Universidade do Minho
Escola de Direito

Hugo André Pinto Fangueiro

Autópsia Digital às Tecnologias de Informação: a licitude do *Intelligence* e as injunções jurídicas, criminais e forenses

janeiro de 2020

Autópsia Digital às Tecnologias de Informação: a licitude do *Intelligence* e as injunções jurídicas, criminais e forenses
Hugo André Pinto Fangueiro
UMinho | 2020

Universidade do Minho
Escola de Direito

Hugo André Pinto Fangueiro

Autópsia Digital às Tecnologias de Informação: a licitude do *Intelligence* e as injunções jurídicas, criminais e forenses

Dissertação de Mestrado
Mestrado em Direito e Informática

Trabalho efetuado sob a orientação do
Professor Doutor Pedro Miguel Freitas
e do
Coronel Doutor Paulo Viegas Nunes

janeiro de 2020

DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS

AGRADECIMENTOS

A presente tese é o produto da investigação na área jurídica, criminal e forense, com uma especial abordagem sobre o *Intelligence*.

Quero publicamente agradecer à Faculdade de Direito da Universidade do Minho, ao Senhor Professor Doutor Pedro Miguel Freitas, ao Senhor Professor Doutor Francisco Pacheco de Andrade e ao Senhor Coronel Doutor Paulo Viegas Pires. Pretendo ainda reconhecer o incrível auxílio e a predisposição do Sr. Eurodeputado Dr. Carlos Coelho e do Dr. Augusto Meireis pelos apontamentos concedidos.

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

RESUMO

Autópsia Digital às Tecnologias de Informação: a licitude do *Intelligence* e as injunções jurídicas, criminais e forenses

O *Intelligence* sempre existiu desde que há vida humana, mas as Tecnologias da Informação e os seus meios digitais transferem-no para outros patamares de pertinência. Logo, deverá ser acompanhado de perto pelas áreas jurídico, criminal e forense.

O *Intelligence*, hoje mais do que nunca, muitas vezes tem como método a autópsia digital às Tecnologias da Informação. Portanto, também outras pertinências se arguem, tais como, a sua necessidade, proporcionalidade e adequação.

Atualmente, a sociedade vive intensamente as Tecnologias da Informação, fazem-no não só indivíduos pró-sociais mas também os inimigos da comunidade, e é sobre estes últimos que deverá recair maioritariamente a autópsia digital. Mas as declarações, as diretivas, as constituições e as leis, que salvaguardam e protegem uns |Pró-sociais|, também protegem os outros |inimigos da sociedade|, e é nesse sentido que aponta, fundamentalmente, esta tese: ponderar os dois lados.

Esta tese vai levantar algumas celeumas e vai também enaltecer e criticar os efeitos jurídicos, criminais e forenses.

As autópsias digitais são levadas a cabo por muitos Estados, mas em diferentes circunstâncias e em diferentes situações, suportando-se em diversas injunções jurídicas, criminais e forenses. Assim, esta tese vai também retratar o *Intelligence* por parte das Organizações Governamentais Internacionais e Nacionais.

A cada nova tecnologia da informação intensifica-se um novo *modus operandi* dos criminosos, novos crimes, novas formas de crimes.

Para dificultar a segurança, o fenómeno do *Intelligence* vive em constante penumbra. Todos sabem que ele existe, todos sabem que é levado a cabo, mas as leis continuam sem permitir grande parte do *Intelligence* desejado.

Uma das tarefas fundamentais do Estado Português é garantir a independência nacional e criar as condições políticas, económicas, sociais e culturais, neste âmbito, entre outros, o terrorismo, o crime organizado, têm de ser fortemente supervisionados pelas Instituições legitimadas para o efeito, em virtude de se camuflarem cada vez mais na panóplia de tecnologias digitais.

Portanto, ponderar o direito à segurança, em detrimento de algumas salvaguardas constitucionais e legais, favoreceria um melhor Estado.

Palavras-chave: comités de Informação, força jurídica, *intelligence*, recolha de Informações.

ABSTRACT

Digital autopsy to Information Technology: the lawfulness of *Intelligence* and the legal, criminal and forensic injunctions

Intelligence has existed since human life, but Information Technology and its digital media transfer it to other levels of relevance. Therefore, it should be closely monitored by the legal, criminal and forensic areas.

Intelligence, today more than ever, often has as its method the digital autopsy to Information Technologies. Therefore, other pertinences are also argued, such as its necessity, proportionality and adequacy.

Nowadays, society lives intensely in Information Technologies, not only pro-social individuals but also the community's enemies, and it is on these that digital autopsy must fall. But statements, directives, constitutions and laws, which safeguard and protect some |pro-social |, also protect the other |enemies of society, and it is in this sense that this thesis fundamentally points: to weigh both sides.

This thesis will raise some stir and will also praise and criticize the legal, criminal and forensic effects.

Digital autopsies are carried out by many States, but under different circumstances and in different situations, and are supported by various legal, criminal and forensic injunctions. Thus, this thesis will also portray Intelligence by International and National Government Organizations.

With each new information technology, a new modus operandi of criminals, new crimes, new forms of crime intensifies.

To make security more difficult, the Intelligence phenomenon is constantly in the dark. Everyone knows it exists, everyone knows it is carried out, but the laws still do not allow much of the desired Intelligence.

One of the fundamental tasks of the Portuguese State is to guarantee national independence and to create the political, economic, social and cultural conditions. In this context, terrorism and organised crime, among others, must be strongly supervised by the institutions legitimised for this purpose, as they are increasingly camouflaged in the panoply of digital technologies.

Therefore, weighing the right to security over some constitutional and legal safeguards would favour a better state.

Keywords: information committees, information gathering, intelligence, legal force.

ÍNDICE

ÍNDICE DE IMAGENS

ACRÓNIMOS

ANS – Autoridade Nacional de Segurança

CCOM – Comando Conjunto para as Operações Militares

CEGER – Centro de Gestão da Rede Informática do Governo

CIA – Central Intelligence Agency

CISMIL – Centro de Informações e Segurança Militares

CNC – Centro Nacional de Cibersegurança

COMINT – Communications Intelligence

CRP – Constituição da República Portuguesa

DIPLAEM – Divisão de Planeamento Estratégico Militar

DIRCSI – Direção de Comunicações e Sistemas de Informação

DLG – Direitos Liberdades e Garantias

DP – Direito Penal

ELINT – Eletronics Intelligence

GNS – Gabinete Nacional de Segurança

FISC – Foreign Intelligence Surveillance Court

FISINT – Foreign Instrumentation Signals Intelligence

GECENI – Grupo de Estudos sobre Contributos para uma Estratégia Nacional de Informação

IETF – Internet Engineering Task Force

IMINT – Imagery Intelligence

INTEL – Intelligence

NI – National Intelligence

NSA – National Security Agency

OTAN – Organização Tratado Atlântico Norte

PCM – Presidência do Conselho de Ministros

SCEE – Sistema de Certificação Eletrónica e de Fiscalização – Infraestruturas de Chaves Públicas

SIGINT – Signal Intelligence

STASI – Ministerium für Staatssicherheit traduzido será Ministério para a Segurança do Estado

TI – Tecnologias de Informação

UKUSA – United Kingdom United States of America

As Tecnologias da Informação sabem mais sobre a pessoa,
do que o familiar mais próximo.

INTRODUÇÃO

CARATERIZAÇÃO GERAL

Apresenta-se o trabalho com o título Autópsia Digital às Tecnologias da Informação: a licitude do *Intelligence* e as injunções jurídicas, criminais e forenses como tese para a obtenção de grau de mestre em Direito e Informática.

O tema escolhido foi motivado por duas grandes inquietações: a primeira diz respeito à descodificação do verdadeiro e real significado de *Intelligence*, dos seus respetivos segmentos e de todas as implicações daí resultantes; a segunda, à qual procuraremos responder neste trabalho de investigação, é a questão relativa à licitude do *Intelligence* e todas as injunções jurídicas, criminais e forenses que o *Intelligence* compreende. A par desta questão, a insuficiência de fontes literárias relativas às matérias do *Intelligence* motivou também a seleção do tema da presente tese, que tem o intuito da definição de conceitos, da exposição da arquitetura dos mais variados sistemas governamentais relativos a esta matéria e de todos os juízos imputados às instituições implicadas no *Intelligence*, bem como retratar o âmbito e a atribuição de matérias a cada uma das instituições implicadas.

Verificam-se imensas contradições implícitas ao *Intelligence* e que levaram também ao estudo de todas as antinomias entre *Intelligence*, privacidade, segurança, defesa, direitos, liberdades, garantias, entre outros.

Assim sendo, pretende-se também analisar de forma crítica a Constituição da República Portuguesa, a Declaração Universal dos Direitos do Homem de 10 de dezembro de 1948, a Proteção dos Direitos do Homem e das Liberdades Fundamentais de 04 de novembro de 1950, bem como o Estatuto de Roma do Tribunal Penal Internacional, a Lei n.º 9/2007 relativa ao Sistema de Informações da República Portuguesa,[1] a Lei n.º 17/2006 do Quadro de Política Criminal, e as várias orientações de política criminal. A par disso, esta tese vai também dissecar as estratégias, os métodos e os meios utilizados no *Intelligence*, obtidos através dos objetos que operem informações representadas sob forma de dígitos associados a impulsos eletrónicos, o que inclui todas as atividades e soluções providas por recurso de computação, que visem permitir a produção, o armazenamento, a transmissão, o acesso e a segurança das Tecnologias da Informação.

1 Crítica à limitação dos funcionários e agentes do SIRP, SIS e SIED no exercício de poderes e prática de atos, conforme se prevê no seu n.º 2 do artigo 6º. Obtendo este normativo uma restrição no que se concerne às competência específica dos tribunais, do MP ou entidades com funções policiais, como é a título de mero exemplo as escutas.

Esta tese abordará uma integração de matérias jurídicas e informáticas, enaltecendo a própria informação enquanto bem jurídico autónomo, revelará também as questões inerentes às injunções jurídico, criminais e forenses por via telemática, que de grande relevância se revestirá para os órgãos de controlo social, sobretudo os que têm ligações ao *Intelligence*.

A atual Constituição da República Portuguesa reduz as probabilidades de sucesso, limitando, assim, o raio de ação do *Intelligence*.[2]

O aumento dos riscos atuais, decorrentes dos importantes desenvolvimentos tecnológicos, económicos e sociais, levam-nos a uma reanálise integral do senso da lei, tendo o legislador de, urgentemente, desenvolver medidas de forma a readaptar-se dentro da atual e complexa sociedade.

Hoje em dia, o controlo das Tecnologias da Informação vai muito mais além da supervisão das associações terroristas internacionalmente catalogadas, pois, o simples lobo solitário poderá causar um prejuízo muito maior à segurança nacional e à salvaguarda do Estado.

Assim sendo, o pensamento lógico de todos deveria ser o de que o controlo das Tecnologias da Informação estivesse muito além das instituições supranacionais.

Sabemos que a característica mais importante de uma comunidade é a sua vinculação estável às relações sociais, como a cultura, o trabalho, a política e a religião, mas, em Portugal, na Europa e no Mundo vive-se uma tensão crescente, aumentando as subculturas autoinventadas e motivadas por intenções religiosas, liberais ou anarquistas. O fundamentalismo reacende o declínio social, transportando-o a atos antissociais. Assim sendo, esta tese vai também abordar os Direitos Civis e Políticos e os Direitos Económicos, Culturais e Sociais, ambos de 16 de dezembro de 1966, contrapondo-os às constantes mudanças dos processos multidimensionais, que trarão o chamado terrorismo doméstico para dentro das nossas portas, o que, a verificar-se, colocará em causa a confiança dos cidadãos e a fiabilidade do Estado. A Teoria da Oportunidade desenrola-se entre a agonia e a incerteza, e as escolhas radicais têm a sua otimização através de redes de comunicação multimodal e nas Tecnologias da Informação.

Assim sendo, impõe-se uma reformulação das noções principais do *Intelligence*, a definição de estratégias, organizando-as por prioridades, impõe-se também a restruturação das próprias estruturas

2 Tal restrição Constitucional ao *Intelligence* verifica-se, entre outros, na CRP artigo 35.º n.3 *"A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis."* Tal situação obstará à catalogação individualmente identificável de radicais islâmicos, entre outros.

dos serviços que trabalham as informações, de forma a optimizar o fulcral papel do *Intelligence* na sociedade.

