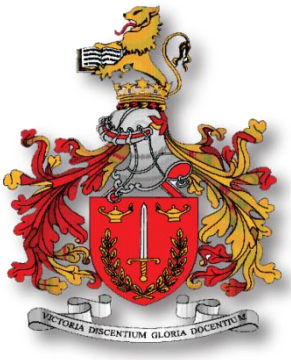
INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA



CIBERPOLICIAMENTO DAS REDES SOCIAIS

O CONTRIBUTO DAS CIÊNCIAS TECNOLÓGICAS

Autor: Carlos Manuel Teixeira Maia (Comissário)

Estudo Teórico

Lisboa, 04 de Julho de 2019

RESUMO

A evolução tecnológica, a disseminação das redes sociais e a facilidade de aceder às mesmas transformaram o modo de funcionamento das sociedades e do universo digital.

O ciberespaço tornou-se num dos maiores desafios a nível social, económico, político e também policial. Surgiram novas oportunidades mas simultaneamente novas ameaças para os seus utilizadores, emergindo assim a cibercriminalidade.

Neste contexto, a existência de um ciberpoliciamento capaz de monitorizar as redes sociais, os conteúdos, os dados produzidos e daí extrair informações relevantes que permitam atuar antecipadamente à ocorrência de cibercrimes, revela-se crucial para uma Polícia moderna e integral como a PSP.

As ciências tecnológicas, através de ferramentas de *big data analytics*, permitem extrair *insights* de dados estruturados, semiestruturados e não estruturados que são processados a cada segundo em todo o mundo, identificando padrões de comportamento dos cibernautas e conteúdos publicados, permitindo a produção de *intelligence*.

Com a elaboração deste artigo pretendeu-se demonstrar a importância do ciberpoliciamento das redes sociais e refletir sobre a monitorização do enorme volume de dados que são produzidos diariamente no ciberespaço.

Palavras-chave: *big data analytics*; cibercrime; ciberespaço; ciberpoliciamento; redes sociais.

ABSTRACT

Technological evolution, dissemination of social networks and the ease of acess to them, have transformed the digital universe and the way on wich societies operates.

Cyberspace has become one of the biggest challenges not only on the social, economic and political level but also on the police field. New opportunities have been created but, with them, new threats to their users, thus emerging cybercrime.

In this context, the existence of a cyberpolicing strategy able of tracking down social media networks: its contents and the data outcome; and able to capture valuable information that allows to take early actions, it´s crucial to a modern and integral police, as PSP aims to be.

Technological sciences, through big data analytics tools, allow to extract insights of structured, semi-structured and unstructured data, that can be instantly processed all over the world, identifying behaviour patterns of the internet users and published contents enhancing the production of intelligence.

With this article we intended to demonstrate the significance of cyberpolicing the social media and also reflect about the tracking of the enourmous volume of data that are daily produced on cyberspace.

Keywords: Big data analytics; cybercrime cyberpolicing; cyberspace; social media.

1. INTRODUÇÃO

A evolução das tecnologias de informação e comunicação (TIC), da *internet* e da *web* alteraram significativamente o funcionamento das sociedades e o modo de vida dos cidadãos em geral. A *internet* liga à escala mundial computadores, pessoas e empresas podendo afirmar-se não existirem dúvidas que efetivamente a evolução tecnológica contribuiu para a melhoria do bem-estar das pessoas e para o desenvolvimento das sociedades, das empresas e das organizações.

Ao nível social, as novas tecnologias e as diversas plataformas que foram igualmente surgindo, contribuíram para uma mudança de paradigma nas relações sociais. Hoje em dia são já poucos aqueles que não utilizam as redes sociais digitais e plataformas da *web* para se relacionarem com outrem, quer seja no âmbito das suas vidas pessoais, sociais ou profissionais.

No entanto, com toda esta evolução surgiram também atos maliciosos contra esta rede global de informação, aproveitando algumas vulnerabilidades que o ciberespaço apresenta e com isso causarem danos ao sistema global de informação, surgindo as atividades delituosas no ciberespaço e que se denominam por cibercrime.

Esta realidade obrigou a que os Estados implementassem medidas de segurança que dificultem estes acessos indevidos e maliciosos à "rede" e os ataques à *internet* que causam inúmeros prejuízos, quer patrimoniais ou pessoais dos envolvidos, sejam eles infraestruturas governamentais, instituições públicas ou privadas, empresas e cidadãos em geral, emergindo assim o conceito de cibersegurança.

Ao nível da cibersegurança existem diversos mecanismos e entidades, públicas e privadas, tanto a nível nacional ou mundial para protegerem e responderem aos incidentes que vão surgindo contra os sistemas de informação e o ciberespaço em geral. Há também diversos programas informáticos desenvolvidos pelo mundo empresarial que defendem esses sistemas e os seus componentes, impedindo ou dificultando os ataques e tentativas de intrusão que o ciberespaço é alvo.

As redes sociais virtuais constituem um importante e variado repositório de informações. Ao nível comercial, as empresas recorrem a estas plataformas digitais para obterem informação sobre os seus produtos, tendências de consumo e perfis dos utilizadores tendo em vista a melhoria do seu negócio, constituindo já um importante auxiliar na tomada de decisão empresarial.

Para isso o mundo empresarial recorre às novas tecnologias e a *softwares* informáticos que existem e que lhes permitem ter conhecimento praticamente em tempo real das referidas tendências de mercado, dos produtos que são mais procurados *online*, dos comentários e avaliações que os consumidores fazem dos mesmos. Isto permite às empresas traçar perfis de consumidores e relacioná-los com utilizadores da *internet*.

Se pensarmos bem, todos nós já pesquisamos produtos ou serviços *online* e depois, quando estamos a efetuar uma outra pesquisa ou a aceder à *internet* somos "inundados" com anúncios publicitários sobre essas pesquisas anteriores.

Isto acontece devido à denominada *big data*, que tal como o nome indica, é uma enorme base de dados que armazena e processa todo o tipo de dados que circulam no ciberespaço e que através de ferramentas computacionais permitem criar associações e padrões de comportamento e daí extrair informação relevante sobre o que se pretende.

Ao nível da informação policial, as redes sociais digitais são designadas fontes abertas de informação. Para a Polícia de Segurança Pública (PSP), a enorme quantidade de informações que circula nas diversas redes sociais é preponderante para a sua atividade, quer seja num plano de investigação de um cibercrime já cometido, na prevenção criminal ou mesmo no planeamento de um grande evento.

Se ao nível da cibersegurança e na repressão do cibercrime, no *post crimen*, há já legislação aprovada e os procedimentos estão previstos, ao nível da prevenção criminal no ciberespaço, em especial nas redes sociais não há ainda um policiamento preventivo que possibilite às forças de segurança atuarem na prevenção de atividades delituosas, pois a imensidão de conteúdos publicados a cada segundo nas redes sociais *online* impede uma eficaz monitorização preventiva das mesmas apenas pela ação humana.

