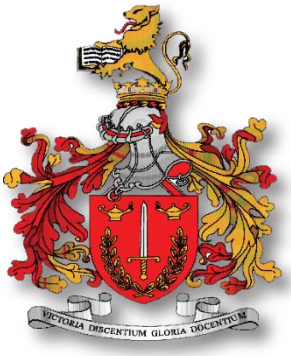
INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA



"APONTAMENTOS SOBRE CIBERSEGURANÇA E CIBERCRIME"

Trabalho Individual Final

3.º Curso de Comando e Direção Policial

Autor: Júlio José Costinha da Silva (Comissário)

Lisboa, 11 de julho de 2019

RESUMO

O presente trabalho teve como objetivo analisar a problemática da cibersegurança e do cibercrime em conjugação com os normativos legais que regem estas atividades, tentando com este breve contributo, de base empírica, criar uma visão integradora e interligada dos vários atores a quem compete regular e disciplinar neste domínio. Para alcançar os objetivos definidos, efetuou-se uma revisão da literatura, recorrendo a um método de investigação qualitativo consumado no estudo interpretativo das normas legais, sistematizando a análise dos seus conteúdos. Procedeu-se a pesquisa em fontes abertas para a consolidação das perspetivas sobre a cibersegurança e o cibercrime e como estes dois conceitos serão estruturantes nas futuras políticas de defesa e de âmbito criminal. O papel que a Polícia de Segurança Pública tem de desenvolver perante esta nova realidade tendo em conta as suas atribuições legais atuais, que são exercidas num campo muito restrito, estando já diagnosticado que este tipo de criminalidade será a principal referência no decorrer do século XXI e que irá exigir um esforço e forte investimento das entidades responsáveis pela área da segurança nacional e internacional.

Palavras-chave

Cibersegurança, Cibercrime, Polícia de Segurança Pública

ABSTRACT

This work aims to analyse the problem of cybersecurity and cybercrime in conjunction with the legal norms that govern these activities, trying with this brief empirical contribution to create an integrative and interconnected vision of the various actors who are responsible for regulating and disciplining in this field. It was decided to reach the defined objectives, to carry out a review of the literature, resorting to a method of qualitative investigation consummated in the study of the legal norms, being carried out the analysis of its contents. Research has been done on open sources to consolidate perspectives on cyber-security and cybercrime and how these two concepts will be structuring in future defence and criminal policies. The Public Security Police's role must be to develop in the face of this new reality, considering its legal attributions, which are limited to small sphere, and it is already diagnosed that this type of crime will be the main reference in the 21st century, it'll

require an effort and strong investment from the national and international entities responsible for the security.

Key words

Cybersecurity, Cybercrime, Public Security Police

1. INTRODUÇÃO

Atualmente a nossa sociedade é altamente influenciada pela internet, mais genericamente, pelo ciberespaço. O quotidiano, os direitos das pessoas, as interações sociais e também as economias dependem cada vez mais do bom funcionamento das tecnologias de informação e comunicação.

A crescente utilização de recursos informáticos tem permitido a recolha e a partilha de informação em grande escala a uma comunidade global. A internet, como rede global de comunicação entre computadores e entre pessoas facilita os processos de conexão e interligação.

O desenvolvimento tecnológico transformou o mundo numa sociedade global, na Era da Informação – que proporciona não só oportunidades, mas também riscos e ameaças.

Uma das características do ciberespaço é ser aberto e livre para que todos possam ter acesso e usufruir das suas potencialidades, tendo diminuído as distâncias entre os países, aproximando diferentes culturas, permitindo assim a partilha de informações, ideias e opiniões entre as diferentes partes do mundo. Apesar de todos os pontos positivos que este novo domínio de ação trouxe, surgiram também ações extremamente negativas e criminosas.

Condutas ilícitas passaram a ser praticadas neste novo ambiente desafiando o Estado, pois o ciberespaço alterou as fronteiras geográficas e a aplicação de instrumentos jurídicos em face do cibercrime.

Estas condutas revelam-se uma nova ameaça e neste trabalho faz-se uma breve exposição sobre o que é a cibersegurança e o cibercrime, assim como os conceitos associados, de forma a perceber esta tipologia criminal que cresce de dia para dia, revelando-se uma verdadeira ameaça para o bem-estar social, numa perspetiva dos Órgãos de Polícia Criminal (OPC), em geral e na Polícia de Segurança Pública (PSP), em particular, procurando desmistificar a necessidade do seu envolvimento e interação com base nos normativos legais vigentes e nas politicas atuais relativas à cibersegurança.

O objetivo principal deste trabalho é responder à questão: qual o papel da PSP como entidade interveniente e responsável na área da cibersegurança?

Para atingir este desiderato, definimos como objetivos específicos;

- A proteção do ciberespaço como fator primordial e estratégico;

- Compreensão do enquadramento normativo da cibersegurança nacional.

A utilização do ciberespaço requer a materialização de normas substanciais que de forma sustentada possam reduzir o risco social, protegendo as instituições públicas e privadas, obrigando a desenvolver uma estratégia integradora e mobilizadora a nível nacional. A cibersegurança tem de ser vista como uma prioridade nacional como forma de responder às ciberameaças. O enquadramento normativo nacional tem de ser visto como resultado dos normativos internacionais e em plena interligação. Internamente a cooperação entre OPC é essencial. A informação obtida deve ser fluída e canalizada para os órgãos competentes de investigação. A legislação nacional no âmbito dos crimes informáticos tem caráter de competência reservada de investigação para a Polícia Judiciária. Janelas de oportunidade surgem para outros OPC investigarem crimes desta natureza e tipologia. Neste quadro a PSP tem um papel ativo e de grande responsabilidade.