Trazer à lei a razão e a justiça, abordando a verdade positiva e negativa do *Intelligence*, trará às organizações que executam tarefas e funções sobre informações e segurança uma legitimidade pura sobre a recolha de metadados recebidos do exterior, onde se julgue uma ordem formal tendo em conta os princípios do direito, as conexões ao crime, o processo criminal, o foro judicial ou os tribunais.

Curar o *Intelligence* através da supervisão das pistas de interações virtuais permite não só perfilar pré-criminosos e antecipar comportamentos delitivos e os seus resultados, como também, harmonizar a montante, de forma mais eficaz, os meios pessoais e logísticos ao dispor dos órgãos de controlo social (autoridade judiciária, órgãos de polícia criminal, autoridade de polícia criminal, serviços de informações, entre outros).

Nesta tese pesar-se-á a necessidade, a proporcionalidade e a adequação na utilização do método do *Intelligence* por via da Autópsia Digital às Tecnologias da Informação. Este método é tão agressivo que deixará chagas para sempre no direito, na liberdade e nas garantias individuais e pessoais, sem esquecer, no entanto, o conjunto de prerrogativas e instituições que, em cada momento histórico, concretizam as exigências da liberdade, igualdade e dignidade entre seres humanos. Alvitraremos também a garantia de confiança na segurança tecnológica a todos os indivíduos pró-sociais, decretando a implementação na ordem jurídica portuguesa da teoria penal do inimigo, na comunidade do *Intelligence*, teoria essa defendida por Gunther Jakobs. Sustentaremos a citação, ainda que restrita, dos *"perigosos dissimulados"*[3] às instituições/organizações competentes, fazendo com que a restrição de alguns direitos fundamentais seja imposta a estes, e só a estes, na certeza, porém, da busca incansável da perfeita harmonia entre os direitos do indivíduo e os direitos da sociedade.

Esta tese vai responder às questões erigidas pela mesma, com enfoque nas que são levadas a cabo através das Tecnologias da Informação na curadoria do *Intelligence*. Este trabalho de investigação vai também demonstrar através de entrevistas anónimas a analistas/técnicos de informações a realidade verdadeira do *Intel*, manifestando os prós e os contras efetivos. Ao longo desta tese, o leitor vai sendo guiado através de passos sequenciais, deslindando pistas que irão vislumbrar um possível desfecho.

O desenlace encontra-se no capítulo da Proposta de Revisão e no subcapítulo Reflexões sobre o Estudo, através das lições apreendidas, mas sobretudo patente de forma inequívoca na Conclusão.

3 Tão bem retratada no livro de Direito Penal do Inimigo de Jacobs, onde se aborda a temática e onde se revelam as noções e as críticas tão bem justificadas a esta teoria.

APRESENTAÇÃO DO PROBLEMA

Os Serviços de Informações (SI) são hoje condicionados pelas leis e, sobretudo, pela Constituição da República Portuguesa, o que torna problemática a adoção de medidas operacionais por parte dos serviços que trabalham informações, impondo-se, por isso, com caráter de urgência, uma adaptação legal às realidades tecnológicas de hoje em dia.

É de referir que em agosto de 2015 foi chumbado o acesso dos SI a dados bancários e de comunicações, após o Presidente da República Portuguesa, à data o Prof. Dr. Aníbal Cavaco Silva, ter pedido a fiscalização ao Tribunal Constitucional que, por sua vez, chumbou o diploma que permitiria aos analistas/técnicos de informações terem acesso a dados bancários, fiscais, de tráfego e de comunicações de quem estivessem a (investigar) supervisionar.

Os metadados como a informação bancária, fiscal e tráfego de internet são maioritariamente intimados no n. 2 do artigo 78.º do Decreto 426/XII do Regime jurídico do Sistema de Informações da República Portuguesa, cuja intenção seria a de rever e alterar os meios e as formas de análise de informações.

A inconstitucionalidade da recolha dos metadados imperou nos Juízes de Ratão, afirmando que esta violaria o princípio constitucional da inviolabilidade das comunicações privadas. Dados, tais como, a localização, a hora e com quem uma pessoa comunica foram considerados uma intromissão. A par dessa consideração, os juízes não viram os SI como uma entidade capaz de supervisionar e controlar e justificaram a sua inconstitucionalidade por também considerarem que não seria garantido de forma suficiente o uso não abusivo da recolha de metadados.

Ainda que contando com divergências em alguns aspetos[4] por parte da Procuradoria-Geral da República, do Conselho Superior do Ministério Público, da Comissão de Fiscalização de Dados do SIRP e da Comissão Nacional de Proteção de Dados, alguns deputados concertaram algumas transformações à anterior lei-quadro, permitindo porventura aos técnicos superiores de informações do SIS e do SIED acederem a dados informáticos de pessoas que estivessem a ser (investigadas) supervisionadas. Assim, os serviços de informações poderiam aceder a dados de tráfego ou a dados de localização de cidadãos suspeitos de terrorismo, crimes de segurança contra o Estado ou alta criminalidade organizada.

4 *"Joana Marques Vidal, procuradora-geral da República, citou a jurisprudência do Tribunal Constitucional (TC) alegando que "o sigilo das telecomunicações" garantido na Constituição, abrange não só o conteúdo das comunicações mas também o tráfego como tal"*. Também o Conselho Superior do Ministério Público (CSMP), por seu lado, alegou uma *"perversa duplicação de meios, a prazo geradora de ineficácia, tanto mais que se confundem as lógicas de prevenção com as de repressão e não estão garantidos os mecanismos de introdução processualmente fiável e válida da informação com relevância criminal assim obtida"*. Secretas: Tribunal Constitucional chumba acesso das secretas a dados bancários e de comunicações in http://observador.pt/2015/08/27/tribunal-constitucional-chumba-acesso-das-secretas-a-dados-bancarios-e-de-comunicacoes/ em 27 de agosto de 2015.

Ainda assim, manter-se-ão muitas dúvidas por dissipar quanto à devassa por parte de algumas instituições que trabalhem estes metadados e, assim, estarão sempre à mercê da recorrente denúncia de inconstitucionalidade.

A reação da Comissão Nacional de Proteção de Dados falava em <<devassa>>, considerando que a nova lei das secretas violava cinco artigos da Constituição. "Permite o conhecimento de muitos aspetos da vida privada de cada um de nós, quando não mesmo, porque analisados no seu conjunto, toda a nossa vida privada, numa agressão grosseira aos direitos à privacidade e à proteção de dados pessoais e, em consequência, ao direito à liberdade, relatava".[5]

Assim sendo, existem já princípios constitucionais salvaguardados que vão continuar a ser abalroados a grande velocidade por outros princípios também estes constitucionalmente protegidos, Artigo 27.º - Direito à liberdade e à segurança da CRP, em detrimento do Artigo 34.º Inviolabilidade do domicílio e da correspondência da CRP, entre muitos outros.

Contudo, não poderemos fragmentar de forma direta os direitos constitucionais, a não ser que se invoque uma ordem jurídico-penal, pois só certos bens jurídicos é que se elevam à ordem penal, criando assim uma intrincada contenda, que só o intérprete (a jurisprudência e a doutrina) poderá legitimar através de uma mediação entre a ação e a determinação[6] espácio-temporal.
Portanto, fará todo o sentido alvitrar e anuir certas condições à violabilidade constitucional sobre alguns indivíduos.

O fenómeno jurídico, que coabita entre o Direito e a Informática, implicará um constante acompanhamento natural com a ciência e na evolução da sociedade.

As configurações económicas, políticas, sociais, culturais e tecnológicas trarão em simetria as solicitações jurídicas.

O tratamento e a troca de informação está patente, hoje mais do que nunca, a todo o momento, quer seja nos processos de automatismos, quer seja pelo caráter evolutivo da nanotecnologia, o que levou ao aparecimento da 4ª revolução industrial, assim sendo, trará, como será por demais evidente, o conteúdo teórico, em matéria das novas tecnologias, pelo seu caráter evolutivo,

5 Iden.

6 *"É uma tarefa que na sua inescapável multiplicidade de aderências toca com as categorias da necessidade e do merecimento da pena e até com todo o processo de legitimação inerente à atividade incriminatória. É tarefa que tem que necessáriamente que se desdobrar, que se desimplificar, na compreensão racional de muitas maquinarias político-sociais, nem sempre de fácil inteligibilidade para olhos sociologicamente menos perscrutadores."* Este aspeto é posto em evidência a partir do capitulo O direito penal, a informática e a reserva da vida privada do Professor José Francisco de Faria Costa no seu livro *Direito Penal da Comunicação: Alguns escritos*, p.63, onde apela a uma realidade do interprete, não só em matérias jurídico-penais, mas também em matérias jurídico-constitucionais, onde o valor de um bem pode e deve envolver-se e recortar-se no ordenamento jurídico, sem nunca esquecer o seu simbolismo protetor.

pela dimensão internacional e pela nova originalidade, o que por sua vez levará a constantes abordagens do Direito das Tecnologias da Informação.

Segundo Bismuth[7] os grandes problemas nestas matérias são:

Proteção das liberdades públicas (ficheiros de informação normativa)

Propriedade da informação (proteção de software e proteção de dados)

Contratos eletrónicos (comércio)

Direito do trabalho (conhecimento)

Informatização da administração pública (justiça vs direitos dos cidadãos)

Um dos problemas primários associados ao *Intelligence*, e relativos às Tecnologias da Informação, é a instalação física dos bastidores de rede, que têm de estar instalados num qualquer território. Território este que pode não ter governo próprio, ou até ser território fideicomisso, neste último tipo de território, por norma, é atribuída a competência da sua gestão aos habitantes locais, assim sendo, a jurisprudência imposta pela territorialidade física colide a grande velocidade com a jurisprudência da territorialidade digital, tendo que contar também com todas as lacunas e contradições que possam advir entre estes diferentes territórios, que na realidade objetiva são um só.

As informações constantes, armazenadas e transmitidas, através dos bastidores em rede, vão sendo submetidas a uma quantidade indeterminada de fatores externos.

Portanto, cabe aos académicos estudar, não só o Direito e Informática, os gigantes da informática e da internet, mas, sobretudo, dissecar as informações enquanto bem jurídico autónomo, pela *"...falta de enquadramento jurídico da sua atividade e à sua sede perante de novos meios..."*[8], pela capacidade digital de extração de dados, que levarão as Tecnologias da Informação à interceção e controlo de todas as atividades hostis, em todo mundo e por todo o mundo, que sejam efetuadas através das Tecnologias da Informação.

OBJETIVOS

Os objetivos principais desta tese de mestrado são, fundamentalmente, legitimar pela afirmação jurídica a recolha de conhecimento total ou parcial de notícias com interesse jurídico, criminal e forense e que sejam oriundas de fontes abertas, ou cobertas, e que se localizem, numa qualquer máquina, que opere informação representada sob a forma de dígitos associados a impulsos elétricos.

7 *Direito da informática*, p. 110.
8 Segundo Lebébrure em *O caso Snowden*, p. 166.

Neste trabalho de investigação cabe também a demarcação do *Intelligence* de forma positiva na sociedade, confinamento este que se torna urgente em virtude de toda a atmosfera de desconfiança em torno dos serviços de informações.

Um dos objetivos desta revisão surge também em virtude da constante mutação tecnológica, assim sendo, anui-se a novas tomadas de posição, relativas às directrizes de investigação e às revisões literárias.

Esta revisão assentará na elevação da informação a bem jurídico autónomo e determinará também o enquadramento dos segmentos da informação como parte integrante dos direitos, liberdades e garantias, a salvaguardar numa futura revisão constitucional.

IMPORTÂNCIA

Hoje, as organizações em particular e a sociedade em geral albergam máquinas das Tecnologias da Informação e aplicam o seu uso de forma intensiva levando, não só mas também, a uma mudança da conceção estratégica, nos tipos e formas de ilicitude contrários às normas da justiça. Também, todos os assuntos que tenham como intuito produzir matéria de difusão maioritariamente restrita (classificada) e de relevo forense deveriam ser expurgados, com prudência adequada, e levados a cabo, só, e por si só, por parte dos órgãos de controlo social, onde se incluem todos os serviços que cuidem das informações, serviços estes que ainda se encontram muito restringidos no seu espectro operacional, quer pela Constituição, quer pelas leis. A título de exemplo, refiro a proibição de escutas telefónicas por parte desses serviços a indivíduos específicos e previamente identificados, mesmo que conjeturem comportamentos antissociais de elevado risco para a sociedade.