Neste contexto, esta investigação procurará dar resposta à seguinte pergunta de partida: Como é que a PSP pode desenvolver um ciberpoliciamento das redes sociais com recurso às ciências tecnológicas?

1.1. Objetivos

A elaboração deste trabalho insere-se no âmbito do 3.º Curso de Comando e Direção Policial (CCDP) e tem como objetivos refletir sobre o policiamento preventivo do ciberespaço e em particular das redes sociais digitais. Verificar a forma como a PSP pode extrair informação relevante dos inúmeros dados que circulam no mundo virtual, tal e qual o mundo empresarial faz com a *big data* e com esse conhecimento produzir *intelligence*

para podermos atuar preventivamente nas redes sociais ou seja, fazer um ciberpoliciamento digital tendo em vista a prevenção de atos delituosos na *internet*.

Perante os objetivos descritos anteriormente, é nossa intenção desenvolver um estudo teórico de caráter descritivo, inserido num paradigma de investigação qualitativa, privilegiando a análise bibliográfica e documental. Segundo Sarmento, (2013) este modelo descreve fenómenos, identifica variáveis e inventaria factos, ao mesmo tempo que promove uma recolha e análise de informação de uma forma controlada e sistemática.

Na elaboração do presente trabalho de investigação recorremos ao método científico que consiste num "conjunto de regras básicas que visam obter novo conhecimento científico" (Sarmento, 2013, p. 4). O método científico quer descobrir a realidade dos factos sendo este "apenas um meio de acesso: só a inteligência e a reflexão descobrem o que realmente os factos são" (Cervo e Bervian, 1996, p. 21).

Assim, a nossa investigação incidiu na consulta e análise de bibliografia que versa sobre esta temática para obtermos o estado da arte e que pretendemos refletir. Esta fase é descrita por Quivy e Campenhoudt (2005, p. 26) como rutura e o "primeiro ato constitutivo do procedimento científico".

Na elaboração das referências ao longo deste trabalho de investigação foi utilizada a 6.ª edição do referencial da *American Psychological Association* (APA, 2010).

1.2. Pertinência

Do ponto de vista das ciências policiais e da atividade policial, a pertinência do tema indicado parece-nos inquestionável sobretudo para a área da *intelligence* policial.

As redes sociais digitais constituem um enorme repositório de informações que a PSP deveria ter a capacidade de monitorizar para poder antecipar-se às atividades delituosas que a *internet* possibilita.

No entanto não existe ainda um modelo de ciberpoliciamento ou forma de policiar o ciberespaço preventivamente sem a intervenção permanente da ação humana.

Por outro lado, ao nível académico, existe uma grande lacuna de trabalhos de investigação sobre ciberpoliciamento, ao contrário de temas como a cibersegurança, e cibercrime em que já existem alguns artigos científicos publicados.

Assim, julgamos que este trabalho reveste-se de enorme importância e pertinência até pelo caráter inovador do tema, cujo objeto de estudo revela-se praticamente inexistente no meio científico.

2. ESTADO DA ARTE

2.1. Contextualização teórica e concetual

No final do século XX a *internet* transformou-se num meio generalizado de edição e interação (O'Reilly, 2005), permitindo à sociedade em geral participar na produção e partilha de informações, o que veio alterar significativamente os hábitos dos cidadãos e as relações sociais.

Este evento fez surgir como que um novo paradigma de organização social resultante da utilização massiva das novas TIC e que Castells (2005) refere como rutura tecnológica, social e económica com o período anterior, cujo impacto é comparável ao da revolução industrial.

Com esta evolução tecnológica surgiram novos vocábulos e novas realidades que originaram conceitos até então desconhecidos e que agora estão cada vez mais presentes no nosso quotidiano. De forma sumária, propomo-nos contextualizar alguns destes conceitos e que são fundamentais para a realização deste trabalho.

2.1.1. Ciberespaço

O termo ciberespaço constitui um conceito amplo e é usado genericamente para referir algo relacionado com a *Internet* e com as novas práticas socioculturais que lhe estão associadas. No entanto, pela sua própria natureza complexa e multifacetada, o ciberespaço no sentido mais rigoroso do termo é suscetível de uma abordagem multidimensional nomeadamente numa perspetiva tecnológica, jurídica, sociológica, estratégica, segurança e política (Fernandes, 2012). Em 1984 o escritor William Gibson, na sua obra de ficção científica intitulada "*Neuromancer*", foi quem utilizou pela primeira vez o termo ciberespaço referindo-se-lhe como o conjunto de dados computacionais existentes no universo das redes digitais (Gibson, 1984).

O ciberespaço não tem fronteiras nem território e caracteriza-se como um novo universo ilimitado, acessível em qualquer parte do mundo e a qualquer hora, basta para isso o acesso a um computador ou simplesmente a um *smartphone* ou outro aparelho com ligação à *internet* para entrar neste mundo virtual e explorar dados e informações ilimitadas. Nesta perspetiva, o ciberespaço pode ser pensado como o conjunto de

comunidades intangíveis e o espaço interativo, tornado possível pelo conjunto de redes da *internet* (Akdeniz, *et al*., 2001).

Como refere a orientação política para a ciberdefesa em Portugal, constante no anexo ao Despacho n.º 13692/2013, de 28 de outubro, o ciberespaço "é por natureza um espaço aberto desprovido de fronteiras tangíveis, onde tanto o setor público como o privado, civis e militares, atores nacionais e internacionais interagem em simultâneo e de forma interdependente e interligada" (p. 31977).

No entanto, apesar das definições distintas dos vários autores, há já um consenso que o ciberespaço não é apenas algo virtual mas também físico pois devemos integrar neste conceito todo o emaranhado tecnológico que serve de suporte, como os "inúmeros computadores interconectados, servidores, *routers*, *switches* e cabos" (Freire e Caldas, 2013, p. 90).

Pierre Lévy (2000) refere que para além da infraestrutura material da comunicação digital este conceito abrange também todo o conjunto das informações que ele abriga, assim como as pessoas que navegam e sustentam todo este universo onde ocorre a comunicação mediada por computador e sistemas informáticos. É o "espaço de comunicação aberta pela interligação mundial dos computadores e das memórias informáticas" (Lévy, 2000, p. 95) e que permite o acesso à distância aos diversos recursos de um computador ou bases de dados.

O ciberespaço é uma espécie de novo ambiente que permite a comunicação e o relacionamento entre as pessoas, partilha de experiências, a realização de negócios, troca de opiniões, novas amizades enfim, uma panóplia de funcionalidades que as novas tecnologias criaram. Para Fernandes (2012, p. 12), o termo ciberespaço está relacionado com a *internet* e com práticas sociais, constituindo um "rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores".

Para Kuehl (2009), ciberespaço constitui um domínio global operacional de caráter único e distinto, enquadrado pela utilização da eletrónica e do espetro eletromagnético com o objetivo de criar, modificar, explorar, guardar e trocar informação através de sistemas baseados em tecnologias de comunicação e de informação interligados e todas as suas infraestruturas associadas, dos quais fazem parte a *internet*, as redes de telecomunicações e os sistemas de computadores.