2. CIBERSEGURANÇA E CIBERCRIME

Num passado recente a cibercriminalidade optava por ataques massivos indiscriminados ou ataques cirúrgicos contra alvo determinado. Atualmente verifica-se o surgimento de campanhas massivas, simultaneamente dirigidas a indivíduos e organizações de determinados perfis com fins concretos e devidamente planeados. As organizações e instituições têm de optar por assumir uma postura defensiva mais abrangente, sistemática e eficiente. A intrusão e comprometimento passará a ser uma crença comum e, com ela, a perceção que estas organizações têm de estar preparadas o mais precocemente possível e a elas responderem de forma célere e eficaz.

A cibersegurança tem cada vez mais impacto no futuro das organizações. A aposta em ferramentas de cibersegurança que possam garantir sistemas e redes altamente seguras é o caminho a seguir. Hoje em dia palavras como cibersegurança, ciberterrorismo ou "*fake news*" já não são totalmente desconhecidas, bem pelo contrário, entram nas nossas vidas de forma quotidiana. O peso da Internet na sociedade é de tal grandeza que atualmente pode ser utilizado para mudar democracias, mesmo aquelas mais esclarecidas.

2.1 O Ciberespaço

Com o surgimento das chamadas tecnologias de informação e comunicação alterou-se a visão sobre a distância, acessibilidade e disponibilidade. Estas tornaram-se plataformas que influenciam de forma determinante a opinião pública, sendo que se encontram à disponibilidade de todas as pessoas. Devido à sua influência no campo político e social, é cada vez mais comum a ocorrência de acérrimos debates sobre a utilização destes instrumentos e plataformas. Está-se então perante o ciberespaço (Militão, 2014).

Foram várias as mudanças ocorridas que potenciaram o surgimento e concretização deste novo universo onde se juntaram um sem número de possibilidades: em primeiro lugar uma mudança e inovação no que respeita à tecnologia informática, sendo que o visor do computador deixou de ser um espaço estático passando a ser um ambiente que permite a manipulação, com janelas abertas e móveis que permitem diversas conexões; também se verificou uma mudança na esfera social onde, hoje em dia, as pessoas assumem uma postura muita menos passiva diante das diferentes mensagens e informações, estando muito mais abertas a intervenção. por fim, verificou-se uma mudança no cenário ao nível da comunicação, onde se passou de uma lógica de (apenas) transmissão para uma lógica de interatividade, modificando assim o clássico esquema emissor-mensagem-recetor (Gontijo, Mendes-Silva, Viggiano & Paixão, s.d).

A virtualidade associada ao ciberespaço é utilizada pelos indivíduos de variadíssimas maneiras, nomeadamente: pode ser utilizada como uma forma de refúgio no que concerne às dificuldades sociais; é um local onde se ampliam inúmeras possibilidades interativas; local de rápido acesso e democrático de informações, oportunidades profissionais, entretenimento, educativas e sociais; é também utilizada como sendo um campo de construção de identidades ou um recurso terapêutico face às dificuldades da vida real. Em contraste, o ciberespaço pode levar também a alienação da vida real e pode ser um espaço de disseminação de informação distorcida e tóxica, nomeadamente, movimentos radicas, extremistas e terroristas (Gontijo *et al*. s.d).

De acordo com o Instituto de Defesa Nacional (2013) o ciberespaço apresenta uma série de características particulares que se passam a descrever:

- Carácter dinâmico: o ciberespaço muda com uma grande frequência. Os diferentes sistemas que o constituem modificam-se constantemente, especialmente no que respeita às suas interligações. As vulnerabilidades deste espaço são descobertas todos os dias e as ameaças surgem e modificam-se constantemente.
- Muito baixo custo de acesso: A barreira económica de acesso ao ciberespaço é muito baixa. Atualmente estima-se que cerca de um terço da população mundial tenha acesso à internet.
- Enorme potencial de crescimento: O crescimento verifica-se quer ao nível de disseminação e troca de informação como ao nível das suas funcionalidades.
- Alta capacidade de processamento: Elevada capacidade de procura, processamento e armazenamento de informação.
- Caráter assimétrico: A assimetria revela-se ao nível dos recursos e do conhecimento necessário para desenvolver determinadas ações, nomeadamente ações hostis de grande impacto.
- Anonimato: Dificuldade em detetar e seguir a origem de um ataque, o que dificulta a capacidade de dissuasão e resposta.
- Alta capacidade para produzir efeitos físicos: Possibilidade em atingir uma ampla gama de indústrias e dispositivos, num ataque informático, por exemplo.
- Transversalidade: uma ação ou evento ocorrido no ciberespaço pode afetar um ou mais domínios de atividade das modernas sociedades, como sejam a área política, económica, social ou mesmo a segurança e defesa dos Estados.

Devido à importância do ciberespaço, a sua segurança e defesa tornam-se uma prioridade que deve ser tratada com o máximo de consciência e de responsabilidade.

