâmicas organizacionais impõem organismos criminosos em pequena escala, bem como a emergência de novos atores periféricos que desafiam os modelos tradicionalmente rígidos dos organismos criminosos que operam no espaço físico.

A figura dos *brokers*, cuja função é preencher os vazios entre as diferentes estruturas de rede do crime organizado, e dos *facilitators*, que proporcionam diferentes serviços técnicos para vários grupos, revelam o surgimento de novos atores periféricos no encalce das organizações criminosas que desfiguram os modelos hierárquicos das estruturas pré-existentes (Clotet, 2003)[6].

No caso da cibercriminalidade organizada, a figura dos *brokers* – correspondente à figura do extensor na tipologia proposta por Lemieux (2003) – assume especial destaque no desenvolvimento de novas redes criminosas (Leukfeldt *et al*., 2016).

Na análise empírica realizada por Leukfeldt *et al.* (2016) verificamos que a capacidade de trocar recursos se revela um fator explicativo da criação de inúmeras relações interorganizacionais típicas do modelo de organização em rede.

A tipologia estabelecida por Mcguire (2012) chama a atenção para dois tipos de estruturas organizativas cuja atividade criminosa passa essencialmente pelo *online*. O destaque atribuído à organização destes dois grupos, face às outras tipologias propostas pelo autor, devese ao facto de operarem apenas *online*: julgamos serem os grupos que atuam

[6] Apesar de alguns autores, tais como Lemieux (2003), não estabelecerem distinção entre os diferentes papéis consoante a proximidade com o núcleo duro, boa parte da literatura consultada, no caso da cibercriminalidade organizada, tende a distinguir diferentes papéis na organização de acordo com a sua posição face ao núcleo permanente da organização (Leukfeldt *et al.*, 2016; Roderic Broadhurst *et al*., 2018; Mcguire, 2012). Neste sentido, podemos falar em atores periféricos que gravitam em torno dos organizadores (partindo da terminologia de Lemieux, 2003) e que estabelecem relações periféricas entre diferentes organizações sem que estas necessariamente envolvam os membros do núcleo duro.

maioritariamente online e não os que alternam entre crimes online e crimes *offline* aqueles que melhor exemplificam as dinâmicas do crime organizado no ciberespaço.[7]

O autor, como já citado no capítulo 3, agrupa os dois tipos nos chamados *swarms* e *hubs.* Os *swarms* apresentam-se como desorganizados e em pequenas cadeias de comando, ao passo que os *hubs* assentam num modelo que se assemelha à estrutura de organização em rede da figura 1, como podemos verificar pelas figuras 2 e 3.

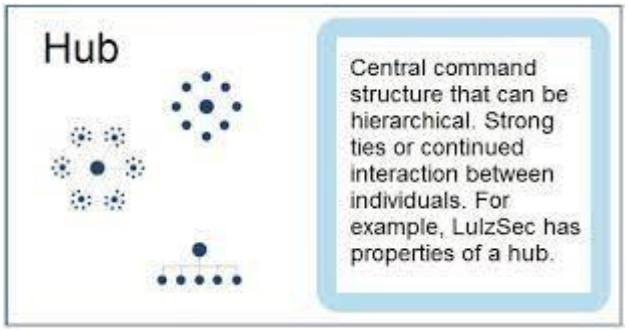

Figura 2- Representação de um *hub*

Fonte: Roderic Broadhurst et al (2018).

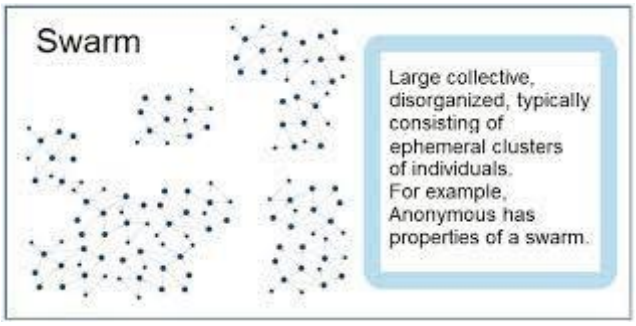

Figura 3- Representação de um *swarm*

Fonte: Roderic Broadhurst *et al.* (2018).