O uso intensivo de Tecnologias da Informação levará estas tecnologias a uma posição predominante em todos os setores de atividade, sejam eles no setor primário (atividade extrativa da natureza), no secundário (transformação), ou no setor terciário (serviços). As instituições/organizações terão de ter uma renovação na conceção e na gestão de novos produtos, assimilando que, por trás dos maiores recursos económicos, estará sempre, como fundamental fonte de energia e de progresso, a informação de forma autónoma, bem como, os seus fluxos.

A tecnocracia [9] (recolha, comparação, comando, associação, exclusão, interação, armazenagem, e difusão) através da globalização da informática, das Tecnologias da Informação, das telecomunicações e, sobretudo, pela velocidade da informação em psicossegundos, levou o direito ao seu apogeu.

9 Martins refere-se à tecnocracia como o reflexo do humano e do social ditado pela cultura, pelo tempo, e pela geografia.

O princípio da liberdade de expressão, o princípio da liberdade de informação, associados aos princípios do direito penal, ou do ilícito da mera ordenação social, ruflam em tudo com os Artigos 37.º, e 38º da Constituição da República Portuguesa[10], pois, o Estado assegura a todos eles a sua salvaguarda e independência, prolongando-a ainda mais quando se trata de liberdades de expressão, informação e imprensa.

A jurisprudência do direito das Tecnologias da Informação tem vindo a evoluir na União Europeia, pelo que o Conselho da Europa, ainda assim, anda um pouco a reboque da jurisprudência das sociedades mais evoluídas tecnologicamente, o que, para além das dicotomias culturais, éticas, resultará muitas vezes numa abordagem oposta, e prejudicial, em diversas matérias, em virtude de muitas dessas sociedades serem mais chegadas ao sistema jurídico anglo-saxónico. Não obstante tudo isto, existirá sempre uma imposição obrigatória de consensos, em virtude da cooperação internacional, no encalço utópico da Era da Globalização.

METODOLOGIA

O *Intelligence* e a informação são matérias indissociáveis da *"Sociedade de Informação"* afluindo na livre circulação de bens e serviços, logo, a informação enquanto bem jurídico usufrui dos processos e serviços alicerçados nos fluxos de informação. Assim sendo, podemos defender que a informação não é devidamente acautelada, pois a internet, por si só, não garante a sua segurança passando os Estados a terem de ultimar meios de *"...proteção, detenção e reação."*[11].

A constante interação informacional entre partes levará os vários Estados a políticas uníssonas e esclarecedoras relativamente aos deveres e obrigações a que cada Estado ficará vinculado, quer nas ações diretas quer nas ações indiretas, com o intuito máximo de garantir a diminuição do risco e o desenvolvimento do mundo virtual.

A emergente *"Era da Informação"* trouxe consigo elevados perigos que, por vezes, colocam em risco a segurança do Estado bem como os seus interesses nacionais. Torna-se então necessária e justificada uma supervisão efetiva sobre as Tecnologias da Informação, sem deixar de ter em conta tudo o que isso implica.

10 Estas liberdades defendem a expressão do pensamento sem censura, à exceção daquelas que tiverem relevo no direito criminal.
11 In I Congresso Nacional de Segurança e Defesa, p. 516.

A UE, a OTAN, a ONU e a OCDE têm áreas comuns de cooperação estratégica internacional no ciberespaço.

As linhas de desenvolvimento, entre outros são: a cibersegurança, onde se inclui o e-governance; o combate ao terrorismo, onde se inclui o combate ao cibercrime e a privacidade; a proteção de infraestruturas críticas, com prioridade as infraestruturas da energia e da informação; segurança e defesa; e a partilha e troca de informação em foro especializado.[12]

Os riscos são inerentes a todos os setores de atividade, mas há poucos setores de atividade que estejam tão dependentes das informações como as repartições que cuidam de assuntos do âmbito jurídico, criminal e forense.

As recorrentes inovações das redes móveis e fixas têm de proteger a segurança interna, mas também a privacidade dos fluxos de informação, e os Estados têm de garantir o seu funcionamento de forma válida, quer seja nas trocas de informações de interesse pessoal ou coletivo.

A derivação das conexões das redes e a sua complexidade deixa por via das redes de informação uma panóplia de ações na mão de cada utilizador, podendo daí advir comportamentos pró ou antissociais. Neste último caso é que se encontra o grande cerne dos fundamentos do *Intelligence*, pois todos os setores de atividade, sejam eles o Primário (agricultura, pesca, etc.), o Secundário (indústria, etc..) ou o Terciário (comércio, serviços, etc.) têm fortes relações com a informação, enquanto bem jurídico, bem como com os seus fluxos.

A sabotagem de redes de informação ou a simples tentativa poderá incapacitar o próprio Estado nas suas formas sociais mais elementares, tais como o fornecimento de água, luz e gás. Impõe-se não só um Programa Nacional e Europeu para conservar a devida proteção das infraestruturas críticas, mas também a implementação de formas de prevenção, entre outras, à sabotagem informática.

Cenário pior do que encurtar alguns Direitos Fundamentais será se algum dia deixarmos de supervisionar comportamentos de índole criminosa através das redes informacionais. Apresenta-se, a título de exemplo, um atentado a uma Central de Produtos Tóxicos ou Nucleares.

12 Tabela 1 – Áreas de Cooperação Internacional Comuns, Estratégia da Informação e Segurança no Ciberespaço, p. 74.

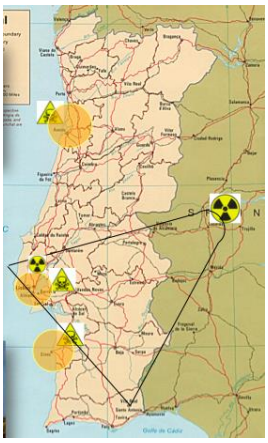

Figura 1 - Mapa (parcial) da Península Ibérica.

> "Os Planos Estratégicos Sectoriais (PES): constituem os instrumentos de estudo e planeamento que abrangem todo o território nacional e que permitirão conhecer, em cada um dos sectores abrangidos, quais são os serviços essenciais prestados à sociedade, o seu desempenho global, as vulnerabilidade do sistema, as potenciais consequências da sua indisponibilidade e as medidas estratégicas necessárias para a manutenção da sua atividade."[13]

LIMITAÇÕES

Esta tese de mestrado foi progredindo com dificuldade a partir da escassa bibliografia sobre as matérias do Intelligence, mas também pela abordagem jurídica, sobretudo a que consta na constituição, nos tratados internacionais, nas leis, nos decretos de lei e em algumas portarias.

Após revelada a pertinência desta revisão literária, prosseguiu-se à reformulação das conceções e das perceções sobre a área do *Intelligence*.

Apesar das constantes discussões em matérias do *Intelligence* e do seu surgimento diário em todos os media, em todo o mundo, este assunto é abordado apenas de forma genérica e quase abstrata, o que revela, desde logo, um profundo desconhecimento por parte da generalidade das pessoas sobre estas matérias, o que deixa também transparecer que os assuntos mais específicos só estão ao alcance de alguns e que as matérias mais sensíveis (classificadas) se encontram ao alcance de muito poucos.

Forte obstáculo foi também todo o "secretismo" envolto nas matérias do *Intelligence*, mais ainda por, à data, praticamente inexistirem estudos que evidenciem, de forma explícita, as intervenções

13 In *IDN Caderno N.º 12,*, p. 19.

e as aplicações das matérias do *Intelligence*, no condicionalismo da estratégia científica e pedagógica, e da sua intermediação com a governação do Estado, no auxílio à sua política, à desconcentração de poderes, e da especialização da respetiva intervenção do *Intelligence* no auxilio à priorização de assuntos, e muito mais, à tomada de decisões do Estado.

É de salientar também a limitação de acesso a estudos realizados internacionalmente, pois todos eles abordam a matéria do *Intelligence* de forma muito generalista e os poucos que existem encontram-se descontextualizados à realidade portuguesa.

ESTRUTURA DA DISSERTAÇÃO

A presente tese de mestrado encontra-se dividida em seis (6) capítulos. Antes dos constitui o enquadramento teórico da tese, tendo como suporte a bibliografia analisada, e dedica-se ainda à caracterização geral, apresentando o problema, o objetivo, e as limitações da revisão. No início da tese, será também apresentada a estrutura da dissertação e um breve enquadramento da metodologia escolhida para o presente trabalho.

No capítulo 1 proceder-se-á a uma introdução ao *Intelligence*, e aborda-se a teoria do direito penal do inimigo, a par dos fundamentos, problemática, abordagem e análise do *Intelligence*, fazendo referência aos comités de informação.

A prossecução do objetivo da tese começa a aprofundar-se a partir do capítulo 2, capítulo este que recorre à enumeração dos intervenientes do *Intelligence*. É também exposta a relevância jurídica, criminal e forense, passando por uma análise ao comportamento das organizações que desempenham as suas funções e tarefas através das Tecnologias da Informação, nomeadamente aquelas que as desempenham sobre o sistema integrado de informações. No capítulo 3 será retratada a sustentabilidade da gestão das estratégias operacionais, tais como: a segurança, a classificação, os métodos e as fontes, levadas a cabo na prática diária do *Intelligence*. Ainda no final do capítulo 3 será efetuada uma análise real a um conjunto de entrevistas anónimas efetuadas a analistas/técnicos de informações.

A parte relativa à informática propriamente dita tem o seu expoente máximo no capítulo 4, com a enumeração dos programas, modelos e sistemas utilizados no exercício do *Intelligence*, bem como a descrição de algumas atividades cibernéticas.

As arguições sobre as escutas judiciárias e administrativas aparecem no capítulo 5, criticando também os meios de obtenção de prova das escutas telefónicas.

Esta tese não poderia ficar concluída sem antes se consagrar a uma reflexão crítica, o que, subsequentemente, conduzirá a uma proposta de revisão do *Intelligence*.

CAPÍTULO 1. *INTELLIGENCE*: A VALORAÇÃO JURÍDICA E A LICITUDE

SUBCAPÍTULO 1. *INTELLIGENCE*: FUNDAMENTOS, PROBLEMÁTICA, ABORDAGEM E ANÁLISE

FUNDAMENTOS

Hoje mais do que nunca vive-se numa dependência extrema de informações, por esse facto é que muitos dirigentes, coordenadores, técnicos, etc.. têm vindo a proceder a restruturações à reconfiguração e ao formato das informações. Um dos fundamentos do *Intelligence* é que a iniciativa tem de estar do lado dos Órgãos de Controlo Social, e não do lado dos delinquentes antissociais.

O *Intelligence* basicamente tem os seus fundamentos na recolha e processamento de informação, que visa gerar uma valoração ao conhecimento total ou parcial de assunto de interesse relevante oriundo de fontes abertas ou cobertas com o intuito de produzir matéria de difusão maioritariamente restrita para auxiliar da melhor forma e cimentar, assim, uma decisão consciente e necessária à proficiência de um qualquer setor de atividade (primário, secundário, terciário) ou segmentos (militares e de segurança, políticos e sociais, económicos e empresariais e científicos e tecnológicos)[14]. Através de meios técnicos e operacionais, assim o Intelligence revela-se em dois planos: o militar e/ou civil.

O *Intelligence* justifica-se não só pela direção, obtenção, proteção e análise de informações, mas também na produção de informações necessárias à salvaguarda da independência nacional e à garantia da segurança interna.[15]

O *Intelligence* coabita de forma estreita, com o Contra-*intelligence*, este último que visa invalidar, danificar e interferir na estratégia, em toda a produção de informação por parte do outro ator, minorando o seu poder de antecipação.

Todas as atividades de informações impõem-nos as temáticas da segurança e guiam-nos não só ao seu direito, mas também ao *"...Direito da guerra e um Direito na guerra..."*[16].

Assim a recolha/difusão do *Intelligence* organiza-se, supostamente, dentro da legalidade legislativa, já não poderemos dizer o mesmo do contra-*intelligence*, pois este, pelo seu conceito, só se fará fora dos quadros legais.