Ao nível da NATO, em junho de 2016, numa cimeira de ministros da defesa, o ciberespaço foi reconhecido por aquela organização também como um domínio operacional de atuação da NATO, para além dos já existentes como terra, ar e mar.

A Estratégia Nacional de Segurança do Ciberespaço (ENSC), aprovada pela Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho, refere que o ciberespaço consiste no "ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação".

Decorrente do conceito ciberespaço, surgiram outros termos relacionados com esta temática, entre os quais o cibercrime.

2.1.2. Cibercrime

De certa forma podemos dizer que não há uma definição exata e consensual de cibercrime, havendo antes várias abordagens a esta temática e outras tantas expressões relacionadas com atividades criminosas num contexto do ciberespaço, da informática e da *internet*.

Tal como menciona o UNODC – United Nations Office on Drugs and Crime[1], não existe um conceito único de cibercrime, referindo ser mais apropriado incluir nesta definição um conjunto de atos ou comportamentos, que podem ser agrupados em categorias, tendo por base o objeto do crime ou o *modus operandi* do que propriamente tipos de atos.

Uma primeira abordagem à definição de crime informático surgiu em 1989 quando o departamento de justiça dos EUA referiu que qualquer violação da lei criminal que envolva conhecimentos de tecnologias de computadores para a sua execução, investigação e acusação constitui crime informático (Keyser, 2003).

Posteriormente, em 1998 há uma distinção entre crime informático e cibercrime. No primeiro, o autor do crime utiliza conhecimentos específicos de tecnologias de computadores, enquanto no cibercrime o ato delituoso é praticado com recurso à *internet* e com conhecimentos sobre o ciberespaço (Parker, 1998).

Em 2000, no 10.º Congresso das Nações Unidas (UN) para a prevenção do crime e tratamento das vítimas, surgiram duas novas definições. Cibercrime em sentido estrito que

[1] Departamento das Nações Unidas sobre Drogas e Crime. Agência especializada da Organização das Nações Unidas, criada em 1997, com sede em Viena.

abrangeria qualquer comportamento ilegal, efetuado através de meios eletrónicos, cujo alvo fosse a segurança de sistemas de computadores e os dados neles alojados. Cibercrime, no sentido lato, referir-se-ia a qualquer comportamento ilegal cometido por meio de, ou relacionado com, sistemas ou redes de computadores, incluindo crimes como a posse ilegal de informação através de sistemas ou redes de computadores (UN, 2000).

Pedro Verdelho (2003) diz-nos que a Convenção sobre cibercrime do Conselho da Europa, em 2001, foi o primeiro trabalho de fundo, ao nível internacional, sobre o crime no ciberespaço, contra sistemas de computadores, redes ou dados e pretendeu harmonizar as várias legislações nacionais sobre esta matéria e facilitar as investigações criminais e cooperação internacional.

Segundo Ghernaoti (2013), cibercrime pode ser definido como qualquer ato criminoso perpetrado através do ciberespaço ou da *internet*. Estão aqui incluídas todas as formas de ação criminosas digitais efetuadas através de tecnologias digitais, dispositivos eletrónicos e redes de telecomunicações.

Conforme refere a Comissão Europeia (JOIN, 2013)[2], este conceito refere-se a um vasto conjunto de diferentes atividades ilícitas que envolvem os computadores e os sistemas informáticos, quer sejam enquanto instrumentos ou alvos principais. A cibercriminalidade abrange as infrações tradicionais (fraude, falsificação e roubo de identidade), infrações relativas aos conteúdos (por exemplo, distribuição de material pedopornográfico em linha ou incitamento ao ódio racial), e crimes respeitantes exclusivamente a computadores e sistemas informáticos (por exemplo, ataques contra os sistemas informáticos, recusa de serviço e *software* malicioso).

No que concerne à ENSC (2019), cibercrime é definido concetualmente como os factos correspondentes a crimes previstos na Lei do Cibercrime e a outros ilícitos penais praticados com recurso a meios tecnológicos e sempre que estes sejam essenciais à prática do crime em causa.

Em Portugal a tipificação criminal destas matérias consta de diferentes diplomas legais, desde logo o Código Penal Português, nomeadamente no artigo n.º 193.º - *Devassa por meio de informática* e artigo n.º 221.º - *Burla informática e nas comunicações*; Na Lei da Proteção de Dados Pessoais, Lei n.º 67/98, de 26 de outubro que transpôs para a ordem jurídica interna a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de

[2]Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido. Comunicação conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões.

outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados; Na denominada Lei do Cibercrime, Lei n.º 109/2009, de 15 de setembro, que estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas 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 Europeu, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

2.1.3. Cibersegurança

A informação disponível no ciberespaço, dada a forma como é facilmente acedida por todos, deve estar salvaguardada por mecanismos de segurança que permitam a sua integridade. Os sistemas de informação, os computadores e a *internet* em geral, dadas as vulnerabilidades e ameaças das mesmas, têm de possuir mecanismos de segurança que impeçam ataques maliciosos e que coloquem em risco os ativos de informação das organizações e de particulares.

Para Vacca (2014), esta segurança é conseguida quando os sistemas de informação e a informação são protegidos contra ataques, através da utilização de serviços de segurança, que assegurem a disponibilidade, integridade, confidencialidade, autenticidade e não repúdio da informação e dos seus componentes.

No mesmo sentido Tralhão (2008), refere que a prevenção, deteção e reação estão intimamente relacionados com esta ideia de segurança.

Concetualmente podemos dizer que a prevenção determina o valor da informação e o risco a que esta está sujeita. A deteção é a monitorização para determinar quando e como ocorreu o incidente bem como os responsáveis. Já a reação consiste na tomada de ações para repor a situação e eliminar o risco.

Esta cibersegurança, tal como os conceitos anteriormente abordados, não tem uma definição adotada de forma unilateral, havendo antes várias definições sendo no entanto que todas elas revelam as mesmas preocupações e áreas de atuação, tendo em conta a segurança do ciberespaço e dos seus utilizadores.

A ENSC (2019) adota concetualmente a cibersegurança como “o conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade,

disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem" (p. 2889).

Em Portugal, inserido no Gabinete Nacional de Segurança (GNS), existe o Centro Nacional de CiberSegurança (CNCS) que, conforme refere o Decreto-Lei n.º 69/2014, de 09 de maio, tem por missão cooperar para que o país faça uso do ciberespaço de forma livre, confiável e segura, promover a melhoria contínua da cibersegurança nacional e da cooperação internacional, articulando com todas as autoridades competentes, "bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais" (p. 2712).

A nível europeu a ENISA[3], agência especializada em cibersegurança, tem por missão colaborar na segurança cibernética na Europa e "contribuir para a realização dos objetivos consistentes em assegurar um elevado nível de segurança das redes e da informação na União e desenvolver uma cultura de segurança das redes e da informação em benefício dos cidadãos, dos consumidores, das empresas e das administrações públicas" (ENISA, 2013, p. 42).