2.2 A Segurança do Ciberespaço: Cibersegurança

No que concerne à segurança e defesa, a terra, o mar, o ar e o espaço sempre foram os domínios tradicionais de desenvolvimento de operações militares, sendo por isso que os esforços militares estão concentrados na obtenção de capacidades e habilidades para defenderem os domínios acima referenciados. Porém, e devido ao seu crescimento, o ciberespaço, já foi considerado e aceite como sendo o quinto domínio operacional, onde indivíduos especializados levam a cabo operações específicas de defesa e segurança de acordo com as características deste domínio (Instituto de Defesa Nacional, 2013).

De acordo com Militão (2014, p.26) a cibersegurança diz respeito ao "conjunto de medidas que procuram garantir o bem-estar e o regular funcionamento da ação de um estado e das suas populações no ciberespaço e fora dele, desde que derivado de ações diretamente a ele acometidas".

Tendo em conta o objetivo de garantir a segurança de todos aqueles que recorrem ao ciberespaço e que dependem deste no seu dia-a-dia, houve a necessidade de delimitar os espaços de ação no que concerne à cibersegurança:

- Cibercrime: Diz respeito ao aproveitamento ilícito das novas potencialidades dadas pelo ciberespaço. Neste domínio a atividade criminosa surge de variadas formas e nos mais diversos contextos. Com o objetivo de se poder regular legislativamente estas práticas ilícitas, foi necessário a determinação de categorias de modo a incluir diferentes tipologias de ação criminosa no ciberespaço. Os crimes podem ser classificados relativamente aos seus conteúdos (pedofilia, difamação e injúria, discriminação, jogos de azar), caso se trate de violação de dados pessoais e confidenciais (crimes informáticos de violação de correio eletrónico, invasão da vida privada),burla relativamente a telecomunicações e informática, falsidade informática, acesso ilegítimo a sistemas (pirataria, interceção ilegítima), dano e sabotagem e por fim crimes relacionados com a autodeterminação (*cyberstalking* e *cyberbullying*) (Santos, Bessa & Pimentel, 2008; Militão, 2014).
- *Hacktivismo*: De acordo com Santos, Bessa & Pimentel (2008), antes de ser uma atividade associada a atos criminosos (que vão desde a pirataria até ao desenvolvimento e implementação de *malwares*), o *hacktivismo* foi uma prática desenvolvida com intuito de encontrar falhas nos sistemas e, posteriormente, corrigi-las. Devido às suas características, consegue-se identificar 4 tipos de atividades desenvolvidas dentro do *hacktivismo*: 1) hackers, que invadem sistemas alheios com o intuito de criar e implementar *malwares*; 2) *phreakers*, burlões e invasores informáticos, exclusivamente em redes de comunicação; 3) *crackers*, que removem as proteções de determinados programas de modo a que possam ser acessíveis a todos sem que seja preciso pagar por isso e por fim 4) *cypherpunks* ou criptoanarquistas, indivíduos que desenvolvem procedimentos que permitem a proteção de ações maldosas e de comunicações no ciberespaço, através de mensagens e informações encriptadas, sendo que estas pessoas são especialistas em criptografia.

- Ciberespionagem: caracteriza-se por ataques informáticos que têm como objetivo a recolha de informação estratégica que coloquem o invasor numa situação de vantagem e poder. A ciberespionagem é altamente utilizada pelos Estados e seus serviços secretos (Militão, 2014).
- Ciberterrorismo: consiste na preocupante união entre o ciberespaço e as suas potencialidades e as práticas terroristas. De acordo com Santos, Bessa & Pimentel (2008) a estrutura da internet e das redes terroristas são muito parecidas no seu *modus operandi*, tendo em conta que ambas funcionam em rede e são transnacionais. O ciberterrorismo aproveita-se do aumento exponencial da dependência real do ciberespaço de forma a atacar importantes organismos estaduais e empresariais, podendo criar graves problemas no dia-a-dia das pessoas.

São várias as motivações que podem levar a que sejam cometidos crimes no ciberespaço. A motivação mais comum para ataques no ciberespaço são os benefícios económicos que podem derivar desses ataques. São vários e cada vez mais eficazes e requintados os atos fraudulentos perpetrados para se conseguir dinheiro, para subtrair informações comerciais e industriais para venda posterior pelo valor mais alto ou ainda a realização de ataques ou facilitar esses ataques em troca de benefícios monetários. Geralmente os cibercriminosos que se enquadram nesta motivação são trabalhadores internos das próprias organizações e espiões industriais.

Outra circunstância verificada prende-se com a obtenção de vantagens competitivas ou táticas, como é o exemplo da subtração de informações acerca de determinada empresa de modo a colocar outra entidade em vantagem competitiva ou ainda a subtração de informações táticas e militares de uma nação em conflito com outra.

Outra razão para os ataques perpetrados no ciberespaço é a fama e/ou vingança. Geralmente a notoriedade e a fama estão associadas aos *hackers*, que procuram reconhecimento nas diferentes comunidades e fóruns da especialidade. Muitas vezes pessoas que trabalham dentro de uma organização podem ser movidas pelos sentimentos de vingança contra a própria organização pelos mais variados motivos.

A cibersegurança aparece então como sendo um domínio cada vez mais importante da defesa dos estados, sendo encarada como uma necessidade, principalmente nos países ocidentais.

2.3 O Cibercrime

O termo "cibercrime" surgiu numa reunião realizada em Lyon, na França, pelo subgrupo das nações mais ricas do mundo, o G8 (Estados Unidos, Japão, Alemanha, Reino Unido, França, Itália, Canadá e Rússia), para estudar os problemas da criminalidade então causados via aparelhos eletrónicos ou pela disseminação de informações para a Internet.