14 É desta forma sistematizada que Ernâni Rodrigues Lopes descreve segundo ele os segmentos das informações no seu contributo em honra do Sr. General Pedro Cardoso in *Informações e Segurança* - Informação, Informações e Estratégia Económica e Empresarial, p. 219 e ss.
15 Artigo 2° da Lei n. 30/84 de 5 de setembro da Lei-Quadro do Sistema de Informações da República Portuguesa.
16 Jesus, A, in *Informações e Segurança*, p. 85.

Sabemos que as regras do processo de informações obscuram a sua fiscalização, bem como a sua troca, deixando assim a pairar um vislumbramento de uma confluência sincera de valores éticos, entre os Estados-Membros, com limpidez de conteúdos, e sem reservas, na confiança da troca de informação classificada.

Assim, por todos estes fundamentos, e também pela exigência constitucional do Artigo 27.º, n.º1 Direito à Liberdade e à Segurança[17], aplicar-se-á o *Intelligence* pela injunção jurídica de salvaguardar bens jurídicos superiores originando uma justificação supralegal.

PROBLEMÁTICAS

Uma das problemáticas do uso do *Intelligence* (Digital) começa logo na Constituição da República Portuguesa, entre outros, nos artigos 34.º, n.º 4 e 32.º, n.º 4[18], circunscrevendo as interceções de comunicações a casos graves decorrentes de processo crime e sempre com a intervenção de um juiz.

Tornam-se assim complexas as relações antinómicas[19] levadas a cabo pela Constituição, bem como o princípio da territorialidade[20], como é possível verificar pela imagem abaixo, ou há uma imposição do direito internacional ou haverá contactos diversos relativos às diferentes ordens jurídicas. Assim, o *Intelligence* estará sempre como que um sentinela alerta, na salvaguarda da preservação da segurança interna e externa, bem como da independência e dos interesses nacionais e unidade e integridade do Estado.

17 Constituição da República Portuguesa
18 Iden
19 O Professor Rui Pereira descreve o êxtase dessa antinomia nos Estados Democráticos invadidos pelo terrorismo paradoxalmente às restrições versus liberdades, em Informação e Segurança, Os Desafios do Terrorismo: A Resposta Penal e o Sistema de Informações, p. 512.
20 Os delitos fazem-se muitas vezes por meio da internet. A título de exemplo a rede TOR que facilita em muito os delitos itinerantes ou de trânsito (ver 4.1.2)

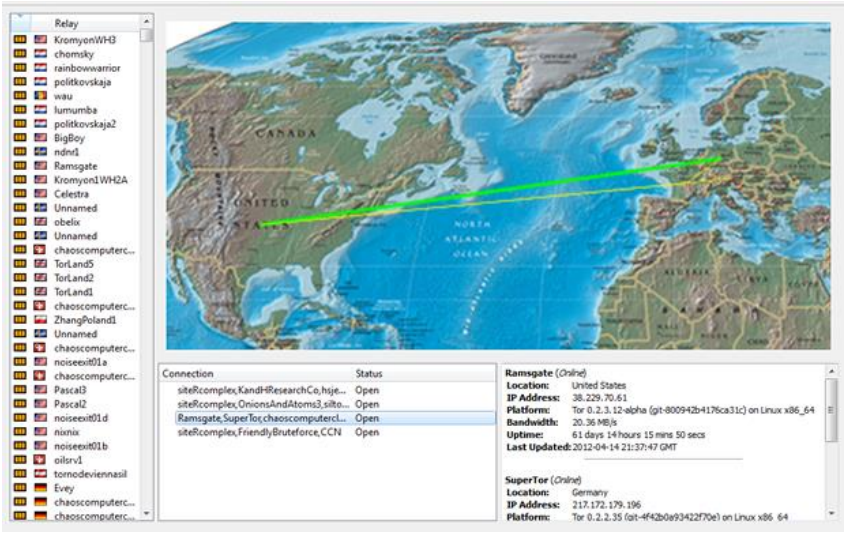

Figura 2 Mapa de uma rede Tor onde se verifica do lado esquerdo os vários países e os relays disponíveis. [21]

Neste caso onde está o princípio da territorialidade, ou da nacionalidade? Como funcionará a compatibilização dos mesmos com outros ordenamentos jurídicos? Funcionarão bem os princípios da convivência internacional especialmente quando um ou mais Estados entrarem em conflito?

A problemática por mais estranho que pareça encontra-se plasmada também na Lei-Quadro do Sistema de Informação da República Portuguesa - Lei n.º 30/84 de 05 de setembro que, ao invés de abrir ao *Intelligence* alguma liberdade de atuação, consagra, de forma condenável, as limitações das atividades dos serviços de informações pelo seu n.º1 do artigo 3.º, descrevendo a proibição de *"...pesquisa, processamento e difusão de informações que envolvam ameaça ou ofensa aos direitos, liberdades e garantias consignados na Constituição e na lei."*, mas como é que se pode trabalhar o Intelligence sem ferir os DLG dos cidadãos? Pior ainda ocorre no mesmo artigo, mas agora no n.º 2, pois refere *"...todas as restrições..."* dos serviços de informação em tudo o que ofenda os DLG por meio da informática. Outro dos obstáculos surge pelo facto de os serviços só poderem desenvolver as atividades de pesquisa e tratamento das informações respeitantes às suas atribuições específicas. Ora se os segmentos de informação tratam de matérias militares, de segurança, políticas, sociais, económicas, empresariais, científicas, tecnológicas, o que realmente fica de fora destas atribuições?

Se englobarmos a tudo o já referido a obrigatoriedade de comunicar mutuamente os dados e informações que, não interessando apenas à prossecução das suas atribuições específicas, possam ter

21 Relays e Sevidores da Rede Tor in, http://windows.appstorm.net/how-to/how-to-browse-the-web-anonymously-with-tor-project/

interesse para a consecução das finalidades do SIRP, então, numa primeira fase, tudo interessará ao SIRP e a posteriori se descartará ou não as matérias de relevo.[22]

A par disso, autores como Rapoport, Jenkin, Laqueur e Schelling argumentam que *"... o terrorismo não obtém sucesso, (...) era incapaz de obter sucessos políticos de algum relevo ..."*. Também Cordes corrobora o insucesso do terrorismo *"Num estudo elaborado por investigadores na RAND Corporation afirmava-se mesmo que o terrorismo era fundamentalmente um fracasso ..."*[23]. Despreza-se a natureza ética, organizacional e substantiva do uso do Intelligence, defendendo que não fará falta derivado ao segredo da sua fundamentação, ou ao desequilíbrio que lhe advém entre os direitos dos cidadãos.

> *"The consequences of mass surveillance tools such as those developed by the United States and allied services falling into the hands of authoritarian regimes would be catastrophic. In times of crisis, it is not impossible for executive power to fall into the hands of extremist politicians, even in established democracies. High-technology surveillance tools are already in use in a number of authoritarian regimes and are used to track down opponents and to suppress freedom of information and expression. In this regard, the Assembly is deeply concerned about recent legislative changes in the Russian Federation which offer opportunities for enhanced mass surveillance through social networks and Internet services."*[24]

Os Serviços de Informações estão sempre sob forte tensão por parte das instituições supranacionais, bem como por parte dos media, levando assim a uma elaboração da sua natureza específica, o que condiciona o seu espectro de atuação com a atribuição de objetivos e missões concretas, exteriorizando a pureza política do Estado ou dos Estados-Membros, levada a cabo pela Segurança Nacional.

"...os serviços são facilmente postos em causa quando não conseguem prevenir situações de catástrofe, mesmo quando a responsabilidade primária desse facto não lhes possa objetivamente ser atribuída."[25]

---

22 Lei n.º 30/84, de 05/09 com as sucessivas, mas não conclusivas alterações.
23 João Pereira citou estes autores em Terrorismo Transnacional, in *Ameaças e Riscos Transnacionais*. Perspetivas Institucionais, P.60.
24 *Resolution 2045 (2015) Mass Surveillance*, Dot 8. Parliamentary Assembly – Council of Europe.
25 O Dr. António Bispo, refere-se não só aos condicionalismos da comunidade das informações, mas também, às fortes pressões a que estão constantemente sujeitos os Serviços de Informações.

ABORDAGEM

A abordagem do *Intelligence* em Portugal segue no trilho, principalmente, dos segmentos das informações, (militares e de segurança; políticas e sociais; económicas e empresariais; científicas e tecnológicas), preservando-os em centros de dados *"...em suporte magnético..."*[26], quer nas instalações do SIS, nas informações destinadas à garantia da segurança interna, nas matérias de sabotagem, terrorismo e de espionagem, e nas instalações do SIED, nas matérias de salvaguarda da independência nacional e dos interesses nacionais e de segurança externa. Quanto às Forças Armadas, estas levam a cabo, de forma autónoma, as suas missões específicas da segurança militar.

Ao SIS e ao SIED são restringidas as atividades que ameaçam os DLG, consignados na CRP, e aplica-se a restrição de praticar atos da competência específica dos tribunais, do ministério público e das entidades policiais.

O dever de colaboração entre instituições ligadas às informações fica assegurando na Lei Orgânica do Sistema de Informações da República Portuguesa, mais propriamente, com as Forças Armadas, com as forças e serviços de segurança, e com as congéneres estrangeiras.

ANÁLISE

O ciclo de produção de informações, entre outros, é composto pela análise, esta apresenta-se como o método de aquisição de conhecimento e passa por um processo de decomposição que pode ser levado a cabo por duas formas: a passiva e a ativa.

A análise na forma passiva traduz-se no processamento de dados, enquanto que, na forma ativa, é revelada através da produção de relatórios.

Michael Herman, do Colégio de Stº António Oxford, distingue a informação do *Intelligence* da seguinte forma: *Intelligence* é o resultado produzido pelo processamento da informação, enquanto que a Informação, resumidamente, é a notícia não processada.[27]

1.1.1 ESTRUTURA E OBJETIVOS DO INTELLIGENCE

O *Intelligence* é definido, entre várias definições encontradas, como o ciclo de produção de informações e é composto pela análise. Esta realiza-se por apropriação e subsequente difusão dessa mesma informação.

26 Alinea e) do n.º 1 do Art. 2.º da Lei n.º 9/2007 de 19 de fevereiro – Lei Orgânica do Sistema de Informações da República Portuguesa.
27 O trabalho da análise, in Informações e Segurança, p. 434.

A fase precursora do *Intelligence* versava as Informações Militares no cumprimento do *peace building*, com todos os problemas que estavam associados ao seu exercício e às suas atividades, que visavam sobretudo a obtenção de conhecimentos sobre o inimigo e sobre a área de operações. Com o decorrer do tempo, o *Intelligence* passou a ser dividido em informações abertas e cobertas, passando a ser consideradas algumas matérias como classificadas e de difusão restrita. Mais tarde, ainda no âmbito militar, as informações passaram a ser menos expostas, em virtude das cooperações técnico-militares e internacionais e pelo descrédito e desconfiança que os Estados erigiam de uns para com os outros.

Ainda assim, o *Intelligence* é primordial no conhecimento que transmite sobre as fações beligerantes.

A Análise das Informações Estratégicas deve ter três vertentes. A primeira é a política, que deriva em duas componentes: a defensiva – que enquadra a produção de informações e que tem como intuito a prevenção (contrainformação) de ameaças ao Estado e a identificação de vulnerabilidades – e a ofensiva, que visa produzir estratégias de interesses conjunturais, nos quadros geoeconómico, geopolíticos e geoculturais. A segunda vertente é a defesa, e esta visa, sobretudo, avaliar o potencial estratégico de defesa de determinada organização ou país. Por último, apresenta-se a vertente da segurança que, através de estudos, avalia o risco e a prevenção de ameaças com origem externa.[28]

1.1.2 O INTELLIGENCE COMO VALOR JURÍDICO

O dissecar da descrição dos conteúdos levará naturalmente a uma interpretação jurídica da funcionalidade prática do *Intelligence*, bem como à ponderação da necessidade da sua sujeição por parte da sociedade. Os conteúdos incluirão de forma mais veemente os Órgãos de Controlo Social. A par disso, empenhar-nos-emos nos conteúdos normativos, abordando a sua forma de interpretação e a sua metodologia jurídica, descrevendo e definindo os seus conceitos, a sua comparação histórico-natural, numa ideologia do movimento do Direito.