A cibersegurança tornou-se numa "área essencial para os Estados e para a sociedade civil, tendo em vista prevenir ataques às redes dos setores público e privado, os quais podem colocar em causa a estabilidade coletiva" (Elias, 2019, p. 18)

Refira-se ainda que sob a alçada da Europol há o denominado EC3 (European CyberCrime Centre), criado em 2013, numa altura de crescente preocupação e ameaça da possibilidade de cibercrime na União Europeia, dada a evolução da *internet* no continente Europeu. O EC3 tem como objetivos o fortalecimento da resposta da aplicação da lei da criminalidade informática na União Europeia e ajuda na proteção dos governos, empresas e cidadãos europeus.

Relacionado com o conceito de cibersegurança existem os termos CERT (Computer Emergency Response Team) cuja função é identificar e responder a riscos cibernéticos e limitar o seu impacto, e o CSIRT (Computer Security Incident Response Team) que tem por missão responder a incidentes relacionados com a segurança informática.

[3] European Union Agency for Network and Information Security (ENISA).

2.1.4. Redes Sociais

O estudo das redes sociais teve início na antropologia social e na sociologia do séc. XX, assumindo desde então um papel de relevo transversal em diversas áreas do conhecimento, alcançando especial importância com a revolução tecnológica e o desenvolvimento da *internet*.

De acordo com Manuel Castells (2005), a *internet* é o instrumento chave desse novo sistema tecnológico e, consequentemente, da sociedade em rede. O conceito de sociedade em rede foi sugerido por este autor para caraterizar esta nova organização social que tem por base um conjunto de redes operadas por tecnologias de informação e comunicação (TIC) fundamentadas na microeletrónica, recorrendo ao conjunto de " redes digitais de computadores que geram, processam e distribuem informação a partir do conhecimento acumulado nessas redes" (Castells, 2005, p. 20).

A ideia de rede social não é de agora, na verdade e de acordo com Gustavo Cardoso (2011), é um conceito usado há mais de um século para classificar as relações que se criam entre elementos de um sistema social. Com o aparecimento da *internet* e evolução das tecnologias digitais este conceito de *social media* adquiriu um novo contexto de aplicabilidade e está intimamente ligado com o aparecimento das redes sociais.

No essencial, uma rede social digital ou virtual é uma estrutura constituída por pessoas ou organizações com interesses, causas, valores e objetivos comuns, organizados em rede na qual os seus membros partilham e comunicam entre si através do ciberespaço.

Para Patrício e Gonçalves (2010), as redes sociais virtuais operam em plataformas digitais que sustentam um espaço comum de interesses, necessidades e objetivos semelhantes para a cooperação, a partilha de conhecimento, a interação e a comunicação. Estas redes sociais formadas em meios *online* podem resultar na constituição de comunidades virtuais que, apesar de diferentes daquelas que detêm um caráter físico, são igualmente eficazes quanto à unificação e mobilização dos indivíduos. (Castells, 2007).

Segundo Kaplan e Haenlein, estas redes sociais podem ser definidas como "um grupo de aplicações *online* baseadas nos fundamentos ideológicos e tecnológicos da *internet*, e que permitem a criação e a troca de conteúdo gerado pelo utilizador" (2010, p. 61). As redes sociais virtuais são interativas e permitem que os utilizadores participem na produção de conteúdos, contactem com outros utilizadores, originando verdadeiros diálogos virtuais e agrupando-se, muitas vezes, em comunidades virtuais (Lempert, 2006).

O progresso das redes sociais fez surgir um novo princípio social: o princípio da popularidade. Segundo Dijck (2013), este princípio sustenta que quantos mais contactos e amigos um utilizador tiver *online*, mais importância terá, pois isso poderá significar que é popular e outros utilizadores poderão querer segui-lo e considera-lo um influenciador.

Atualmente as redes sociais digitais são já um dos principais meios de comunicação e interação do mundo mas também é verdade que sem utilizadores não há redes sociais, pois estas alimentam-se do conteúdo produzido pelos seus utilizadores e da interação entre eles (Rashtchy, *et. al.*, 2007). Existe uma grande diversidade de redes sociais, com diferentes finalidades e as mais conhecidas e utilizadas são: Facebook, Twitter, WhatsApp, YouTube, Instagram, Skype, Snapchat, LinkedIn, Google +, Viber, Pinterest, entre outras.

3. PERSPETIVAS/DIRETRIZES

Com o aumento exponencial da quantidade de dados digitais gerados a cada minuto no mundo e sendo esses dados cada vez mais valiosos, pois representam informação, surge a *Big Data*. Esta representa uma nova era na sociedade moderna, mudando a forma como a economia e a ciência observam os processos, extraem e geram valor desse caos de dados.

A análise automática dos dados gerados nas redes sociais e processados pela *Big data* permitem extrair conhecimento (*insights*) e traçar perfis com base em padrões de comportamento dos utilizadores da *internet*.

Esta perspetiva é adotada por vários setores da sociedade com a finalidade de obterem informações que lhes permitam atuar nos diferentes mercados.

Vejamos agora de que forma estas ciências tecnológicas podem ser igualmente adotadas na PSP numa perspetiva de ciberpoliciamento das redes sociais.

3.1. Análise de dados por *Big Data*

3.1.1. *Big Data*

O termo *Big Data* é um conceito que surgiu com um trabalho de investigação nas áreas de análise e visualização de dados (Vasconcelos e Barão, 2017) que descreve o grande volume de dados estruturados, semiestruturados e não estruturados que são gerados a cada segundo na *internet* e que não podem ser processados por ferramentas convencionais de processamento de dados.

Segundo Saisse (2017), *Big Data* pode ser considerado como uma região de conhecimento transversal que abrange diversas áreas produtivas e pesquisas científicas. É um método concebido para gerar conhecimento e inteligência a partir de grandes quantidades de dados complexos e desorganizados.

Para Antunes e Rodrigues (2018, p. 30), o termo *Big Data* refere-se ao conjunto gigantesco de dados que resultam normalmente da escrita em massa para a *cloud* e que são recolhidos e "analisados computacionalmente com o objetivo de identificar padrões, associações e tendências relacionadas com um determinado negócio ou atividade".

Relacionado com o conceito *Big Data* existem os denominados 5Vs que caraterizam a informação numa espécie de cinco dimensões e que pode ser retirada da *Big Data* e que constituem desafios para a gestão e preparação desses dados:

- **Volume** – Quantidade de informação armazenada e que está em constante crescimento, assim como os dispositivos de armazenamento, incluindo a *cloud* que guarda dados já na ordem de peta e zeta *bytes* (Antunes e Rodrigues, 2018);
- **Variedade** – Diversidade de dados criados e consumidos em diferentes formatos como dados multimédia, ficheiros áudio, vídeo, imagens e de diferentes fontes como os serviços *web*, e-mail, redes sociais, fóruns, *blogs*, *smartphones*, *IoT*[4], entre outros;
- **Velocidade** – Possibilidade de dados em tempo real, dada a permanente evolução das TIC e das infraestruturas físicas de ligação das redes, baseadas na fibra ótica que permite ainda mais velocidade de criação de dados bem como o seu processamento, tratamento e análise;
- **Veracidade** – Confiança, confiabilidade, consistência e origem dos dados. Refira-se que apesar dos dados provenientes das redes sociais serem por natureza subjetivos (não estruturados), estes são "amplamente analisados e escrutinados pela *big data*, pois podem conter informação relevante para a tomada de decisão (Antunes e Rodrigues, 2018);
- **Valor** – Diz respeito à relevância dos dados após o processamento e o tratamento dos dados em bruto no sentido de acrescentar valor à empresa, melhorar os resultados e disponibilizar informação estratégica.