[7] Porém, consideramos que tipologias como os *clustered hybrid* e os *extended hybrid*, cuja organização assemelhase, respetivamente, aos *hubs* e aos *swarms* , integrem as dinâmicas de *swarmização* que apontamos. Não obstante, a atuação apenas no ciberespaço torna os *hubs* e os *swarms* (segundo a tipologia de Mcguire, 2012) o tipo ideal mais adequado às considerações do presente estudo.

Pela representação das figuras verificamos que ambos os modelos sugerem a existência de um agrupamento em rede, por contraposição com o modelo tipicamente piramidal organizado do topo para a base.

Como sugere a legenda da figura 2, apesar do modelo dos *hubs* – tipicamente associados a crimes tais como a propagação de *malware* – assentar numa lógica de estrutura hierarquizada, tal não implica que seja incompatível com o modelo de organização em rede (Agra, 2018). Importa clarificar que os modelos em rede podem apresentar dinâmicas hierárquicas, apesar de tendencialmente apresentarem relações do tipo horizontal.

Como indica Spapens (2010), as particularidades do ciberespaço e do recurso às novas tecnologias permite a criação de redes mais alargadas[8]. Deste modo, os estudos indicam que a internacionalização das redes criminosas justifica-se pela teoria das oportunidades sociais (o chamado "social snowball effect" cunhado por Kleemans e Van de Bunt, 1999), cujo alargamento se deve à presença de atores periféricos, tais como os *Brokers,* responsáveis pela internacionalização das redes (Leukfeldt *et* al, 2016*;* Clotet, 2003).

As perspetivas teóricas de Pareto (1910), Mayo (1933) e Whyte (1951), já referenciadas no capítulo 3, remetem para a ideia de que a base tecnológica se revela fator determinante para as alterações nas relações no seio das organizações.

Por isso mesmo, o contributo para a Criminologia de conceitos emprestados de áreas como a Economia e a Gestão tem se revelado cada vez mais importante para a interpretação de fenómenos criminológicos tais como o crime organizado (Kleemans, 2014; Foucault, 1979; Reuter, 1983).

A formação de organismo em rede, cremos, permite a potenciação das particularidades do ciberespaço de modo a permitir às organizações criminosas uma melhor adaptação às incertezas constantes do mercado ilícito (Leal, 2018).

A estrutura de relações piramidais rígidas, cujo desenrolar obedece a uma lógica da base para o topo, implica a existência de relações de poder estratificadas entre os membros da organização, cuja autoridade emana da existência de normas e regulamentos bem definidos (Weber, 1922).

[8] O alargamento territorial das redes não implica a tendência de redução do número de membros que apontamos nas páginas seguintes. O alargamento territorial, – correlato da internacionalização das redes sofisticadas – no caso da cibercriminalidade organizada, permite uma expansão com o mínimo de atores possível, pelo que ainda podemos falar em organizações de pequena escala.

Ora, no caso das organizações que operam maioritariamente no ciberespaço – e pensemos desde já nos *hubs e swarms* (Mcguire, 2012) – as relações de poder, cremos, diluemse à medida que a organização criminosa se expande.

Como sugere Spapens (2010), as particularidades do ciberespaço permitem que os indivíduos operem a partir de locais isolados, ou mesmo de forma isolada. Assim, com a expansão emerge a dispersão dos membros em aglomerados não centralizados e com isso, cremos, esbatem-se a tendências de dominação assentes na proximidade das relações que caraterizam o modelo centralizado de crime organizado (do estilo máfia).

A internacionalização, que Leukfeldt *et al. (*2016) apontou como a tendência das organizações tecnologicamente mais sofisticadas, introduz novos atores periféricos.

A introdução destes novos atores periféricos – cujos serviços técnicos ou os conhecimentos sociais se revelam cada vez mais indispensáveis para o alargamento das redes – tende a desenrolar-se de acordo com o padrão de desenvolvimento a que nós apelidamos de *swarmização*: isto é, a tendência para os organismos criminosos se alargarem e com esse alargamento apresentarem uma composição organizacional semelhante à descrita na figura 3.

Podemos pensar no processo de *swarmização* como o correlato do esboroamento das relações de poder no seio das organizações cibercriminosas. Consideramos que, à medida que a internacionalização assume o seu caminho, os cibercriminosos tendem a operar de forma isolada, explorando a sua autonomia técnica para escolherem os seus parceiros em função das especificidades dos ataques e dos vínculos sociais.