Dissecar o *Intelligence* através da ciência do direito impõe de forma subjacente uma reflexão de valores, contrapondo a materialização do direito, na sua *"...criação, interpretação, aplicação e integração das lacunas."*[29]

A injunção de objetividade que determina a causa acarretará critérios interpretativos ao leitor, mais ainda, quando se otimizar uma resolução através do Direito Internacional pela via *jus cogens*.

28 O Professor Heitor Romana em O Novo Fremework do Terrorismo Internacional de Matriz Islâmica: Desafios ao Modelo de Análise em Informações Estratégicas in *Informações e Segurança*, p. 257.
29 A objetividade do direito segundo o Professor Sousa Lara em *Ciência Política O estudo da Ordem e da Subversão*, p. 99.

Semelhante resolução aparecerá conjuntamente revelada por uma interpretação doutrinal e jurisprudencial, o que traduzirá a realidade jurídica e a justaposição prática do *Intelligence*.

1.1.3 O DIREITO PENAL DO INIMIGO NO INTELLIGENCE

O direito penal converge com a Intel quando se tocam conflitos jurídicos por ofensa a bens jurídicos substanciais para a atividade normal da humanidade, mais propriamente em todos os conflitos que surgem pela via dos fluxos informacionais ou da informática.

Assim teremos de esgrimir genericamente a função (essencial) do Intel, confrontando-a com a valoração do bem jurídico danificado.

A comunicação à distância é frequentemente utilizada na nossa sociedade atual, ainda assim, a forma de orquestração das tecnologias digitais não aclama uma nova forma de comunicação diversa da fala e da escrita, mas apela a uma transmutação por subsunção na virtual.

A ideia de instrumentalização do Intel aparece quando utilizamos, por exemplo, o telemóvel ou o correio eletrónico, como uma forma de comunicação fechada, assim, Faria Costa sustenta uma tutela jurídico-penal, nas áreas das telecomunicações digitais, quer *"... a autodeterminação pessoal refratada em autodeterminação informacional, quer a privacidade, quer a intimidade."*[30], o referido autor afirma ainda que os meios de comunicação social ou telecomunicação social são *"... meros veículos tecnológicos..."*[31].

O Direito penal do inimigo distingue-se de outras teorias do direito penal, pois parte da teoria da defesa das políticas de combate à criminalidade, defendendo, ao nível processual, um processo penal para os indivíduos pró-socias, e outro processo penal para os indivíduos antissociais. Esta tese – defendida por Gunther Jakobs – embora verse o processo penal, poderia por analogia ser aplicada também ao Intelligence, muito por razão da sua ideia primária de defender os riscos futuros, o que mais não é do que o objetivo do Intelligence.

Esta tese tem como intento a destrinça fiel e positiva de dois vetores: o Direito Penal do Cidadão e o Direito Penal do Inimigo, afirmando-os através de um contexto jurídico-penal, revelando o autor de um delito como pessoa, ou como fonte de perigo, respetivamente. Para que se possa invocar o direito penal do inimigo, terá de existir sempre um comportamento desviante e perigoso para a sociedade.

30 Faria Costa em o *Direito Penal da Comunicação*, 1998, p. 154.
31 Idem

Esta tese recorda o facto passado na hora de submeter um juízo ao presente, com uma medida de segurança, salvaguardando, assim, a segurança do futuro.

Esta tese gerou numerosos censuradores, e acérrimos defensores!..

Rosseau afirma que *"...qualquer «malfeitor» que ataque o «direito social» deixa de ser «membro» do Estado..."*.

Fichte declara que *"... quem abandona o contrato cidadão (...) perde todos os direitos como cidadão e ser humano (...) morte civil..."*.

Hobbes proclama *"...a submissão por meio da violência (regras inconstitucionais) (...) deve ser entendida como metáfora de que (futuros) cidadãos não perturbem o Estado em seu processo de auto-organização (...) quando se trate de uma rebelião (...) são castigados como (...) inimigos..."*.

Kant assevera obrigação *"...a qualquer outra pessoa a entrar em uma constituição cidadã (...) pode ser tratado <<como um inimigo>>..."*.[32]

O Direito (penal) do cidadão (indivíduo pró-social) adjudica o simples criminoso como aquele que não é um delinquente por tendência. Ao contrário do Direito (penal) do inimigo que se atribui ao malfeitor que se desvinculou do contrato social, que coloca em perigo a sociedade e que é incapaz de garantir aos outros o seu direito de segurança.

Qualquer Estado moderno e democrático, que se encontre no tempo da *"Era da informação"*, deverá vincular regras de Direito não só ao delinquente, que por tendência é perigoso, mas também à sociedade, como instrumento de segurança, com medidas necessárias, adequadas e proporcionais.

Em resumo, o Direito penal do cidadão é o Direito de todos, o Direito penal do inimigo é para os inimigos da sociedade.

Logo, se alguns autores, perante a definição de indivíduos perigosos, clamam a definição de guerra, à vanguarda da segurança, deve-se então articular este Direito penal do inimigo com o *Intelligence*, com a criação de leis direcionadas aos delinquentes *"perigosos dissimulados"*, ou, por exemplo, ausentando as escutas telefónicas da autorização da autoridade judicial, entre outras medidas.

32 in *Direito Penal do Inimigo* - Noções e Críticas, p. 25, ss.

1.1.4 OS ESTADOS E O USO DO INTELLIGENCE

A sociedade em rede e as Tecnologias da Informação comportam, logo à partida, um pensamento estratégico sobre os segmentos da informação, colocando aos Estados novas inquietações e obrigando-os assim *"...ao levantamento de novas capacidades, à revisão dos seus modelos de governação e à geração de competências, cada vez mais associadas à exploração das Tecnologias de Informação e Comunicação – (TIC), ao acesso à internet e à utilização do ciberespaço"*[33].

Os Estados ficam assim obrigados a coordenar todas as sinergias, assentando edificações, sobretudo em estratégias políticas.

A política a implementar para alcançar uma certa finalidade é confinada pela atitude a adotar e pela ação a desenvolver. Assim ter-se-á de ter em conta a estratégia geral e a estratégia operacional. Traduzindo a estratégia geral na finalidade política e a estratégia operacional na forma concreta como esta se desenrola.

O *Intelligence* enquadra-se na estratégia operacional.

O *Intelligence* está a dominar o novo alinhamento mundial, quer seja através das cooperações internacionais, ou como uma das respostas aos novos ataques e ameaças prováveis aos segmentos da informação.

Debater os pressupostos de toda a envolvência do *Intelligence* e a sua forma de reconfiguração profunda desencadeará um novo movimento no fluxo de informações, de certa forma vanguardista e preponderante na reintegração da Europa como um só e do mundo como um todo. Aproximando, desta forma, os serviços de informação dos Estados e prolongando a afinação de credenciais e formas de troca de informação, criando uma estabilidade que acabará de certo modo com os conflitos circunstanciais, de forma a poder globalizar e maximizar a expressão *Intelligence*.

Quanto à forma concreta como o *Intelligence* se desenvolve, esta figura-se por duas vias: por ação ofensiva e direta através da intrusão nas Tecnologias da Informação tendo em conta a limitação do tempo, a confrontação e a intensidade; por ação defensiva e indireta através da análise de notícia recebida, por fontes abertas ou por organizações aliadas, com um tempo indeterminado e perda da iniciativa

É com esta panóplia de interações que se esclarece a forma paradoxal sob a qual muitas vezes se manifestam as particularidades da ação estratégica que é o *Intelligence*. Esta interação coerente dos diferentes componentes, que pressupõe a interdependência e a interatividade, verifica-se como

33 O Sr. TCor Doutor Viegas Nunes referindo-se ao desenvolvimento de todo um conjunto de garantias e iniciativas para uma utilização da internet.

expoente máximo na União Europeia (UE), por exemplo, que possibilita transformar o desejável em exequível.

A UE foi pensada e estruturada como meio para permitir a mobilidade e a livre circulação de pessoas e bens, contudo, quando foi arquitetado o formato da autoestrada da informação, esta ainda se encontrava numa fase praticamente embrionária, sem os mega fluxos de comunicações, o que também fez com que as novas ameaças jurídicas, criminais e forenses se consubstanciassem através de organizações internacionais, e muito por influência da internet, globalizando, assim, também a criminalidade, bem como as suas novas formas de manifestação.

As novas vulnerabilidades da sociedade aberta incrementam movimentos contrários aos fundamentos pró-sociais, assim concerne aos Estados um esforço para uma melhor finura nas relações inter Estados, assumindo-se, desde logo, o Programa *Frontex* como um dos grandes princípios estratégicos na defesa de interesses comuns, prevenindo e combatendo a criminalidade. Mas no Programa *Frontex* onde é que pára a dimensão internet? Os Estados não se podem deixar ludibriar pela dimensão física da pessoa individual, pois a internet possui formas de mascaramento.

Assim, Portugal deverá desenvolver uma cooperação estratégica de magnitude, dimensão e alcance de operacionalização e constante revisão de *"...geometria variável (...) bi-multilaterais".*[34]

Ainda segundo Luís Bernardino, o Estado deverá operar a segurança em estratégias inovadoras, atendendo a fatores, tais como, o espaço e a oportunidade, a possibilidade de intervenção, o reforço das capacidades, a inserção em espaços pouco explorados. Este autor descreve a estratégia da seguinte forma:

"... uma Estratégia de Segurança Nacional deve abranger os espaços donde podem derivar as nossas principais ameaças e, se tivermos uma participação ativa nessas regiões, melhor compreenderemos o nível de risco que pode daí derivar..."[35]

Desta forma, pode o Estado Português ordenar os seus interesses, de forma duradoura e estável.

Um fator verdadeiramente essencial na Era da Informação é a Geolocalização das infraestruturas de informação que, em grande parte devido à globalização, estão situadas em locais que podem muito bem ser fora do Estado mãe, ou de países extracomunitários à UE, alterando assim

34 Luís Bernardino defende que Portugal terá que se alicerçar às alianças e que terá também que fazer constante adaptações de variáveis inconstantes ao que os técnicos apelidam de "geometria variável", in *I Congresso Nacional de Segurança e Defesa*, p. 180.
35 Iden

a natureza e as formas de combate à ameaça da informação, pois, os sistemas integrados em rede estão em espaços virtuais, designados por Ciberespaço.

Assim sendo, todos os processos estratégicos e de tomada de decisão terão de ter sempre em conta as sinergias a criar para alcançar as cooperações internacionais, para contornar a vulnerabilidade dos fatores supracitados, levando o poder circunstancial do domínio do Ciberespaço ao Estado. Estado esse que deverá implementar os aspetos físicos e matérias, inerentes ao funcionamento e curadoria do espaço virtual.

A *"Aldeia Global"* teve a sua formação assente no espaço físico multidimensional, expandido e despertado pelas novas plataformas tecnológicas de interação social, fomentando ainda mais a evolução comunitária como um todo de integração efetiva dos intervenientes nas trocas de comunicação e fluxos de informação, podendo daí resultar uma dissonância entre a sociedade real e a sociedade virtual com todos os seus riscos e implicações reais. Assim, não podemos descorar que com novas oportunidades advirão também novas ameaças.

1.1.5 COMPORTAMENTO DAS ORGANIZAÇÕES

Todas as organizações apresentam comportamentos diferenciados, sejam eles estruturais ou estratégicos, assim também os Estados. Os Estados, enquanto organizações, readaptam as suas condutas, o que decorre da necessidade e das opções da análise conceptual, contextualizando a estratégia.

Assim, compreender o comportamento das organizações é compreender os Estados e vice-versa.

Os planos de política interna/externa estão dependentes da conexão estrutural das instituições (governo) que conduzem a estratégia nacional.