Este "Grupo de Lyon" empregava o termo "cibercrime" para descrever, de forma muito vasta, todos os tipos de crime praticados na Internet. Este tipo de crime designa todas as formas de comportamento ilegal realizado mediante a utilização de um computador, conectado ou não a uma rede.

O Conselho Europeu, por intervenção do Grupo de Lyon, iniciou um esboço da Convenção sobre o Cibercrime, celebrada em Budapeste - Hungria, em 23 de novembro de 2001, pelo Conselho da Europa, e teve como signatários 43 países, europeus na sua maioria, e ainda Estados Unidos, Canadá, África do Sul e Japão.

A reunião teve como finalidade a unificação de um novo conjunto de técnicas de vigilância consideradas pelas instituições incumbidas do cumprimento da lei como necessárias para combater o "cibercrime".

Esta Convenção entrou em vigor para os primeiros Estados signatários a 1 de julho de 2004. A Convenção obriga os Estados que façam parte a adotar medidas a nível nacional de legislação específica, relativamente à confidencialidade, medidas práticas para o combate a estes fenómenos e a uma rede de cooperação internacional ciente da dimensão planetária do cibercrime (Rocha, Bravo & Verdelho, 2003).

Portugal, como signatário, adotou um importante instrumento jurídico internacional no combate aos crimes praticados através das redes informáticas e da informação eletrónica na Convenção sobre o cibercrime em Budapeste.

Neste seguimento surgiu a Lei n.º 109/2009, de 15 de setembro que aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

Simultaneamente Portugal adotou o Protocolo Adicional da Convenção relativo à criminalição de atos de natureza racista e xenófobos praticados através de sistemas informáticos, adotado em Estrasburgo em 28 de janeiro de 2003.

São exemplos de crimes informáticos, previstos na Lei do Cibercrime, Lei n.º 109/2009, de 15 de outubro, na Lei de Proteção de Dados Pessoais, Lei n.º 67/98, de 26 de outubro e no Código Penal Português, Decreto-Lei n.º 48/95, de 15 de março: reprodução ilegítima de programa protegido; acesso indevido ou ilegítimo/interceção ilegítima; violação ou destruição de dados/dano relativo a dados/programas; falsidade informática; sabotagem informática; não cumprimento de obrigações relativas a proteção de dados; violação do dever de sigilo e burla informática e nas comunicações. Existem outros crimes que podem admitir a sua execução nos meios informáticos, sendo os mais usuais: ameaça e coação; pornografia de menores; difamação, calúnia e injúrias; devassa por meio informático; burla relativa a trabalho ou emprego; descriminação racial ou religiosa; crimes contra a soberania nacional; tráfico de estupefacientes; terrorismo; crimes contra os direitos de autor.

2.3.1 Cibercrime na Lei Portuguesa

A lei portuguesa inclui vários normativos legais que são relevantes no âmbito da cibersegurança:

A Lei de Segurança Interna, Lei n.º 53/2008, de 29 de agosto, com relevância no âmbito das competências de controlo (art.º 18º) do Secretário-Geral do Sistema de Segurança Interna das forças e serviços de segurança e da gestão de incidentes tático-policiais graves, onde se incluem os ataques contra infraestruturas críticas ou destinada ao abastecimento e satisfação de necessidades vitais dos cidadãos.

A Lei da Organização e Investigação Criminal (LOIC), Lei n.º 49/2008, de 27 de agosto, que estipula ser da competência reservada da Polícia Judiciária a investigação dos crimes informáticos e praticados com o recurso a tecnologia informática, nos termos da alínea l), n.º 3, do art.º 7º, sem prejuízo da possibilidade de competência deferida a autoridade judiciária (AJ) a outro OPC, conforme confere o seu art.º 8º.

A Lei n.º 32/2008, de 17 de julho, que nos termos do art.º 1º, regulariza "a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar

o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes".

O Decreto-Lei n.º 62/2011, de 9 de maio, que tem por objetivos previstos no art.º 1.º, estabelecer "os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos setores da energia e transportes".

O cibercrime em Portugal está regulamentado pela Assembleia da República segundo a Lei n.º 109/2009 de 15 de Setembro: "A presente lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, referentes ao domínio do cibercrime e da recolha de prova em suporte eletrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa."

No capítulo II desta lei são apresentadas as disposições penais materiais para os crimes realizados em espaço de internet.

Para a falsidade informática as penas variam entre 120 dias de prisão a 5 anos dependendo da gravidade do crime informático.

Para falsidades informáticas com intenção de provocar danos nas relações jurídicas, "introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias". Quando estas mesmas ações afetam sistemas de cartão bancário ou permitam acesso a sistemas de pagamento, comunicação ou serviço de acesso condicionado, assim como para fins comerciais, a pena é de 1 a 5 anos de prisão.

Caso os crimes referidos anteriormente sejam praticados por funcionários no exercício das suas funções a pena aplicada pode variar de 2 a 5 anos de prisão.

O artigo 4.º da Lei n.º 109/2009 diz respeito ao dano relativo a programa ou outros dados informáticos. No caso de alguém sem permissão legal ou autorização, apagar, alterar,

destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afetar a capacidade de uso, está sujeito a uma pena de prisão até 3 anos ou a uma multa. A tentativa de efetuar estes atos é também punível.

Está também sujeito a pena de 3 anos de prisão ou multa quem violar a lei e produzir, comercializar, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não permitidas, descritas no parágrafo anterior.