Neste sentido, e como sugere (Leukfeldt *et al*., 2014), a maior complexidade tecnológica dos ataques provoca uma tendência de diminuição dos membros do núcleo duro das redes. Ora, com a diminuição dos membros do núcleo duro esbatem-se as relações de poder, dada a contingência das formações que a organização pode assumir.[9]

[9] As relações de poder implicam relações de proximidade existencial, pelo que quanto maior for a liquidez, instabilidade e transitoriedade das relações mais frágeis serão os laços de poder constituídos no seu seio (Foucault, 1978).

A organização tenderá a *swarmizar-se*, o que equivale a dizer que tenderá a descentralizar-se de forma fluída, por meio de relações tendencialmente baseadas na cooperação e não na autoridade[10].

Podemos pensar numa tendência de atomização do cibercriminoso, se assim podemos chamar, que desagua numa expansão descentralizada e marcadamente individualista ao estilo da dispersão caraterística dos *swarms.*

Apesar deste processo de descentralização, a que apelidamos de *swarmização,* afetar, cremos nós, mais os grupos que maioritariamente operam *online* – pois que são esses que, tendencialmente, atuam sem estarem dependentes do enraizamento territorial das suas estruturas na comunidade – acreditamos que o processos de *swarmização* afetará também os grupos que, apesar de alternarem entre o online e o offline, apresentam a atuação criminosa offline como meramente instrumental das operações no ciberespaço.

Citando Kleemans (2014, p. 8):

(…) *hierarchical models focus upon "bosses and lieutenants", while this different approach also highlights more peripheral players, facilitators, who are important players for many offenders as they provide crucial services for many groups of offenders.*

[10] A flexibilidade apresenta-se cada vez mais como o desígnio das organizações atuais, que assim conseguem escapar mais eficazmente ao radar das instâncias formais de controlo. As organizações pautam-se pela descentralização das tarefas, sendo que a existência de poderes centrais viera a revelar-se um fator determinante da fraca resiliência das organizações (Agra, 2018). Gonçalves (2013) aponta para o consenso na literatura criminológica e entre a polícia em relação à maior subtileza de organização das estruturas em rede. A dispersão horizontal dos papéis, cremos, revela-se fator dificultador da investigação criminal. Ao passo que na típica composição hierárquica clássica a cartografia das posições ocupadas e das relações de poder estabelecidas permite uma investigação criminal consciente dos degraus da caminhada epistemológica das periferias para o centro, – numa lógica de poder-saber dos membros, – na dinâmica de rede as interpretações das dinâmicas organizativas por parte das instâncias formais de controlo revelam-se incertas, dada a dispersão de papeis, funções, desígnios e atividades desenvolvidas. A constante fluidez destas apresenta-se como uma dificuldade acrescida à sua deteção por parte dos órgãos de polícia criminal. Por isso mesmo, cremos, o modelo de organização em rede é mais resiliente que o modelo piramidal na relação com as instâncias formais de controlo. [11] A independência, enquanto valor chave do empreendedorismo, revela-se em parte incompatível com o modelo burocrático de relações altamente dependentes de diretivas, estruturadas por meio de regulamentos e reforçadas coercitivamente (Rodrigues, 2008; Neves *et a*l., 2015)

Esta tendência para o desenvolvimento dos nós periféricos, – o processo de *swarmização* entenda-se – cuja expansão não obedece ao crescimento dos centros para os nós caraterística de organizações como os *hubs*, é favorecida pelas caraterísticas psicológicas do ciberdelinquente empreendedor, já devidamente descritas no capítulo precedente.

O perfil inovador, capaz de identificar novas oportunidades de negócio e disponível para assumir riscos, – enquadrável no perfil de cibercriminoso económico referenciado no capítulo primeiro (Miró Llinares 2012; Fanjul Fernández *et al*., 2018), – permite equacionar que boa parte dos cibercriminosos estarão menos recetivos a relações de poder centralizadas e estáticas (típicas do modelo burocrático) e mais abertos a novos desafios com atores periféricos.

A operacionalização das redes emerge menos da autoridade e mais da iniciativa dos cibercriminosos, cujas competências técnicas sofisticadas permitem que se ofereça a diferentes parcerias, consoante as conveniências e os vínculos sociais.