Assim sendo, relativamente ao *Intelligence*, os Governos optam à partida por um dos dois tipos de atitude, ou então recorrerem a ambos, esta última situação é a que se verifica de forma mais recorrente. Recorrendo os Estados aos seus SI, ou então a serviços não institucionais, que na maior parte das situações são utilizados, quando as operações são de elevado risco, para que, caso não tenham sucesso, não coloquem em causa a imagem do Estado.[36]

A participação de grupos elitistas sempre foi tida em conta pelos Estados, bem como o seu respeito, na máxima consideração, tendo a ponderação dos seus intuitos políticos, dos pensamentos

36 O Sr. Embaixador Jubilado José de Jesus descreve de forma pormenorizada, no seu livro *Espionagem e Contraespionagem em Portugal*, a importância destes serviços não institucionais, tais como, a Aginterpress, que teve uma atividade intensa, nas ações de guerra de subversão, ações psicológicas e de propaganda nas décadas de sessenta e setenta durante as guerras do ultramar, e as suas interações de convivência com os serviços *"secretos"* do Estado, tais como a Legião Portuguesa.

ideológicos e do poder económico. Esses grupos têm cada vez maior proeminência entre a comunidade dirigente,[37] mas nem só de governantes se faz o poderio elitista, também entre outro tipo de organizações se eleva esse poder, tais como as academias universitárias, ou os sindicatos da indústria. Se por um lado uns manipulam as leis e as normas sociais, outros impõem condicionantes de comportamento aos pares (povo).

Ao Estado cabe então correlacionar as conveniências das organizações de poder entre si para melhor manipular a maioria da sociedade, que se encontra repartida, desincorporada e desagregada A manipulação incorreta por parte do Estado sobre estas organizações de poder pode levar ao declínio das elites e à transferência das suas conveniências para outros domínios.

Por princípio, os Estados que já tenham utilizado uma ou mais organizações de poder para impor a sua estratégia, por norma, logo após a restauração segura da sua estratégia, desmantelam-na, em virtude da fácil manipulação do seu grande poderio por outro tipo de fações.

Os media também têm grande influência no fator da catalisação social de comportamentos, assim sendo, cabe não só ao Estado mas também às empresas privadas dos media a responsabilidade de uma informação imunizada.[38]

A imprensa tem como únicos limites *"...os que decorrem da Constituição e da lei, de forma a salvaguardar o rigor e a objetividade da informação, a garantir os direitos ao bom nome, à reserva da intimidade da vida privada, à imagem e à palavra dos cidadãos e a defender o interesse público e a ordem democrática."* [39]

Já em 1960, com o intuito de gerar saber científico através do congregar de provas sistemáticas e controladas, com o intuito de gerar resultados lógicos, foi criado o Centro de Estudos Políticos e Sociais, no já extinto Ministério do Ultramar, com assento no Gabinete dos Negócios Políticos, este centro analisava as informações de imprensa nacional e estrangeiras.[40]

Assim, entender o comportamento das organizações é conjeturar uma arquitetura do *Intelligence*, nas mais variadas formas.

37 A originalidade da teoria das elites, advém do facto da detenção do poder ser de uma minoria, logo maior organização, in *Mosca, Pareto e Michels e la teoria delle elites*, in http://people.unica.it/lucianomarrocu/files/2015/03/Storia-culturale-Modulo-2-Mosca-Pareto-Michels-e-la-teoria-delle-%C3%A9lites.pdf
38 Entre outros o Grupo Impresa está consciente da sua responsabilidade social assumindo, o desenvolvimento da comunicação social, e do impacto que tem sobre a sociedade, promovendo, várias iniciativas, que sustentem e transmitam os valores tais como, a defesa da liberdade de expressão, e a independência da comunicação social no funcionamento da democracia, in http://www.impresa.pt/arquivo/2016-02-24-Responsabilidade-Social.
39 Lei n.º 2/99, de 13 de janeiro – Lei de Imprensa Artigo 3.º Limites
40 In *Espionagem e Contraespionagem em Portugal*, p. 47 e ss.

1.1.6 ARQUITETURA DE TECNOLOGIA DE INFORMAÇÃO

A estruturação da arquitetura das tecnologias de informação aparece muito devido ao grande desenvolvimento das sociedades em rede, que necessitam de uma estrutura própria, de forma a estruturar a prospeção de informação, a facultar uma boa pesquisa, a facilitar o processamento, e por último, a proporcionar uma boa análise dos dados recolhidos, tendo sempre em conta em qualquer das fases o objetivo principal dos SI, que têm a incumbência da divulgação das matérias classificadas a quem de direito.

A sociedade moderna e do conhecimento assenta em redes e plataformas, gerando um fluxo informacional infinito seja qual for o formato informacional.

> *"...uma sociedade em rede, em que a interação entre os homens deixa de ser influenciada por barreiras geográficas e passa a ser condicionada pela disponibilidade e pelo tempo de acesso aos recursos de informação."* [41]

Esta sociedade em rede tem como princípio básico a melhoria da qualidade de vida dos indivíduos e dos serviços de apoio à cidadania.

Os serviços de apoio passam muito pela parte informática, mais propriamente no que diz respeito ao processamento de texto, imagem, som ou vídeo, por meio digital. Há que centralizar num bom sistema de gestão, de bases de dados, de dados documentais de desenho assistido por computador, de informação geográfica, de tratamento de imagem, de desenvolvimento de ambientes virtuais, de hipertexto, de análise e descoberta do conhecimento em que se traduz uma interação organizacional e simbólica.

Os pilares de uma boa estrutura das TI passam por integrar todo o processo de informação de forma harmoniosa. A construção de um sistema de relações entre agentes é também um dos vetores mais importantes da gestão da informação, pois permite centralizar e descentralizar a unidade móvel de dados, consoante o método escolhido pelo curador da informação.

A Europa, com o intuito de estimular a sociedade em rede, desenvolve em quadriénios programas-quadro de ações em matéria de investigação, desenvolvimento tecnológico e demonstração, que incentivam a evolução de hardware e software aumentando assim o conhecimento da geração

41 Enquadramento do Ciberespaço: Conceito e Âmbito em Segurança e Defesa, in *IDN cadernos* Estratégia da Informação e Segurança no Ciberespaço, n.º12, 2013, p. 8.

tecnológica e, subsequentemente, do seu utilizador de forma a tornar acessível uma interação de uma multiplicidade de serviços e aplicações, otimizando desta forma as tecnologias de computação.

> *"(...) a investigação sobre ferramentas de gestão da informação e sobre as interfaces que permitam interações mais fáceis preconiza-se, nomeadamente:*
>
> *a) Sistemas de representação e gestão do conhecimento baseados no contexto e na semântica, incluindo sistema cognitivos, bem como ferramentas de criação, organização, navegação, recuperação, partilha, preservação e difusão de conteúdos digitais;*
>
> *b) Interfaces multissensoriais capazes de compreender e interpretar a expressão natural do homem através das palavras, dos gestos e dos diferentes sentidos, ambientes virtuais, bem como sistemas plurilinguísticos, indispensáveis à construção da sociedade do conhecimento à escala europeia."*[42]

1.1.7 DIREÇÃO DE SISTEMAS DE INFORMAÇÃO

Os sistemas de informações assentam no esboço do *Intelligence*, quer seja no âmbito situacional ou estratégico.

O processamento do *Intelligence* requer como motor de ignição a presunção de determinado objetivo de interesse, o que levará à recolha de notícias desse determinado interesse oriundas das fontes (ver em 4.6), à posteriori esse processamento assentará na conceção de um esboço temporal, conjeturando a dinâmica estratégica que possibilita a maior eficácia e eficiência da projeção do *Intelligence*.

A materialização do *Intelligence* surge com a apresentação documental dos relatórios de informações para auxiliar a tomada de decisão, por quem de direito. Alguns autores, entre eles o Professor Heitor Romana[43], afirmam que um dos problemas do ciclo de produção de informações surge na objetividade analítica. Assim sendo, cabe ao técnico de informação a transformação do caráter compreensivo e interpretativo da pesquisa efetuada, traduzindo-a no relatório final. O técnico de informação tem ainda uma tarefa acrescida: integrar a perceção operacional na racionalidade

42 Garcia Marques e Lourenço Martins descrevem assim a gestão da informação em *Direito da Informática*, p. 74.
43 Conforme descreve em O Novo Framework do Terrorismo Internacional de Matriz Islâmica: Desafios ao Modelo de Análise em Informações Estratégicas, in Informações e Segurança, p. 265.

administrativa, porque *"Na maioria dos serviços de informações externos, os departamentos de análise funcionam de uma forma não integrada com os departamentos de gestão operacional..."*[44].

Pelo que o caminho a traçar pelos Sistemas de Informação tem de resultar da comutação de várias variáveis, cuja maior influência é imposta pelas situações espácio-temporais.

> *"... a partir da entrada em vigor do tratado de Maastricht (1993) que a Política Externa e Segurança Comum - PESC passou a ser um dos três pilares da UE e o seu desenvolvimento uma componente fundamental da integração europeia, através de um leque variado de procedimentos e atos que foram sendo implementados – declarações comuns, ações comuns, posições comuns, estratégias comuns e decisões comuns."* [45]

Mais tarde no Tratado Constitucional se concertaria uma unidade de Serviço de Ação Externa da UE, com o objetivo de desenvolver ainda mais a capacidade de segurança e defesa da UE fazendo da Europa uma superpotência capaz de rivalizar com os EUA, China, Rússia, Brasil, Índia, mas o processo de informatização parou no tempo!..

A UE carece ainda de um maior enfoque coletivo e paradoxal à dimensão da integração europeia.

Em 28 de maio de 2015, a Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos em conjunto com a Casa dos Representantes da Justiça e Segurança Interna da Bélgica (responsáveis pela supervisão), com os Euro Deputados do Parlamento Europeu da Alemanha e com a Comissão dos Euro Deputados do Parlamento Europeu da Itália (responsáveis pela Segurança da República) e o Italian Parliament's Committee for the Security of the Republic promoveram uma conferência sobre A Democracia dos Serviços de Informações na União Europeia.[46]

Esta conferência aparece em grande parte devido às divulgações sobre os Programas de Vigilância levados a cabo pelos EUA, mais propriamente devido ao parágrafo 133[47], da Resolução do

---

44 Idem

45 Luís Tomé descreve ainda o chamado Hard Power que ampliará uma panóplia de ações externas relativas à dimensão de segurança e defesa, em *Estratégia: Portugal e o Futuro da Europa de Roma a Lisboa*, p. 65, ss.

46 Consultado em 10 de outubro de 2016 in, https://polcms.secure.europarl.europa.eu/cmsdata/upload/d44e4bb2-f8d7-45e5-8727-62544ea349e1/Background%20links%202015-05-28.pdf

47 *"(133) Atendendo a que os objetivos do presente regulamento, a saber, assegurar um nível equivalente de proteção das pessoas singulares e a livre circulação de dados na União, não podem ser suficientemente alcançados pelos Estados-Membros mas podem, em razão da dimensão e dos efeitos da ação, ser mais bem alcançados a nível da União, a União pode tomar medidas, em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não*

Parlamento Europeu de 12 de março de 2014, sobre os Programas de Vigilância dos EUA, a vigilância sobre membros do Estado da UE e sobre os seus cidadãos.

Tendo em conta o impacto dos programas nos Direitos Fundamentais dos membros da UE, o Parlamento Europeu instaurou uma Comissão de Inquérito sobre A Vigilância Eletrónica em Massa aos cidadãos da UE, que se converteu na Resolução (2013/2682(RSP)) de 4 de julho de 2013 tendo como intuito o esclarecimento dos seguintes factos:

- reunir todas as informações e provas das evidências sobre as fontes dos EUA e da EU;

- investigar a alegada atividade de vigilância que os EUA impuseram a alguns membros de Estado da UE e apurar as respetivas responsabilidades;

- verificar o impacto dos programas de vigilância nos direitos fundamentais dos cidadãos da UE, em particular a privacidade das comunicações, traduzindo-se em mecanismos de restrição territorial na UE à vigilância eletrónica;

- impor os mecanismos administrativo-legais;

- prevenir futuras violações e aumentar o nível de proteção dos cidadãos Europeus;

- elaborar recomendações de segurança em matéria das Tecnologias da Informação e dos Sistemas de Comunicações.

Esta conferência trouxe à UE uma acesa discussão sobre a real democracia na <<Era Digital>>, com o intuito de impor regras e normas de conduta sobre os Programas de Vigilância.