É esta análise de dados que vai permitir criar a inteligência. Sem uma análise correta e criteriosa é impossível criar *insights* que possam depois indicar o caminho a seguir, daí a análise de dados ser uma das etapas mais importantes do processo em que o *big data* está inserido.

Existem análises avançadas que são compostas por várias técnicas diferentes e capazes de realizar, por exemplo, análises preditivas, exploração de dados, estatísticas, entre outros. Se juntarmos o *big data* com essas análises temos o *Big Data Analytics* que pode ser definido como a aplicação de técnicas informáticas analíticas avançadas no *big data* (Williams, 2016).

[4] IoT – *Internet of Things* (a *Internet* das coisas). Compreende todos os aparelhos e objetos que se encontram habilitados a estarem permanentemente ligados à *Internet*, sendo capazes de se identificar na rede e de comunicar entre si com capacidade para recolher imensa quantidade de informação sobre o que os rodeia. Veículos, eletrodomésticos, câmaras de vigilância, detetores de condições ambientais, sensores de presença, *smart TVs* e dispositivos médicos são apenas alguns exemplos do que hoje já existe no universo da IoT.

3.1.2. *Big Data Analytics*

A *Big data analytics* é todo o processo que vai permitir o cruzamento de dados. É uma espécie de ciência tecnológica que examina dados brutos com o objetivo de encontrar padrões e tirar conclusões sobre essa informação, aplicando um processo algorítmico ou mecânico para obter informações (*insights*).

Numa perspetiva das novas tecnologias, são ferramentas que utilizam modelos de algoritmos computacionais para decifrar dados para a tomada de decisão, sendo que os algoritmos são mecanismos de reconhecimento de padrões.

Com esta ferramenta extraímos, tratamos, organizamos e compreendemos os dados "em bruto" e transformámo-los em informação útil para auxiliar na tomada de decisão, seja ela qual for. Segundo Leskovec, *et al*., (2014), estas ferramentas estão preparadas para o processamento de dados estruturados, semiestruturados e não estruturados, o que permite uma melhor compreensão dos mesmos e antecipar possíveis comportamentos, gerando *insights* contínuos em tempo real.

Assim, a *big data analytics* constitui um auxiliar na tomada de decisões em várias áreas como os negócios, ciências, educação, saúde, defesa, (Tien, 2013), comércio eletrónico, inteligência de mercado, governo e segurança (Chen *et al*., 2012), atendimento ao cliente e segurança da informação (Soares, 2012).

Da mesma forma, dadas as potencialidades da *big data analytics*, também pode ser utilizada para monitorizar de forma contínua as redes sociais e explorar as relações entre amigos e as várias redes sociais para identificar fraude em tempo real (McAfee, A. *et al*. 2012).

A análise de dados efetuada pela *big data analytics* pode ser classificada em prescritiva, diagnóstica, descritiva e preditiva (Saisse, 2017). A **análise prescritiva** baseia-se no estudo de casos ou factos e possíveis consequências sobre decisões tomadas. É o tipo de análise utilizada para identificar quais os resultados esperados para cada ação tomada. Já a **análise diagnóstica** tem em conta a história dos eventos ocorridos para viabilização de tomadas de decisão baseadas em factos. É a análise que responde às perguntas de quem, quando, onde e porquê.

Por outro lado, na **análise Descritiva** existe uma análise de dados em tempo real. É a principal forma de resposta ao presente, ou seja, é a exploração dos dados captados para percebermos o seu significado originando respostas para aquele momento atual. Por fim, na **análise preditiva** existe como que uma previsão do futuro. Utiliza a exploração de

dados históricos para traçar tendências futuras ou possibilidades futuras. É o que já se faz com o denominado policiamento preditivo.

3.1.3. Policiamento preditivo

O termo policiamento preditivo (PP), originário do termo anglo-saxónico *Predictive Policing* é um conceito ainda relativamente recente nas forças de segurança, assim como no meio académico. De forma muito genérica, podemos definir este PP como um policiamento efetuado através da previsão, ou seja, usando ferramentas de análise de dados criminais aferir-se futuros comportamentos criminosos e atuar antes que eles ocorram.

O PP assenta na ideia de análise e fusão de dados, mesmo aqueles que não têm natureza policial, de forma a delinear a atuação da Polícia numa perspetiva do que poderá acontecer, direcionando os meios de forma mais eficiente (Fernandes, 2014). É qualquer tática ou estratégia policial que utilize informação e métodos avançados de análise que permitam antever e atuar preventivamente sob o crime (Uchida 2009).

Como nos diz Clemente (2006), no PP a Polícia recolhe informação para antecipar a prevenção, isto é, para trabalhar na prevenção da prevenção, desempenhando assim uma tarefa de previsão e que deverá estar a cargo dos serviços de informações.

Nas palavras de Ferguson, (2012), PP consiste na utilização de *software* que auxiliará a prever locais onde é mais provável que ocorrerão crimes no futuro, utilizando estatísticas criminais e outros tipos de dados. Para Pearsall (2010), o PP depende de informação e das respetivas técnicas de análise, de teorias criminológicas e algoritmos preditivos de modo a alcançar uma diminuição dos índices criminais.

3.1.4. Ciberpoliciamento das redes sociais – O recurso à ciência tecnológica

O ciberpoliciamento é um conceito ainda indefinido, cuja literatura existente é escassa, sendo um termo que se encontra em construção. Neste sentido, se pensarmos que policiamento é o ato de policiar que se consubstancia em vigiar, guardar, controlar, proteger, zelar por algo, seja pessoa, espaço ou objeto físico, diremos que ciberpoliciamento é tudo isto mas aplicado ao mundo virtual, ao ciberespaço. É como que patrulhar de forma preventiva a *internet* e a *web*, nomeadamente as redes sociais.

Ora este processo de patrulhamento preventivo das redes sociais não pode ser efetuado apenas pela ação humana, dada a impossibilidade natural de termos pessoas à frente de inúmeros computadores a tentar vigiar as redes sociais, o que é impossível.

As redes sociais são por natureza fontes abertas de informação[5] e a PSP, de uma forma natural, recorre a estas *OSINT* para recolher dados e informações no processo de produção de inteligência, que visa obviamente auxiliar na prática o trabalho da PSP, nomeadamente na organização da segurança de grandes eventos. Para isso, a PSP monitoriza as redes sociais e vai acompanhando os *posts* ou conteúdos publicados sobre determinando evento e os seus comentários a fim de recolher informação útil e que possa interessar à tomada de decisão em termos de ação policial.