Na ocorrência do dano provocado ser de valor elevado a pena é de até 5 anos ou de multa até 600 dias, se o dano for consideravelmente elevado a pena de prisão pode ir de 1 a 10 anos.

O artigo seguinte diz respeito à sabotagem informática, e no caso de sem autorização, "entrevar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático", é condenado com pena de prisão até 5 anos ou com pena de multa até 600 dias. No caso de comercialização, produção ou distribuição nas ações descritas anteriormente a tentativa não é punível.

No que diz respeito aos danos por sabotagem informática, se for de valor elevado a prisão será de 1 a 5 anos, ou de 1 a 10 anos no caso de valores consideravelmente elevados, perturbações graves no sistema informático que interfiram nas funções sociais ou atividades públicas.

O artigo 6.º, enumera as punições para quem pratica o acesso ilegítimo a um sistema informático, que sem permissão legal à autorização, traduz-se numa condenação de 1 ano de prisão ou multa de 120 dias. A mesma pena incide sobre quem ilegitimamente produz, comercializa, distribuiu num ou mais sistemas informáticos, dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos.

Se este acesso for conseguido através da violação das regras de segurança a pena é até 3 anos de prisão, ou de 1 a 5 anos através de dados confidenciais, para benefício patrimonial de valor considerado elevado.

A Lei n.º 109/2009 de 15 de setembro, refere no artigo 7.º sobre quem interceta transmissões de dados informáticos que se processam no interior de um sistema informático, com pena até 3 anos de prisão. Neste caso a tentativa também é punível e quem ilicitamente produzir, vender, distribuir sistemas informáticos, dispositivos, programas para produzir a interceção de transmissões de dados informáticos está sujeito à pena até 3 anos de prisão.

No caso da reprodução, divulgação com comunicação ilegítima de programa protegido (artigo 8.º) a condenação pode ser com pena de multa ou até 3 anos de prisão. Na mesma pena incorre quem reproduz ou comercializa topografia de um produto. A tentativa em ambos os casos é punível.

O artigo 9.º desta Lei n.º 109/2009 de 15 de setembro determina que "as pessoas coletivas e entidades equiparadas são penalmente responsáveis pelos crimes previstos na presente lei nos termos e limites do regime de responsabilização previsto no Código Penal".

O Capítulo II termina com o artigo 10.º que o "tribunal pode decretar a perda a favor do Estado dos objetos, materiais, equipamentos ou dispositivos que tiverem servido para a prática dos crimes previstos na presente lei e pertencerem a pessoa que tenha sido condenada pela sua prática", e ainda "avaliação, utilização, alienação e indemnização de bens apreendidos pelos OPC que sejam suscetíveis de vir a ser declarados perdidos a favor do Estado é aplicável o disposto no Decreto –Lei n.º 11/2007, de 19 de Janeiro.".

O Capítulo III, referente às disposições processuais, começa por esclarecer que as penas se aplicam aos processos relativos aos crimes previstos na Lei n.º 109/2009 de 15 de setembro, cometidos por meio de um sistema informático ou em relação aos crimes que seja necessário proceder à recolha de prova em suporte eletrónico (exceção dos dispostos 18º e 19º deste capítulo).

No decorrer dos processos relativos ao cibercrime, se for necessário à produção de prova, para se descobrir a veracidade dos factos, a obtenção de dados informáticos específicos armazenados num sistema informático, a AJ competente ordena a quem tenha

disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que os preserve.

A sua preservação pode também ser ordenada pelo OPC mediante autorização da AJ competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à AJ e transmitir-lhe o relatório previsto no artigo 253.º do Código de Processo Penal (CPP) (artigo 12.º).

A ordem de preservação discrimina, sob pena de nulidade: a natureza, origem e destino dos dados e o período de tempo pelo qual deverão ser preservados, até um máximo de três meses. Por outro lado, quem tenha o controlo dos dados, deve proteger, preservar a integridade pelo período de tempo fixado, de modo a permitir à autoridade competente a sua obtenção, e fica assim obrigado a assegurar a confidencialidade da aplicação da medida processual. No processo penal do cibercrime a AJ competente pode ordenar a renovação dos períodos até ao limite máximo de um ano (artigo 12.º).

O artigo 13.º, e tendo como objetivo assegurar a preservação dos dados de tráfego, determina que o fornecedor de serviço a quem essa preservação tenha sido ordenada nos termos do artigo anterior indica à AJ ou ao OPC, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efetuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efetuada.

Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a AJ competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência.

O disposto neste artigo é aplicável a fornecedores de serviço, a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, que permita determinar: "o tipo de serviço de comunicação utilizado; a identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou

acordo de serviços; ou qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços."

A injunção prevista no presente artigo não pode ser dirigida a suspeito ou arguido nesse processo, nem pode igualmente fazer-se uso da injunção prevista neste artigo quanto a sistemas informáticos utilizados para o exercício da advocacia, da atividade médica e bancária e da profissão de jornalista. O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do CPP é aplicável com as necessárias adaptações.

A pesquisa de dados informáticos deve sempre ser ordenada pela AJ competente por despacho, devendo presidir à diligência. O despacho tem um prazo de 30 dias, sob pena de nulidade.