Pense-se por exemplo na figura dos *facilitators* (Clotet, 2003) cuja função é proporcionar diferentes serviços a vários grupos e na analogia que poderá ser estabelecida entre estes e a figura dos empreendedores descrita por Cruz *et al.* (2015).

Numa perspetiva teórica, já devidamente referenciada nos capítulos precedentes, as teorias propostas por Elton Mayo (1933) apontam no sentido de uma relação tensional entre a formalidade das regras e a informalidade das interações: para o autor, as regras internas da organização encontram-se numa relação dialética com os valores que os indivíduos trazem consigo para o seio da organização (Henriques, 2014)[11].

Ora, o contexto de valores da pós-modernidade favorece precisamente a diluição de sistemas rigidamente definidos (Bauman, 1998). Tal contexto sistémico marca a interligação dos indivíduos em redes cada vez mais flexíveis, – flexibilização de horários, empregos e papéis sociais – como correlato dos processos de globalização e mercantilização das relações. Neste contexto, defendemos que a tendência sistémica apontada não é alheia ao mundo do crime em geral e ao mundo do cibercrime em especial. O papel das tecnologias de informação, aliás,

[11] Entenda-se neste caso a tensão entre os valores de independência, autonomia e criatividade e a formalidade das regras dos modelos burocratizados. Esta tensão provoca no seio das organizações criminosas a tendência para a descentralização das relações, cujo desenrolar deixa de passar necessariamente pelo centro. Partindo da ideia de Pareto, de que os equilíbrios nos grupos sociais se revelam frutos de ajustamento a processos de desequilíbrio resultantes de mudanças sociotécnicas, o processo de *swarmização* das organizações cibercriminosas apresenta-se como corolário de um processo relacional dialético entre as caraterísticas sociotécnicas do ciberespaço e os valores do empreendedorismo (independência, autonomia e criatividade) que os indivíduos trazem para o seio da organização.

é amplamente reconhecido como um fator que contribui para a aceleração dessa mesma flexibilização.

O cibercrime, por isso mesmo, acaba por refletir, em maior ou menor grau, os valores da pós-modernidade. E o cibercriminoso, como subproduto em parte dessas vicissitudes sistémicas, reflete-o, em maior ou menor grau, acreditamos nós, na assunção dos sistemas de valores empreendedores, cuja tendência revela uma crescente autonomização do indivíduo face à organização.

Sintetizando, a organização em rede pauta-se na maioria dos casos pelo distanciamento físico – que operam no ciberespaço - dos membros e pela predominância do lucro financeiro como móbil (Roderic Broadhurst *et al*., 2014). Estes dois fatores, cremos nós, aliados a um espírito empreendedor dos cibercriminosos (Cruz *et al*., 2015; Sherizen, 1990) e a uma alta especialização técnica – (Fanjul Fernandez, 2018) que lhes confere uma autonomia maior comparativamente aos criminosos com menor capital cultural) – conduz, acreditamos, ao que designamos de *swarmização* das organizações criminosas.

6.3- Conclusões

A incursão da Cibercriminologia no estudo do cibercrime fora marcada, numa fase inicial, por alguma resistência em considerar o cibercrime como uma nova forma de crime. O estudo dos cibercrimes era essencialmente da autoria de cientistas computacionais, fundadores de áreas tais como a cibersegurança e de estudos ciberforenses (Jaishankar, 2018).

Apenas em 2007 surgiu a disciplina da Cibercriminologia enquanto espaço multidisciplinar do estudo do comportamento criminal no ciberespaço e da cibervitimização sob a lente teórica da Criminologia (Jaishankar, 2018).

O estudo da Cibercriminologia encontra no *International Journal of Cyber Criminology* o seu maior repositório de estudos e artigos científicos no campo da Cibercriminologia.

As abordagens quantitativas do cibercrime têm se revelada de difícil execução, devido à dificuldade em estabelecer contacto com os ofensores, ao contrário dos estudos no campo da cibervitimologia. Deste modo, as abordagens seguem maioritariamente a lente teórica e qualitativa (Jaishankar, 2018).

A revisão de literatura efetuada veio demonstrar a heterogeneidade de perfil do cibercriminoso e das organizações cibercriminosas – o que torna a tarefa da Criminologia de destrinça e individualização das diferentes nuances do fenómeno cibercriminal ainda mais desafiante.