Mas o que entendemos como ciberpoliciamento não é apenas este recurso da PSP às *OSINT* mas antes um policiamento digital e preventivo de atividades delituosas que são executadas *online*, podendo ou não haver contacto físico entre os criminosos e as vítimas. É a PSP ter a capacidade de prever que determinados padrões de comportamento nas redes sociais constituem atos preparatórios de uma atividade delituosa e intervir antes que o crime ocorra, ou seja, atuando preventivamente no espaço digital tal e qual como se de um espaço físico se tratasse.

O desenvolvimento de capacidades que permitam à PSP efetuar ciberpoliciamento nas redes sociais só poderá ser feito com recurso às ciências tecnológicas, sendo que a perspetiva é o recurso à *big data analytics* em conjunto com a ação humana e na dependência dos serviços de *intelligence* da PSP.

Para que esta perspetiva seja possível propomos que a PSP crie parcerias com o meio académico, em especial com universidades capazes de projetar e desenvolver algoritmos computacionais que permitam a monitorização automática das redes sociais e interpretar os dados, tendo em conta as caraterísticas dos crimes que a PSP entender mais importantes para desenvolver a sua atividade de prevenção criminal.

Segundo Dickey (2016), algoritmos são conjuntos de regras que os computadores seguem para resolver problemas e tomar decisões sobre determinada tarefa.

Estes algoritmos, através da combinação automática de um conjunto de regras e variáveis predefinidas, constituiriam uma espécie de inteligência artificial com capacidade de traçar perfis, e tendências de atuações ilícitas com base em padrões de comportamento.

[5] As fontes abertas de informação, ao nível da inteligência, são denominadas por OSINT (Open source intelligence ou Inteligência de Fontes Abertas). É o termo usado no sentido de informações obtidas através de dados disponíveis para o público em geral.

Conforme refere Júnior (2017), trata-se de um projeto cuja ideia é possibilitar a procura de dados em redes sociais através de *posts* publicados, ou identificar eventos que podem acontecer baseados no volume de discussão a respeito de um tema.

A nível internacional são já várias as polícias que utilizam estas ferramentas informáticas. Como exemplo, referimos apenas o Departamento de Polícia de Los Angeles (LAPD), que juntamente com a Universidade da Califórnia, desenvolveu um *software* chamado "*PredPol*" (Preditive Policing Software), com o objetivo de usar dados da *big data* para auxiliar as polícias na identificação de problemas relacionados com a criminalidade e possíveis soluções que auxiliem na gestão de recursos e escolha de estratégias para prevenção de ocorrências futuras (Pinheiro, 2018).

Relativamente à prevenção criminal, Tasinaffo (2018) refere que a *big data* é de extrema importância, sendo que nos EUA a *Big Data* é utilizada desde 2011 para análise preventiva de ações criminosas permitindo uma atuação antecipada da polícia, havendo mesmo casos em que potenciais criminosos foram previamente abordados mesmo antes da ocorrência de qualquer crime**.**

Conforme podemos constatar e como resposta à nossa pergunta de investigação, o recurso às ciências tecnológicas para uso na atividade policial é possível. O recurso à *big data analytics*, através do desenvolvimento de algoritmos computacionais adequados permitiriam, estamos em crer, a implementação do ciberpoliciamento na PSP.

Este ciberpoliciamento teria de ser complementado com a ação de analistas dos serviços de informações para a produção de *intelligence* que auxiliaria a PSP nas diferentes tomadas de decisão na prevenção do ciberespaço. Esta seria uma tarefa conjunta entre a máquina e o Homem.

4. CONCLUSÃO

As últimas décadas foram marcadas pela evolução e disseminação das novas tecnologias e da *internet*, o que veio permitir por um lado o aumento exponencial de utilizadores destas ferramentas e por outro, um enorme aumento de dados e conteúdos trocados *online* de forma sistemática e instantânea.

O ciberespaço comporta um ambiente virtual, global e sem fronteiras que permite uma diversidade de atividades, quer ao nível empresarial, governamental, estatal ou pessoal. Este é considerado como um novo espaço de intervenção em que por vezes a realidade se confunde com o virtual, devendo ser acedido com responsabilidade.

Quando acedemos à *internet* deixamos várias pegadas no mundo digital, como as pesquisas sobre algo que pretendemos fazer ou publicações e isso vai ficando depositado na *web*, o que constitui um verdadeiro rasto.

Ao acedermos a uma rede social virtual há muita informação que fica disponível, quer sejam publicações, os denominados *posts*, *likes* ou partilhas. Tudo isso são dados que vamos deixando e que ficam armazenados e relacionados connosco, o que permite depois relacionar esses dados aos utilizadores de *internet* e nomeadamente de redes sociais.

Da mesma forma, ao nível empresarial, sempre que acedemos a algum serviço da *web*, seja por computador, *smartphone*, ou outro, as empresas, através de ferramentas tecnológicas, tentam perceber quem está a aceder à *internet* e tentam compreender o que aquele utilizador procura de forma a poder traçar um perfil.

As redes sociais digitais são as plataformas da *web* ideais para sustentar e dar expressão a toda esta dinâmica e podem ser definidas como comunidades virtuais de indivíduos que partilham os mesmos interesses, objetivos, causas ou valores e que utilizam o ciberespaço para se relacionarem entre si.

A expansão das redes sociais virtuais e as suas potencialidades apresentam vantagens e desvantagens, pois conjuntamente com esta dinâmica de oportunidades que as redes sociais possibilitam, surgem de forma natural atividades delituosas tal e qual como se do mundo físico se tratasse.

Aliás, há atividades ilícitas que são concretizadas no mundo físico cuja relação de conhecimento iniciou-se no mundo virtual, numa rede social ou num *chat* qualquer. É este tipo de perigos que as redes sociais comportam e que devemos prestar atenção.

Daqui resulta que alguns destes perigos constituem crime, o designado cibercrime e que podemos descrever como a prática de um ato criminoso realizado através do

ciberespaço, da *internet* e dos computadores. Para a cibercriminalidade existe legislação nacional e internacional que enquadra devidamente este tipo de crimes.

Numa perspetiva de segurança do ciberespaço existe o conceito de cibersegurança que, segundo Ralo (2013), baseado em programas informáticos, constitui o conjunto de atividades de monitorização, prevenção e resposta às ameaças que possam colocar em risco o ciberespaço, cabendo às forças e serviços de segurança o seu eficaz policiamento.

No entanto, no que à intervenção das polícias diz respeito, esta surge num momento após a prática do crime, cuja ofensa ao bem jurídico protegido já fora cometida, pois não é possível às polícias, apenas pela ação humana, monitorizarem todo um conjunto de dados existente no ciberespaço e atuarem antes da concretização de um cibercrime.