Apenas os OPC podem proceder à pesquisa, sem prévia autorização da AJ, quando esta for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

O OPC que procede à investigação aquando da realização desta diligência é, sob pena de nulidade, comunicada de pronto à AJ competente e por esta apreciada em ordem à sua validação. Contudo em qualquer caso, é elaborado e remetido à AJ competente o relatório previsto no artigo 253.º do CPP.

A busca criminal pode ainda ser estendida mediante autorização e esta está regulamentada pelas regras das buscas previstas no CPP (artigo 174º, Capítulo III – das revistas e buscas) e no Estatuto do Jornalista.

Aquando das buscas informáticas, se forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a AJ competente ordena por despacho a apreensão dos mesmos.

Caso sejam apreendidos dados informáticos cujo conteúdo seja suscetível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respetivo titular ou de

terceiro, sob pena de nulidade esses dados devem ser presentes ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto.

As apreensões no cibercrime deverão ser sempre sujeitas a validação pela AJ, no prazo máximo de 72 horas.

As apreensões relativas a sistemas informáticos utilizados para o exercício da advocacia e das atividades médica e bancária estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no CPP e regras do Estatuto do Jornalista. Novamente neste caso o segredo profissional previsto no artigo 182.º do CPP é aplicável com as devidas adaptações.

O confisco dos dados informáticos, deve ter em conta os interesses do caso concreto, e pode ser efetuado das seguintes formas (artigo 16.º):

a) "Apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respetiva leitura;

b) Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo (a cópia é efetuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital);

c) Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos;

d) Eliminação não reversível ou bloqueio do acesso aos dados".

Ainda relacionado com apreensão de dados informáticos, e segundo o CPP, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência de correio eletrónico e registos de comunicação semelhante (artigo 17.º).

O artigo 18.º, referente à interceção de comunicações, alega que a interceção pode acontecer quando praticados cibercrimes, para prova em suporte eletrónico, como gravações

de chamadas, ao abrigo dos artigos 187.º /188.º/ 190.º do CPP. Estas só podem ocorrer durante o inquérito, para a descoberta da verdade.

2.3.2 A Prova no Cibercrime

Devido à natureza dos crimes cometidos, a natureza da prova do cibercrime também muda substancialmente, recebendo o nome de prova digital. A prova digital é definida por Rodrigues (2011, p.722) como sendo "qualquer tipo de informação, com valor probatório, armazenada em repositório eletrónico-digital de armazenamento, ou transmitida em sistemas e redes informáticas ou redes de comunicações eletrónicas, privadas ou publicamente acessíveis, sob a forma binária ou digital".

Esta é um tipo de prova que se encontra inserido num contexto técnico e complexo, que é de difícil apreensão para a maioria das pessoas. Por essa razão, esta deve ser apresentada numa linguagem simples, clara e objetiva, de modo a ser percebido e aplicável por todos os operadores judiciais. Esta deve ainda ser duradoura, sendo necessário que tome as medidas essenciais para que a sua recolha e conservação esteja garantida (Rodrigues, 2011).

A prova digital deve ser recolhida rapidamente, cumprindo todos os preceitos associados para que esta não perca a sua integridade, sendo que o investigador deve sempre considerar a natureza temporária da porta, dificultando a sua conservação num dispositivo próprio para esse efeito para além do tempo deste.

Por existir o risco da prova digital desaparecer, os investigadores devem também considerar a natureza deste tipo de prova como instável e volátil. A sua instabilidade torna a sua apreensão muito difícil, uma vez que esta é facilmente modificável, podendo apresentar, inicialmente, certas características e mais tarde, quando vai ser novamente analisada, esta encontra-se totalmente ou parcialmente diferente (Rodrigues, 2009).

Por fim, o investigador deve considerar a natureza imaterial da prova digital, sendo que este deve conhecer determinadas técnicas específicas, de modo a que prova não perca o seu valor e a sua força e que o investigador não modifique o seu conteúdo, devido ao desconhecimento de como a manusear corretamente (Rodrigues, 2009).

As provas digitais podem ser apreendidas em vários meios diferentes: em telemóveis, computadores, onde se destacam os *e-mails*. Por exemplo, relativamente aos telemóveis, as mensagens SMS têm sido utlizadas cada vez mais como meio de prova. O tratamento dado às SMS e aos *e-mails* são iguais, dividindo-se em dois momentos: o primeiro diz respeito à transição da mensagem entre o emissor e o recetor e a respetiva chegada ao domínio do destinatário de acordo com o art.18º da Lei 109/2009. Num segundo momento, e após a leitura da mensagem, a SMS e o *e-mail* devem ser submetidos ao regime geral de correspondência (art.º 179º CPP).

3. PAPEL DA POLÍCIA DE SEGURANÇA PÚBLICA

Com a globalização do mundo, os Estados têm de enfrentar novas realidades de segurança, sendo a cibersegurança uma das mais prementes e incontornáveis, sabendo-se as necessidades e dependência inerentes às interações dos sistemas informáticos para que exista um real e eficaz funcionamento. As soberanias nacionais têm de ser afirmadas, também, no ciberespaço o que implica que os serviços de segurança têm de ajustar as suas realidades e adaptarem-se aos novos desafios do ciberespaço e aos seus riscos.