O estudo do cibercrime organizado apresenta-se como um terreno ainda por explorar do ponto de vista empírico, com apenas alguns estudos de base a servirem de alicerce para a construção de teorias explicativas (Roderic Broadhurst *et al*., 2018; McGuire, 2012; Kleemans e van de Bunt, 1999; Kleemans, 2014).

A abordagem criminológica da cibercriminalidade sob a lente teórica apresenta-se como um fenómeno altamente complexo. Esperamos com este trabalho académico contribuir para um melhor entendimento dos padrões de organização do cibercrime, desbravando o caminho teórico para futuros estudos empíricos da cibercriminalidade organizada.

BIBLIOGRAFIA

Agra, C. (2008). Entre a Droga e o Crime. 2.ª edição. Casa das Letras, Lisboa.

Agra, C. D. (2001). Elementos para uma epistemologia da Criminologia. Estudos em comemoração dos cinco anos (1995-2000) da Faculdade de Direito da Universidade do Porto.

Agra, C. D. (2018). Criminalidade reticular: nótula para um modelo de análise sistémica do crime organizado. Universidade Lusíada, Porto.

Agra, C. D., & Torrão, F. J. D. S. P. (2018). Criminalidade organizada e económica: perspetivas jurídica, política e criminológica. Universidade Lusíada, Porto.

Agra, C. D., & Torrão, F. J. D. S. P. (2018). Criminalidade organizada e económica: perspetivas jurídica, política e criminológica. Universidade Lusíada, Porto.

Alazab, M., & Broadhurst, R. (2015). The role of spam in cybercrime: data from the Australian cybercrime pilot observatory. In Cybercrime Risks and Responses (pp. 103-120). Palgrave Macmillan, London.

Amador, N. J. R. (2012). Cibercrime em Portugal: Trajetórias e Perspetivas de Futuro (Doctoral dissertation, Instituto Superior de Ciências Policiais e Segurança Interna).

Arroyo, S. C. (2020). La Cibercriminología y el perfil del ciberdelincuente. Derecho y Cambio Social, (60), 470-512.

Bauman, Z., & Haugaard, M. (2008). Liquid modernity and power: A dialogue with Zygmunt Bauman. Journal of Power, 1(2), 111-130.

Beck, U. (2018). Sociedade de Risco Mundial-em busca da segurança perdida. Leya.

Brenner, S. W. (2002). Organized cybercrime-how cyberspace may affect the structure of criminal relationships. NCJL & Tech., 4, 1.

Broadhurst, R., Grabosky, P., Alazab, M., & Bouhours, B. (2013). Organizations and cybercrime. Available at SSRN 2345525.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cybercrime. An analysis of the nature of groups engaged in cybercrime, International Journal of Cyber Criminology, 8(1), 1-20.

Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2018). Phishing and cybercrime risks in a university student community. Available at SSRN 3176319.

Carrapiço, H. (2005). O crime organizado e as novas tecnologias: uma faca de dois gumes. Nação e Defesa.

Chang, Y. C. (2012). Cybercrime in the Greater China Region: Regulatory responses and crime prevention across the Taiwan Strait. Edward Elgar Publishing.

Cohen, A. (2013, January 18). Was Aaron Swartz Really "Killed by the Government"? Time Ideas. Retrieved from http://ideas.time.com/2013/01/18/was-aaron-swartzreally-killed-by-thegovernment/

Costa, J. F. D. F. (1998). Algumas reflexões sobre o estatuto dogmático do chamado "Direito penal informático"". COSTA, José Francisco de Faria. Direito Penal da Comunicação: Alguns Escritos. Coimbra: Coimbra.

Cruz, J. N. (2007). O "crime de colarinho branco empreendedor": conceptualização e inferências para a dinâmica dos sistemas judiciais (Doctoral dissertation, Universidade Portucalense).

Cusson, Maurice (2011), Criminologia, 3.ª edição, Alfragide: casa das letras.

da Agra, C. (2011). A Criminologia: Um arquipélago interdisciplinar (Vol. 26). Universidade do Porto. Editorial.

DA AGRA, R. F. E. C. (2011). 1 a história epistemológica da criminologia. A Criminologia: Um arquipélago interdisciplinar, 27-63.

Foucault, M. (2009). Nacimiento de la biopolítica: curso del Collège de France (1978-1979) (Vol. 283). Ediciones Akal.

Furedi, F. (2006). Culture of fear revisited. A&C Black.