A 7 de abril de 2015, em Estrasburgo, a European Commission For Democracy Through Law apresentou o seu estudo N. 719/2013 Cdl-Ad(2015)006 Or. Engl. (Venice Commission) Update Of The 2007 Report On The Democratic Oversight Of The Security Services And Report On The Democratic Oversight Of Signals Intelligence Agencies, que apresentou as seguintes conclusões:

> *"139. A inteligência dos sinais tem um potencial muito grande para infringir a privacidade e certos outros direitos humanos. A compreensão da vigilância estratégica apenas através da lente do direito à privacidade pode não capturar completamente os seus potenciais danos. Ao contrário da situação da rendição, onde o dano é claro, imediato e individualizado, o dano que a inteligência de sinais insuficientemente regulada e controlada pode*

---

excede o necessário para alcançar esses objetivos." Consultado em 25 de setembro de 2016 in, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//PT#BKMD-6

fazer à sociedade é mais difusa e a longo prazo. A situação existente pode resultar na imposição de obrigações concorrentes ou incompatíveis às empresas (tipicamente de divulgação versus protecção de dados) e na evasão de procedimentos mais fortes de vigilância doméstica das telecomunicações. Assim, parece ser necessário um acordo sobre as normas mínimas internacionais de protecção da privacidade.

140. A inteligência dos sinais pode ser regulada de forma laxista, o que significa que um grande número de pessoas é apanhado numa rede de vigilância, ou de forma relativamente apertada, o que significa que a violação real da privacidade dos indivíduos e de outros direitos humanos é mais limitada. Para as partes da CEDH, é necessário, de qualquer forma, regular os principais elementos da inteligência de sinais de forma estatutária. O legislador nacional deve ter uma oportunidade adequada para compreender a área e estabelecer os equilíbrios necessários. Contudo, os Estados europeus não devem contentar-se em satisfazer as normas de qualidade do direito da CEDH. Somente fortes mecanismos independentes de controle e supervisão podem amenizar a preocupação pública de que a inteligência de sinais não está sendo abusada". [48]

Em suma, o *Intelligence* tem um potencial elevado em matérias de segurança, mas também efeitos devastadores de dano à privacidade, pelo que se torna muito difícil legislar o *Intelligence* pela sua diversidade multifatorial, contudo deverá ser levado a cabo um protocolo internacional sobre a proteção da privacidade. Só com a regulação e supervisão de alguns parâmetros sobre o *Intelligence* se poderá assegurar a proteção dos Direitos Humanos.

1.1.8 O PAPEL DOS COMITÉS DE INFORMAÇÃO

Os Comités de Informações têm um papel fundamental para minorar as dúvidas e clarificar a conjuntura estratégica, avaliando as reações possíveis e também a reserva de informação.

48 Firmado em 20 e 21 de março de 2015, pela Venice Commission na 102nd Plenary Session. Consultado em 10 de outubro de 2015 in, http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e

Os grande comités de Intel[49], devido ao seu evidente poder, estão quase sempre numa posição superior quando se pratica a troca de informações de matérias com um grau elevado de classificação, causando assim um abuso de propriedade, bem como o desequilíbrio do resultado final.[50]

As atuais formas do processo do *Intelligence*, por força das convenções Europeias, determinam uma afinidade aparente entre as instituições Europeias, estabelecendo uma verdadeira feira de (des)informações, o que leva a desconfianças e, subsequentemente, incrementa fortemente a contrainformação, o que por sua vez eleva o bem jurídico da Segurança Nacional (interna e externa) para patamares nunca vistos.

O verdadeiro papel dos Comités de Informações é a eficácia e a credibilização do sistema propriamente dito. Cabe assim aos comités a prestação de um serviço de interesse público, em prol da globalidade comunitária, que seja *"... credível, funcional e multiparticipado."* [51]

Em Portugal, é através da Presidência do Conselho de Ministros que se dá lugar ao Conselho Superior de Informações que tem a seu cargo a consulta e coordenação em matéria de informações dos vários ministérios tendo como competência o seguinte:

> *" a) Aconselhar e coadjuvar o Primeiro-Ministro na coordenação dos serviços de informações;*
> *b) Pronunciar-se sobre todos os assuntos que lhe forem submetidos em matéria de informações pelo Primeiro-Ministro ou, com autorização deste, por qualquer dos seus membros;*
> *c) Propor a orientação geral das atividades a desenvolver pelos serviços de informações e a orientação específica das respetivas atividades de pesquisa;*
> *d) Elaborar, rever, propor alterações e dar pareceres sobre os regulamentos de segurança nacional para a proteção das matérias classificadas."* [52]

49 Relativamente a esta matéria irá ser alvo de um capítulo 2.
50 António de Jesus Bispo descreve esta troca de informações recorrendo à analogia da lei da sobrevivência, como um dos bens mais básicos, da existência humana, em *Função de Informar*, p. 77.
51 Pedro Esteves concetualiza a democracia das informações in Informações e Segurança, p. 439.
52 Artigo 5.º do Despacho normativo n.º 22/2006 Presidência do Conselho de Ministros Gabinete do Primeiro-Ministro Nos termos do disposto no artigo 18.º da Lei Quadro do Sistema de Informações da República Portuguesa, aprovada pela Lei n. 30/84, de 5 de Setembro, na redação da Lei Orgânica n. 4/2006, de 6 de Novembro, é aprovado o anexo «Regimento do Conselho Superior de Informações», que faz parte integrante do presente despacho normativo.

SUBCAPÍTULO 2. NORMAS JURÍDICAS SUPRANACIONAIS E NACIONAIS

1.2.1 UNIÃO EUROPEIA

A Comissão Europeia, contrapõe, através de documentos, a democracia e o *Intelligence*, transmitindo os aspetos judiciais e de autorizações discutindo a estratégia do *Intel* e das suas agências.

A União Europeia, principalmente a Alemanha, tem vindo a demonstrar fortes preocupações quanto ao pessoal e às técnicas de Intel usadas, desejando implementar ainda níveis de autorização relativamente ao uso do Intel para os assuntos de procedimentos administrativos, civis, ou criminais.

A UE está especialmente atenta às consultas sobre pessoas, levadas a cabo pela NSA e CIA, nos EUA, e aos documentação de apoio.

O problema é que grande parte da coleção SIGINT dos Estados Unidos cai fora do âmbito do FISC. A vigilância dos cidadãos estrangeiros não é sujeita à regulamentação nacional sob FISA.[53] . Com a agravante da falta geral de transparência em torno do *Intel*, não havendo um conhecimento público da quantidade de dados recolhidos pelo SIGINT.

A Suécia tem um modelo que combina autorização judicial com acompanhamento especializado pelo *Tribunal de Inteligência da Defesa (Försvarsunderrättelsedomstolen ou UNDOM)* em conjunto com um organismo de controlo e monitorização, a Inspecção de Informações de Defesa, composto por dois antigos juízes seniores e seis membros leigos (principalmente ex-políticos, de vários partidos políticos). Os juízes são nomeados pelo governo após um recrutamento aberto. Os ex-políticos são nomeados pelo governo após consultas entre os partidos representados no parlamento. A UNDOM é assim um organismo híbrido.

1.2.2 ESTADOS UNIDOS DA AMÉRICA

Os EUA, para as matérias do *Intel*, têm um sistema judicial próprio, que trata do *Intel* relativo ao exterior dos EUA, e que é controlado pelo Foreign Intelligence Surveillance Court – FISC, desde 1978.

Este tribunal desempenha um papel de supervisor e tem também o poder de autorizar a vigilância estratégica[54]

53 Ordem Executiva 12333
54 nos termos da Secção 215 da FISA, o Governo deve solicitar um mandado perante um juiz dos 15 membros.

O FISC aprova tanto a "Ordem Primária", que autoriza o programa global, como as "Ordens Secundárias", esses pedidos são sujeitos a renovação a cada 90 dias e as candidaturas podem incluir uma audiência. Os juízes do FISC têm autoridade para aceitar o testemunho de elementos do governo e de funcionários familiarizados com os detalhes técnicos de uma aplicação. (Ver em NSA)

Os juízes do FISC são nomeados pelo Presidente de entre o poder judiciário federal e cumprem mandatos de sete anos.

Os metadados são armazenados em redes da NSA, com o FISC a impor restrições ordenadas sobre quando e como a base de metadados pode ser acedida.

Para a consultar os metadados é necessário um número de telefone ou outro identificador associado a uma organização terrorista estrangeira.

Antes de ocorrer a consulta, um analista da NSA de alto escalão oficial ou um funcionário especialmente autorizado deve determinar que há uma "razoável suspeita" de que o identificador (n. de telefone, IP, nome, etc.) está associado a uma organização terrorista estrangeira e que deverá ser sujeito de uma investigação do FBI.

A consulta poderá revelar dados tais como: telefones em contato direto com o identificador, e números indiretos, em 2009, o Governo implementou uma alteração ao software limitando os números indiretos a três, e em 2011, o Presidente Obama limitou os números indiretos a dois tendo também alterado a conduta aquando de uma “razoável suspeita” fazendo dela uma exceção usada só em situações de emergência e sujeita a aprovação individual.

Já para os dados em massa, o Procurador-Geral da República e o Diretor de Inteligência Nacional fazem certificações anuais que autorizam este direcionamento para adquirir informações de inteligência estrangeira, sem especificar ao FISC as informações particulares não americanas e quais as pessoas que serão alvo.

Não há nenhuma exigência de que o governo demonstre, mas o governo desenvolve procedimentos de segmentação e "minimização" que devem satisfazer certos critérios. Como parte do FISC a revisão e aprovação das certificações anuais do governo, o tribunal deve aprovar estes procedimentos e determinar que eles cumpram as normas necessárias. A segmentação e procedimentos de minimização devem ser fornecidos aos comités de inteligência do Congresso.

O FISC, assim, autoriza e estabelece anualmente condições sobre o programa da secção como um em particular, especificando os limites gerais dos dados que podem ser utilizados, os dados que

devem ser eliminados e os tipos de consultas que podem ser feitas aos dados em massa recolhidos. Isso faz não autorizar o uso de dados em casos individuais.[55]

1.2.3 PORTUGAL

Em Portugal, existe uma Lei que obriga ao intercâmbio de dados e informações de natureza criminal com os países da UE, para fins de deteção, prevenção ou investigação de uma infração. Porém estes dados são fornecidos mediante condições específicas. [56]

A nível interno, desde 2013 que está regulamentado o acesso a dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas que se mostrem estritamente necessários para a prossecução da atividade de produção de informações. Estes dados tem de estar relacionados com a *"... segurança interna, a defesa, a segurança do Estado e a prevenção da espionagem e do terrorismo ...".* [57]

A estes dados podem aceder o SIS e o SIED, pois, estão sob a alçada do Sistema de Informações da República Portuguesa, com o devido acompanhamento do Ministério Público e controlo judicial.[58]

Similarmente aos EUA, aqui também os dados de telecomunicações e Internet obtidos são processados e conservados nos próprios centros de dados dos serviços de informação (SIS e do SIED).

Os prazos para conservação destes dados é que são indeterminados, pois deixam nas mãos dos analistas o prazo do tratamento de dados, e define-se que é *"... durante o período necessário para a prossecução das finalidades da recolha (...) findo o qual devem ser apagados ...",* logo esta duração é incerta.

A Lei n.º 59/2019 ratifica as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais. Ainda que transpondo a Diretiva (UE) 2016/680, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, levanta algumas questões jurídicas pela sua possibilidade de "*pseudonimização*".

55 https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e

56 *"a) Mediante pedido de uma autoridade competente de aplicação da lei que, actuando no âmbito das competências que lhe são conferidas pelo direito interno, conduza uma investigação criminal ou uma operação de informações criminais; b) De forma espontânea, nos termos do artigo 11.º da presente lei; 2 - Os dados ou informações são igualmente* trocados com a Europol e a Eurojust, na medida em que o intercâmbio diga respeito a uma infracção ou a uma actividade criminosa que se enquadre nos seus mandatos, nos termos definidos pelos instrumentos em vigor sobre as respectivas atribuições e competências." Art. 6.º Fornecimento de dados e informações - Lei n.º 74/2009, de 12 de Agosto Intercâmbio de Dados e Informações de Natureza Criminal na União Europeia

57 Artigo 1.º da Lei 4/2017

58 Idem.

Portanto, o Indivíduo, a certo ponto, deixa de estar identificado por si só, mas, se posteriormente houver acontecimento similar, será relembrado o episódio anterior, funcionando assim como uma espécie de agravante.