Nas Grandes Opções Estratégicas da PSP para 2017-2020, são valorizados 5 eixos de importância vital para a instituição. Destes destacam-se:

Eixo 2 - "Reforçar a valorização humana, profissional e técnica dos recursos humanos, para criar valor e melhorar a segurança pública"

Eixo 4 – "Comunicação e informação – Consolidação evolutiva do modelo de comunicação e dos sistemas e tecnologias de informação", destacando-se " a gestão da informação, a cibersegurança, o reforço dos meios de segurança da informação já implementados e a participação reforçada nos mecanismos de prevenção e cooperação existentes a nível nacional e internacional serão prioridade, não descurando a criação de competências e capacidades próprias, promovendo uma mais adequada e necessária presença da PSP no ciberespaço."

Eixo 5 – "Cooperação Organizacional e Internacional – Reforçar a imagem institucional, as capacidades, as competências e o profissionalismo", dando realce, a nível nacional, à articulação com outros atores que integram o sistema de segurança interna e a nível internacional fomentar a participação nos mecanismos e instrumentos de cooperação

internacional, especialmente com as agências FRONTEX, CEPOL, INTERPOL e EUROPOL, aumentando o relacionamento institucional com os países que integram a AMERIPOL, a IBERPOL e a CPLP.

As atribuições da PSP estão consignadas no art.º 3.º da Lei n.º 53/2007, de 31 de agosto, que aprova a sua orgânica. Destacam-se pela sua abrangência no contexto do cibercrime e da cibersegurança, as alíneas de a) a e) e m), do n.º 2:

a) Garantir as condições de segurança que permitam o exercício dos direitos e liberdades e o respeito pelas garantias do cidadão, bem como o pleno funcionamento das instituições democráticas, no respeito pela legalidade e pelos princípios do Estado de direito;
b) Garantir a ordem e tranquilidade públicas e a segurança e a proteção das pessoas e dos bens;
c) Prevenir a criminalidade em geral, em coordenação com as demais forças e serviços de segurança;
d) Prevenir a prática dos demais actos contrários à lei e aos seus regulamentos;
e) Desenvolver as acções de investigação criminal e contra-ordenacional que lhe sejam atribuídas por lei, delegadas pelas autoridades judiciárias ou solicitadas pelas autoridades administrativas;
m) Prevenir e detetar situações de tráfico e consumo de estupefacientes ou outras substâncias proibidas, através da vigilância e do patrulhamento das zonas referenciadas como locais de tráfico ou consumo.

A LOIC, Lei n.º 49/2008, de 27 de agosto, define a Investigação Criminal como "o conjunto de diligências que nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher provas, no âmbito do processo." Esta é uma definição aproximada do teor do art.º 262.º do CPP, no entanto, a sua abrangência é superior, pois não se resume à fase de inquérito, mas também à fase de instrução. A direção da investigação em cada fase do processo é distinta. Na fase de inquérito o Ministério Público é a AJ competente, enquanto na fase de instrução é o Juiz de Instrução, sendo que em ambas as fases são assistidos pelos OPC.

O art.º 2º indica que os OPC ao tomar conhecimento de um crime devem comunica-lo no prazo mais breve possível, que não pode exceder 10 dias à AJ. Devem ainda, iniciar investigação e de pronto, praticar "os atos cautelares necessários e urgentes para assegurar os meios de prova."

Os OPC atuam na direção e dependência funcional da AJ competente, mas não estão submetidos hierarquicamente, dai resultando a sua autonomia técnica e tática, podendo decidir quando, como e com que meios deve atuar. A autonomia técnica consiste na utilização de um conjunto de conhecimentos e métodos adequados para a investigação concreta do caso. A autonomia tática verifica-se na escolha do tempo, lugar e modo entendidos adequados à prática dos atos correspondentes ao exercício das funções consignadas legalmente aos OPC.

Os OPC podem ser considerados de 3 formas a nível das competências de investigação:

- Competência genérica (PJ, PSP e GNR);

- Competência específica (todos os outros OPC);

- Competência reservada (previsão legalmente expressa).

A PSP tem competência genérica na investigação criminal em todos os crimes cuja competência não esteja reservada a outros OPC e ainda de crimes cuja competência pode ser delegada, conforme o resultante do art.º 7.º, n.º 3, por força expressa da delegação de competências prevista no art.º 8.º, onde se destacam os crimes constantes nas alíneas seguintes:

b) Furto, dano, roubo ou recetação de coisa móvel que:

ii) possua significado importante para o desenvolvimento tecnológico ou económico.

l) Informáticos e praticados com recurso a tecnologia informática;

n) Conexos com os crimes referidos nas alíneas d), j) e l).

Com base nestes pressupostos legais a PSP como OPC tem competência para:

- Efetuar pesquisas e apreensões de dados informáticos, de forma a assegurar os meios de prova decorrentes do cumprimento de atos processuais ordenados pela AJ competente;

- Pode efetuar pesquisa e apreensão de dados informáticos em crimes conexos, cuja tipologia não tenha a caraterística de crime informático nem o objeto central do crime seja conseguido através do recurso a computador, com as devidas instruções da AJ competente;

- Deve promover os atos cautelares necessários e urgentes para assegurar os meios de prova e remeter, com o conhecimento da AJ, para o OPC competente, o expediente realizado, no mais breve prazo, de qualquer facto tipificado como crime, cuja investigação se encontra legalmente reservada a outro OPC, sem prejuízo dos casos de competência deferida previstos no art.º 8.º da LOIC.

4. CONCLUSÕES

A nossa sociedade está em constante mutação. Estamos perante um momento de grandes transformações. Tudo se transforma rapidamente, as distâncias encurtam e o choque entre diferentes culturas é maior devido ao ciberespaço que permitiu uma aproximação entre as pessoas do mesmo mundo.