Gameiro, P. A. D. (2008). As organizações em rede. Universidade Lusófona de Humanidades e Tecnologias.

Gonçalves, A. A. S. (2013). O crime organizado em Portugal: sua caraterização e ambiguidades (Master thesis, FDUP).

Han, B. C. (2017). In the swarm: Digital prospects (Vol. 3). MIT Press.

Henriques, G. H. D. S. (2014). Significados-tipo e moral-em-uso nas organizações: uma aplicação aos gestores das burocracias modernas (Doctoral dissertation, ISCTE).

Leal, J. M. P. (2018). Sociedade, governança e manifestações criminais sobre a forma de crime organizado: conhecer para intervir. Universidade Lusíada, Porto.

Leukfeldt, E. R. (2015). Organised cybercrime and social opportunity structures: A proposal for future research directions. The European Review of Organised Crime, 2(2), 91-103.

Leukfeldt, E. R., & Kleemans, E. R. (2019). Cybercrime, money mules and situational crime prevention. Criminal Networks and Law Enforcement: Global Perspectives on Illicit Enterprise, 75-89.

Llinares, F. M. (2013). La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio. Revista Española de Investigación Criminológica, 11, 1-35.

McGuire, M. (2012). Organised Crime in the Digital Age. London: John Grieve Centre for Policing and Security.

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. Summary of key findings and implications. Home Office Research report, 75.

McQuade, S. C. (2006). Understanding and managing cybercrime. Boston: Pearson/Allyn and Bacon.

Paoli, Letizia. 2002. “The Paradoxes of Organized Crime.” Crime, Law and Social Change 37(1): 51-97.

Paya Santos, C., Cremades Guisado, A. y Delgado Morán, J. D. (2017). El fenómeno de la ciberdelincuencia en España: La propuesta de la Universidad Nebrija en la capacitación de personal para la prevención y el tratamiento del ciberdelito. Revista Policía y Seguridad Pública, 7(1), 237-270.

PERRIN, Stephanie. O Cibercrime. IN: AMBROSSI, Alain. PEUGEOT, Valérie

Poiares, N. C. L. D. B. (2019). A cibersegurança à luz da criminologia moderna. Cyberlaw by CIJIC, 7.

Pontell, H. N., & Geis, G. (Eds.). (2007). International handbook of white-collar and corporate crime (pp. 562-63). New York: Springer.

Reuter, Peter. 1983. Disorganized Crime: Illegal Markets and the Mafia. Cambridge, MA: MIT Press.

Rodrigues, S. (2008). Manual Técnico do Formando: "Empreendedorismo". ANJE - Associação Nacional de Jovens Empresários e EduWeb

Santos, S. I. D. S. (2018). "Estudo das perceções de cibersegurança e cibercrime e das implicações na formulação de Políticas Públicas-estudo exploratório do caso português (Doctoral dissertation, Instituto Superior de Ciências Sociais e Políticas).

Sherizen, S. (1990). Criminological concepts and research findings relevant for improving computer crime control. Computers & Security, 9(3), 215-222.

Smith, R., Grabosky, P., & Urbas, G. (2004). Cyber criminals on trial. Criminal Justice Matters, 58(1), 22-23.

Spapens, T. (2010). Macro Networks, Collectives, and Business Processes: An Integrated Approach to Organized Crime. European Journal of Crime, Criminal Law and Criminal Justice, 18(2), 185–215.

Sutherland, E. (2018, March). Cybersecurity: Governance of a new technology. In Proceedings of the PSA18 Political Studies Association International Conference, Cardiff (pp. 26-28).

Taivo, R. (2015) Cyber Behavior. Encyclopaedia of Information Science and Technology, 3rd Edition, Hershey, 638-646.

Tatarinova, L. F., Shakirov, K. N., & Tatarinov, D. V. (2016). Criminological analysis of determinants of cybercrime technologies. International Electronic Journal of Mathematics Education, 11(5), 1127-1134.

Walker, R. and Bakopoulos, B. 2005. Conversations in the dark: how young people manage chatroom relationships. First Monday, vol. 10, no. 4

Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. International Review of Law, Computers & Technology, 22(1-2), 45-63.

Wall, D. S. (2010). Criminalising cyberspace. The rise of the internet as a ‘crime problem’. Handbook of internet crime, 88-102.