Os dados que falamos são criados por máquinas na sua relação com o Homem. O fenómeno da *IoT* tende a generalizar-se e atualmente apenas uma parte desses dados criados pela *IoT* é analisada, pois os *softwares* existentes ainda não conseguem suportar a imensidão de dados produzidos (Antunes e Rodrigues, 2018).

A extração desses dados normalmente exige um investimento, um *software* especializado ou empresas dedicadas a este tipo de serviços para se conseguir retirar da imensidão de dados a informação que se pretende. "A *big data* permite decisões eficazes e o aperfeiçoamento dos processos" (Antunes e Rodrigues, 2018, p. 36).

Big data representa o conjunto enorme e variado de dados que são guardados por todos nós à medida que navegamos na *internet* e que se forem bem trabalhados originam *insights* que ajudam na tomada de decisões. Esta ferramenta tecnológica surgiu no mundo empresarial com o objetivo de identificar hábitos de consumo dos utilizadores que frequentam as redes sociais e assim obterem o máximo de potenciais clientes. Esta análise de dados que é feita por *softwares* especializados permite às empresas obterem perfis de utilizadores com base em padrões de comportamento.

Este cruzamento e análise de dados que as ciências tecnológicas permitem fazer através da *big data analytics* pode ser usado não só pelas empresas, mas também pelas Polícias na criação de perfis de utilizadores, com base em determinados padrões de comportamento, que pode ser crucial para a atividade policial. Para Hansen, Shneiderman e Smith (2011), a análise de redes sociais é uma aplicação do campo da ciência das redes sociais para estudar as conexões e relacionamentos humanos.

O policiamento preditivo é já um exemplo de como as ciências tecnológicas auxiliam a polícia na sua atividade. O PP utiliza as novas tecnologias algorítmicas para prever locais onde possam ocorrer crimes e atuar preventivamente. Este surgiu também

com base nas análises que o mundo empresarial faz com recurso ao *business intelligence* e *business analytics* e das suas técnicas e ferramentas de análise como *data mining*, *hot spots*, previsão geoespacial, análise de redes sociais e probabilidades estatísticas mas aplicadas à atividade policial.

Neste contexto, tendo por base a génese do policiamento preditivo, a análise de dados da *big data analytics* em conjunto com a criação de um algoritmo tecnológico pode representar uma opção no ciberpoliciamento das redes sociais.

A produção de *intelligence* é da responsabilidade dos serviços de informação da PSP pelo que o ciberpoliciamento deve situar-se nestes serviços.

O mundo académico é o espaço, por excelência, onde este tipo de ferramentas podem ser idealizadas e concebidas através da investigação científica que estas instituições de ensino superior comportam. Cabe à PSP a disponibilidade para colaborar e obter conhecimento científico capaz de auxiliar na atividade policial, com novos métodos e novas ferramentas por uma segurança pública melhor, mais eficaz e eficiente.

A atualidade, a evolução das sociedades e das tecnologias representam oportunidades mas também comportam problemas de segurança. O século XXI constituirá um permanente desafio para as polícias. Estas devem estar permanentemente preparadas e atualizadas para poderem adotar estratégias de segurança pública de forma diversificada e acompanhar a evolução tecnológica, constituindo o ciberpoliciamento um grande passo.

Quanto a futuras investigações, propomos uma abordagem ao direito à privacidade relativamente à monitorização dos dados de navegação na *internet* e nas redes sociais em particular para efeitos de ciberpoliciamento e prevenção criminal das forças de segurança.

REFERÊNCIAS BIBLIOGRÁFICAS

Akdeniz, Y., Walker, C., & Wall, D. (2001). *The Internet, Law and Society*. Harlow: Pearson Education.

Antunes, M. & Rodrigues, B. (2018). *Introdução à Cibersegurança - A Internet, os Aspetos Legais e a Análise Digital Forense*. Lisboa: FCA Editora.

APA. (2010). *Publication Manual of the American Psychological Association* (6.a Edição). Washington, DC: American Psychological Association.

Cardoso, G. (2011). *Mudança social em rede. Políticas sociais: ideias e práticas*. Lisboa: Centro Ruth Cardoso.

Cardoso, G. & Lamy, C. (2011). Redes sociais: comunicação e mudança. *JANUS.NET. ejournal of International Relations*, vol. 2 (1). Retrieved from htp://observare.ual.pt/janus.net/images/stories/PDF/vol2_n1/pt/pt_vol2_n1_art6.pdf

Castells, Manuel (2005). *A Sociedade em Rede: do Conhecimento à Política*. Lisboa: Imprensa Nacional Casa da Moeda.

Castells, M. (2007). *A Galáxia Internet: reflexões sobre Internet, Negócios e Sociedade*. Lisboa: Fundação Calouste Gulbenkian.

Cervo, A. L. & Bervian, P. A. (1996). *Metodologia Científica*. 4.ª Edição. São Paulo: Makron Books.

Chen, H., Chiang, R. H. L. & Storey, V. C. (2012), Business intelligence and analytics: From big data to big impact . *MIS Quarterly*. V. 36, n.º 4, PP. 1165-1188. Retrieved From https://pdfs.semanticscholar.org/f5fe/b79e04b2e7b61d17a6df79a44faf358e60cd.pdf.

Clemente, P. (2008). Informações e policiamento: conhecer e agir. *Revista Polícia Portuguesa*, 7, 34-38.

Decreto-Lei n.º 69/2014, de 09 de maio. Procede à segunda alteração ao Decreto-Lei n.º 3/2012, de 16 de janeiro, que aprova a orgânica do Gabinete Nacional de Segurança, estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança. Diário da República, 1.ª série, n.º 89, 2712-2719.

Despacho n.º 13692/2013, de 28 de outubro (2013). Orientação política para a ciberdefesa em Portugal. *Diário da República* n.º 208, série II, 31976-31979.

Dickey, M. (2016) Algorithmic accountability. Retrieved from https://techcrunch.com/2017/04/30/algorithmic-accountability/.

Dijck, J. (2013). *The Culture of Connectivity: A Critical History of Social Media*, New York: Oxford University Press.

Elias, L. (2019). Cyberlaw. CIJIC, Direito: a pensar tecnologicamente. Ciberameaças e (In) segurança. *Revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa*, 7. Retrieved from https://www.cijic.org/wp-content/uploads/2019/05/Luis-Elias_CIBERAMEAÇAS-E-INSEGURANÇA.pdf.

Europol. (2013). European Cybercrime Centre - EC3: *Combating crime in a digital age*. Retrieved July 02, 2019, from https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

Ferguson, A. G. (2012). Predictive policing and reasonable suspicion. *Emory Law Journal*, 62, 259-320.

Fernandes, J. P. T. (2013). Cibersegurança: Utopia, liberdade e soberania no ciberespaço. *Nação e Defesa* - Revista do IDN, 133, 11-31. Retrieved from https://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD133.pdf.

Fernandes, L. F. (2014). *Intelligence e segurança interna*. Lisboa: ISCPSI.