O ciberespaço veio oferecer um novo espaço de interação humana tão relevante como o espaço físico, sendo que o primeiro é de livre acesso e disponível a todos. No entanto estas duas características acarretam perigos, dando a oportunidade a ações criminosas que podem criar o caos e a destruição em países e organizações.

A PSP no cumprimento das suas obrigações legais tem um papel de vital importância para a segurança nacional e o espectro do cibercrime. Muitos passos terão de ser dados para se atingir e concretizar a prevenção e a resolução dos crimes informáticos. A alteração dos normativos legais, deve ser equacionada, perspetivando-se em consonância com a realidade atual, visto que a reserva de competência a um só OPC, já não responde às verdadeiras e reais exigências de investigação nacional. No quadro atual legislativo, a PSP, embora com avultadas limitações, tem algumas possibilidades de mostrar serviço, desde que eleve os seus padrões de qualidade, numa área onde existe muita competição e especificidade.

A PSP terá que se adaptar a esta nova realidade e apostar na investigação e desenvolvimento, deve normalizar e certificar os seus procedimentos, enraizar a formação e a consciencialização do seu público interno e externo, como objetivos principais.

A PSP terá de efetuar um avultado investimento em termos de formação na área do cibercrime para prosseguir os objetivos estruturantes da investigação criminal. É uma área onde a PSP está com parcos conhecimentos, pouca capacidade tecnológica e os seus recursos humanos não têm as habilitações consideradas adequadas. No Instituto de Ciências Policiais e Segurança Interna deveria ser constituída doutrina para projetar iniciativas de investigação e desenvolvimento nas áreas de investigação criminal relativo ao meio digital com base na experiência policial.

A consciencialização dos públicos, interno e externo é importante. A cibersegurança não é de exclusiva responsabilidade do Estado, mas deve ser entendida como de responsabilidade partilhada entre o setor público, os cidadãos e empresas do setor privado, apostando na consciencialização relativa às ameaças que podem surgir do ciberespaço.

Na perspetiva de normalizar e certificar os procedimentos é crucial a adoção de futuras estratégias de cibersegurança, por forma a facilitar a cooperação a nível nacional e internacional com os vários atores, quer públicos quer privados.

Existe a necessidade de investimento para promover as condições ideais para responder a este tipo de criminalidade específica que de forma gradual está a causar um forte impacto nas estruturas das instituições, na área económica/financeira e nas relações sociais por forma a garantir as condições de segurança e o exercício dos direitos e liberdades dos cidadãos.

REFERÊNCIAS BIBLIOGRÁFICAS

Gontijo, C., Mendes-Silva, I., Viggiano, A. & Paixão, E. (s/d). Ciberespaço: que território é esse? [em linha]. Disponível: http://ticsproeja.pbworks.com/f/Ciberespaco.pdf . Acedido a 8 de julho de 2019.

Grandes Opções Estratégicas da PSP para 2017-2020 (2016), Lisboa: Direção Nacional da PSP

Instituto da Defesa Nacional. (2013). Caderno IDN, Investigação conjunta IDN-CESEDEN, *Estratégia da Informação e Segurança no Ciberespaço*. Lisboa: Instituto da Defesa Nacional.

Militão, O. (2014). *Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional*. Dissertação de Mestrado da Faculdade de Ciências Sociais e Humanas, Faculdade Nova de Lisboa, Lisboa.

Rocha., M., Bravo., R. & Verdelho, P. (2003). *Leis do Cibercrime – Volume 1*. Lisboa. Edições Centro Atlântico.

Rodrigues, B. (2009). *Das Escutas Telefónicas – À Obtenção da Prova [Em Ambiente] Digital*. Coimbra: Coimbra Editora.

Rodrigues, B. (2011). *Da Prova Penal – Tomo IV, Da Prova Electrónico-Digital e da Criminalidade Informático-Digital*. Lisboa: Rei dos Livros.

Santos, P., Bessa, R. & Pimentel, C. (2008). *Cyberwar - O Fenómeno, as Tecnologias e os Actores*. Lisboa: FCA – Editora de Informática.

LEGISLAÇÃO

Decreto-Lei n.º 78/87, de 17 de fevereiro, Diário da República, 1.ª Série, n.º 40, 617-699, Assembleia da República;

Decreto-Lei n.º 48/95, de 15 de março, Diário da República, 1.ª Série - A, n.º 63, 1350-1416, Assembleia da República;

Decreto-Lei n.º 62/2001, de 9 de maio, Diário da República, 1.ª Série, n.º 89, 2624-2627, Assembleia da República;

Lei n.º 67/98, de 26 de outubro, Diário da República, 1.ª Série - A, n.º 247, 5536-5546, Assembleia da República;

Lei n.º 53/2007, de 31 de agosto, Diário da República, 1.ª Série, n.º 168, 6065-6074, Assembleia da República;

Lei n.º 32/2008, de 17 de julho, Diário da República, 1.ª Série, n.º 137, 4454-4458, Assembleia da República;

Lei n.º 49/2008, de 27 de agosto, Diário da República, 1.ª Série, n.º 165, 6038-6042, Assembleia da República;

Lei n.º 53/2008, de 29 de agosto, Diário da República, 1.ª Série, n.º 167, 6135-6141, Assembleia da República;

Lei n.º 109/2009, de 15 de setembro, Diário da República, 1.ª Série, n.º 179, 6319-6325, Assembleia da República.