Gama (2017). *Big Data* como ferramenta para a polícia. Retrieved from https://gamademedeiros.com.br/big-data-como-ferramenta-para-policia/.

Ghernaouti, S. (2013). Cyber Power: Crime, conflict and security in *cyberspace*. Lausanne: EPFL Press.

Gibson, W. (1984). *Neuromancer*. Tradução de Fernando Correia Marques. Lisboa: Gradiva.

Hansen, D. L., Shneiderman, B. & Smith, M. A. (2011). *Analysing Social Media Networks with NodeXL: Insights from a Connected World*. Burlington: Morgan Kaufmann.

Júnior, S. (2017). *Big data* contra o crime. Retrieved from https://www.linkedin.com/pulse/big-data-contra-o-crime-efeito-minority-report-renan-saisse/.

Kaplan, A. M. & Haenlein, M. (2010). *Users of the world, unite! The challenges and opportunities of social media.* Business Horizons, 53, 59-68. Retrieved from http://michaelhaenlein.eu/Publications/Kaplan,%20Andreas%20-%20Users%20 of %20the%20world,%20unite.pdf.

Kato, R. (2014). Tecnologia: *Big Data* contra o crime. Retrieved from https://exame.abril.com.br/tecnologia/big-data-contra-o-crime/.

Keyser, M. (2003). The Council of Europe Convention on Cybercrime. *Journal of Transnational Law & Policy*, 12, 287–327.

Kuehl, D. (2009). *From Cyberspace to Cyberpower: Defining the problema*. Retrieved from https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210.

Lempert, P. (2006). Caught in the Web. *Progressive Grocer*, 85(12), 15-28.

Leskovec, J., Rajaraman, A., & Ullman, J. (2014). Link Analysis. Mining of Massive Datasets, 163–200. Retrieved from http://i.stanford.edu/~ullman/mmds.html.

Lévy, P. (2000). *Cibercultura*. Lisboa: Instituto Piaget.

Lévy, P. (2000). *Filosofia world. O mercado, o ciberespaço, a consciência*. Lisboa: Instituto Piaget.

McAfee, A. & Brynjolfsson, E. (2012). Big Data: The management revolution. *Harvard Business review,* V. 90, (10), 60-66. Retrieved from https://hbr.org/2012/10/big-data-the-management-revolution.

Natário, Rui M. P. (2013). O Combate ao Cibercrime: Anarquia e Ordem no Ciberespaço. Retrieved from https://www.revistamilitar.pt/artigo/854.

O'Reilly, T. (2005). *What is web 2.0: Design patterns and business models for the next generation of software*. Retrieved from <http://www.elisanet.fi/aariset/Multimedia/Web2.0/What%20Is%20Web%202.doc >.

Parker, D. (1998). *Fighting Computer Crime: A New Framework for Protecting Information*. Canadá: John Wiley & Sons.

Patrício, R. & Gonçalves V. (2010). *Facebook: rede social educativa?* Retrieved from https://bibliotecadigital.ipb.pt/bitstream/10198/3584/1/118.pdf.

Pearsall, B. (2010). Predictive policing: The future of law enforcement? *National Institute of Justice Journal*, (266), 16-19.

Pinheiro, J., (2018). Como a polícia de Los Angeles usa *big data* para prever crimes. Retrieved from https://canaltech.com.br/seguranca/entenda-como-a-policia-de-los-angeles-usa-big-data-para-prever-crimes-114390/.

Quivy, R. & Campenhoudt, L. V. (2005*). Manual de Investigação em Ciências Sociais*, 4.ª Edição, Lisboa: Gradiva.

Ralo, J. (2013). CiberSegurança e CiberDefesa. In Direcção-Geral de Política de Defesa Nacional. Retrieved from: http://dgpdn.blogspot.com/2013/03/artigo-de-opiniao-ciberseguranca-e.html.

Rashtchy, S., Kessler, A. M., Bieber, P. J., Schindler, N. H. & Tzeng, J. C. (2007). *The user revolution: The new advertising ecosystem and the rise of the Internet as a mass medium.* Retrieved from http://people.ischool.berkeley.edu/~hal/Courses/StratTech09/Lectures/Google/Articles/user-revolution.pdf.

Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho (2019). Aprova a Estratégia Nacional de Segurança do Ciberespaço (ENSC). *Diário da República* n.º 108, 1.ª série, 2889-2895.

Saavedra, R. (1998). *A proteção jurídica do software e a internet*. Lisboa: Publicações Dom Quixote.

Saisse, R. (2017). *Big Data contra o crime: efeito Minority Report*. Retrieved from http://direitoeti.com.br/artigos/big-data-contra-o-crime-efeito-minority-report/#_edn1.

Sarmento, M. (2013). *Metodologia Científica para a Elaboração, Escrita e Apresentação de Teses*. Lisboa: Universidade Lusíada Editora.

Soares, S. (2012), A Framework that focuses on the "data" in big data governance. *IBM data magazine*. Retrieved from https://www.ibmbigdatahub.com /blog/framework-focuses-data-big-data-governance.

Tasinaffo, F. (2018). A utilização do *Big Data* para prevenção de crimes**.** Retrieved from https://canalcienciascriminais.com.br/big-data-prevencao-crimes/.

Tien, J. (2013). Big Data: Unleashing information. Journal of systems sciences and systems engineering, Vol. 22, (2), 127-151. https://doi.org/10.1007/s11518-013-5219-4.

Uchida, C. D. (2009). *A national discussion of predictive policing: Defining our terms and mapping successful implementation strategies*. Washington, DC: National Institute of Justice.

UE (2013). Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido - *Comunicação conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*. Retrieved from https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:PT:PDF.

UE, (2013). Regulamento n.º 526/2013 do Parlamento Europeu e do Conselho relativo à Agência da União Europeia para a Segurança das Redes e da Informação (ENISA). Retrieved from https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013R0526&from=pt

UN, (2000). Crimes related to computer networks: Background paper for the workshop on crimes related to the computer network. *10th UN Congress on the Prevention of Crime and the Treatment of Offenders*. Retrieved from https://digitallibrary.un.org/record/432663/files/A_CONF.187_15-EN.pdf.

UNODC, (2013). *United Nations Office on Drugs and Crime: Comprehensive Study on Cybercrime.* Retrieved from https://www.unodc.org /documents/organized-crime/UNODC_CCPCJ_EG.4_2013/ CYBERCRIME_STUDY_210213.pdf.

Vasconcelos, J. & Barão, A. (2017). *Ciência dos dados nas organizações. Aplicações em Python*. Lisboa: FCA - Editora de informática.

Verdelho, P., Bravo, R., & Rocha, M. L. (2002). *Leis do Cibercrime*. Vol. I. Lisboa: Centro Atlântico.PT.

Verdelho, P. (2003). Cibercrime. *Direito da Sociedade da Informação*. Vol. IV. Associação Portuguesa do Direito Intelectual. Coimbra: Coimbra Editora.

Williams, S. (2016). *Business intelligence strategy and big data analytics: a general management perspective*. Cambridge, MA: Morgan Kaufmann.