Em 2019 foi instituído o Sistema Integrado de Informação Criminal, pelo secretário-geral do Sistema de Segurança Interna. Esse sistema de intercâmbio de dados e informações é composto numa plataforma que assegura o intercâmbio de informação criminal.[59]

O acesso à plataforma faz-se de acordo com os seguintes perfis: [60]

> *"Órgãos de Polícia Criminal*
>
> *Perfil 1 - reservado aos responsáveis máximos de cada órgão de polícia criminal;*
>
> *Perfil 2 - reservado às chefias das unidades de investigação criminal de cada entidade participante na plataforma;*
>
> *Perfil 3 - reservado aos utilizadores que desempenhem funções de analistas.*
>
> *(...)*
>
> *Autoridades Judiciárias e Ministério Público*
>
> *Perfil 1 - reservado ao Procurador-Geral da República;*
>
> *Perfil 2 - reservado aos magistrados do Ministério Público envolvidos em funções de coordenação da investigação criminal ou no âmbito da prevenção criminal;*
>
> *Perfil 3 - reservado aos juízes que exerçam competências no âmbito da instrução criminal, relativamente aos processos de que sejam titulares, e aos magistrados do Ministério Público afetos aos inquéritos, sempre que estes desempenhem funções no Departamento Central de Investigação e Ação Penal (DCIAP) e, no âmbito da respetiva área de jurisdição processual, nos tribunais de primeira instância ou nos departamentos de investigação e ação penal (DIAP) das comarcas."*

59 *"a) A componente de segurança; b) Uma interface de acesso uniforme para cada órgão de polícia criminal; c) Uma componente técnica de apoio aos interfaces e ao acesso à informação; d) Uma componente de indexação, pesquisa e relacionamento de dados. 2 - As comunicações necessárias ao regular funcionamento da plataforma são efetuadas numa rede virtual cifrada dedicada."* Artigo 4.º da Lei 73/2009 de 12 de agosto.
60 Artigo 10.º da Lei 73/2009 de 12 de agosto.

CAPÍTULO 2. *INTELLIGENCE*: OS INTERVENIENTES

SUBCAPÍTULO 1. INSTITUIÇÕES INTERNACIONAIS

2.1.1 COMITÉS DE INFORMAÇÕES E DECISÃO

A integração de serviços de informações constitui-se a partir da abordagem democrática compreendida entre a política e as informações e, se por um lado existem aspetos positivos no uso dos serviços de informações, tais como o combate às novas ameaças e o auxílio à tomada de decisões sobre políticas internas e/ou externas, sobretudo nas áreas da economia e da segurança, por outro lado, encontram-se também aspetos negativos, tais como o abalo causado pelos serviços de informações aos Direitos Humanos internacionalmente afiançados, como o disposto no Art. 12.º da Declaração Universal dos Direitos do Homem, que data de 10 de dezembro de 1948.[61]

Os pioneiros da edificação de um sistema de informações envolveram a administração Parlamentar dos EUA, *"... por via do Senado (Senate Comittee on Intelligence) e do Congresso (House Permanent Select Committee on Intelligence)..."* [62]

Atualmente, quase todos os Estados Democráticos absorvem os seus Serviços de Informações na administração central.

A par disso, há hoje, mais do que nunca, uma tendência para as crescentes técnicas intrusivas na interceção de comunicações, tendência essa que transgride alguns direitos fundamentais constitucionalmente garantidos.

Contudo, credibilizar o processo do sistema das informações também passa pela curadoria dos Comités de Informações, pois só assim se poderão responsabilizar os serviços e garantir que os operacionais das informações não profanam princípios, direitos, liberdades e garantias.

Nos EUA, os Serviços de Informações são obrigados a informar os comités parlamentares, o sistema das informações tem um corpulento elemento de membros governamentais, através dos diversos órgãos de controlo e de direção, assente num Conselho Nacional de Segurança composta pelos responsáveis dos órgãos ligados ao Intel, entre eles destaco o Órgão de Assessoria Presidencial para as Informações Externas, ficando assim a licitude de todos os procedimentos administrativos, sobre forte controlo.

---

61 *"Ninguém sofrerá intromissões arbitrárias na vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito à proteção da lei."*

62 Esteves quando descreve as organizações, sistemas e modelos, mais propriamente, na descrição do Sistema anglo-saxónico in Informações e Segurança, p. 446 e ss.

Desde 1976 que o Intelligence Oversight Board supervisiona todas as informações, controlando a legalidade entre outras das seguintes atividades:[63]

- Interceção das comunicações;

- Violação da propriedade privada.

A par dos EUA, também o Reino Unido – RU – tem forte controlo sobre as informações, desta feita sobre a alçada do Comité de Informações e Segurança – CIS – que tem como tarefa examinar a administração, despesas e políticas dos três principais serviços de informações (MI5, MI6, GCHQ) do RU.

No Reino Unido, existem grandes diferenças jurídicas entre o MI5 e o MI6, a título de exemplo o *Interception of Comunnication Act* já não está em vigor – ICA de 1985, que foi criado com o intuito de avaliar queixas relativas as atividades do Serviço de Informações, sendo que o MI6 e o GCHQ ficaram de fora deste ICA. Só em 1994 é que o MI6 e o GCHQ ficaram também sobre a alçada jurídica do ICA, e a partir dessa mesma data, o CIS teve a delegação de competências para fiscalizar a totalidade dos serviços sobre a sua alçada.[64]

Em Portugal, o correspondente ao CIS, seria a união do SIRP com a Comissão de Fiscalização do SIRP (ver 3.4).

Então, o ponto de partida para os Comités de Informações e Decisão Intel resultará sempre pela precedência do interesse nacional, em detrimento de tudo o demais.

JOINT INTELLIGENCE COMITTEE - JIC (MI5, MI6, DIS, GCHQ)

O controlo da internet, hoje mais do que nunca, é supervisionado pelos serviços de informações dos quais fazem parte, entre outros, o JIC (Comité Conjunto do Serviço de Informações), entidade responsável pela produção diária de relatórios que após seriação são dados a conhecer ao Primeiro-Ministro Inglês.

O Governo Inglês divide as informações da seguinte forma:[65]

- MI5 Serviço de Segurança Interna.

- MI6 Serviço de Informações Externas

- SOCA Criminalidade Organizada

63 In Informações e Segurança, p. 446.
64 Idem
65 In, Informações e Segurança, p. 447.

GOVERNMENT COMMUNICATIONS HEADQUARTERS - GCHQ

O GCHQ tem vindo internamente a adotar medidas para acompanhar a evolução tecnológica e, desde 1998, está organizado em quatro ramos, conforme se descreve de seguida:

> *"- Sigint missions (missões de informação de origem eletromagnética), que inclui as subdivisões de matemática e criptanálise, tecnologias de informação e sistemas informáticos, linguísticos e de tradução, bem como a unidade de análise de informação;*
> *- Enterprise, que passa a pente fino as subdivisões da investigação de aplicações e das tecnologias emergentes, biometria, gestão dos conhecimentos e dos sistemas de informação, bem como relações com os fornecedores e subcontratados comerciais;*
> *- Corporate Management, que inclui os recursos humanos, auditoria interna e a equipa de arquitetura SINEWS (sigint New Systems);*
> *- Communications-Eletronics Security Group (CESG), encarregada da segurança da informação."* [66]

O GCHQ criou programas de vigilância da internet e das comunicações efetuadas através de telemóveis, assim, tem a possibilidade de garantir a constância da ciberdefesa e da luta contra o terrorismo, de dominar a internet, passando também por a intercetar, armazenar e vigiar de forma continuada.

FOREIGN INTELLIGENCE SURVEILLENCE - FIS

Ao FIS compete levar a cabo o Projeto-lei relativo à vigilância das informações externas, o Relatório *Fink*, que data de 1978, revelou já nessa data, que a privacidade pessoal para o FIS é algo de secundário, quando se tem como anfitrião e parceiro o Mega Programa de Vigilância *Echelon*, mais ainda com o seu upgrade com o quadro do Programa P415.[67]

66 In, *O Caso Snowden como os EUA espiam o mundo*, p. 206, e ss.
67 Idem, p. 204

SECURE AND TRUSTWORTHY CYBERSPACE - SATC

A SATC é a mais forte aliada da *Federal Cybersecurity Research and Development Strategic Plan* – RDSP – e da *National Privacy Research Strategy* – NPRS – que tem como intuito proteger e preservar o desenvolvimento social e económico, o RDSP menciona seis áreas críticas para o desenvolvimento da cibersegurança:

> *"...(1) scientific foundations; (2) risk management; (3) human aspects; (4) transitioning successful research into practice; (5) workforce development; and (6) enhancing the research infrastructure..."* [68]

O SATC desenvolve a cibersegurança e a privacidade através da interdisciplinaridade das seguintes áreas:

> *"...computing, communication and information sciences; engineering; economics; education; mathematics; statistics; and social and behavioral sciences..."* [69]

UNITED NATIONS SPECIAL COMMISSION – UNSC

A UNSC, doravante denominada por Comissão Especial das Nações Unidas – CENU – pertence às Comissões não permanentes, e que são acionadas após uma Resolução do Conselho da UN, havendo o Conselho de definir os seus termos e a sua abrangência, após isso deverá ficar demarcada um estratégia, bem como o plano de implementação da Missão de Observação.

Por norma, estas Comissões, numa primeira fase, recomendam aos infratores o cumprimento das obrigações no âmbito dos Protocolos previamente assinados, acessoriamente, é elaborado um relatório onde constem todas as matérias submetidas a análise prévia. Em seguida, estabelece a CENU concernente às inspeções físicas, caso se materializem. Também é frequente que, após Resolução, a UN prossiga com os objetivos, impondo sanções que por norma decretam prazos de execução para a implementação das recomendações anteriormente apontadas.

A parte mais relevante das resoluções, para além da prossecução dos objetivos, compreende por vezes medidas adicionais de restituição do dano causado, em forma de compensação, que possam

68 Consultado em 12 de outubro de 2016, in https://www.caecommunity.org/news/2016-secure-and-trustworthy-cyberspace-satc-program-solicitation
69 Idem

ser essenciais para a implementação da resolução e que garantam o correto cumprimento da observância dos Protocolos.[70]

FOREIGN INTELLIGENCE SURVEILLENCE COURT - FISC

O FISC data de 1978 e nasce da Recomendação do Senado Americano, pela necessidade de supervisionar o pedido de mandatos, relativos à vigilância de espiões dentro dos EUA. Grande parte desses mandatos são solicitados pela NSA e pelo FBI, contudo, após as revelações de Snowden, o FISC deixou de estar sediado no edifício Robert F. Kennedy do Departamento de Justiça e passou a estar localizado no edifício E. Barrett Prettyman U.S. Courthouse, ainda assim, mesmo com todas as restrições que deveriam ser garantidas pela reserva da privacidade, dos 35.529 pedidos de vigilância eletrónica só doze [71] é que foram recusados, isto desde 1978.

2.1.2 SISTEMA INTEGRADO DE INFORMAÇÕES

O Sistema Integrado de Informações agita os direitos fundamentais, quando integra as escutas judiciais e administrativas, em contraponto com os acordos de "segurança".

A lesão dos direitos fundamentais só pode operar se as normas que o permitam forem excecionais, ainda que, em alguns casos, possam admitir também uma interpretação extensiva, assente na sua utilização e valoração, tendo em conta para isso a necessidade, a proporcionalidade e a adequação.

A investigação criminal atua sempre num processo autónomo, decorrente de uma notícia de crime, o que logo à partida faculta a lesão de direitos fundamentais, visto estar em conformidade com a obediência à lei.

No caso das escutas administrativas, jamais podemos recorrer à analogia, mas segundo a redação do Art. 11° do Código Civil *"As normas excecionais não comportam aplicação analógica, mas admitem interpretação extensiva".*[72]

Nada repele que se faça uma valoração da escuta administrativa quando se opere uma conexão suportada em injunções relevantes de reconhecido interesse em matérias da segurança nacional.

---

70 Consultado em 14 de outubro de 2016, in https://search.un.org/results.php?query=resolu%C3%A7%C3%B5es&ie=utf8&output=xml_no_dtd&oe=utf8&Submit=Search&__utmt=1&__utma=114554307.777122877.1476469220.1476469220.1476469220.1&__utmb=114554307.1.10.1476469220&__utmc=114554307&__utmz=114554307.1476469220.1.1.utmcsr%3Dgoogle%7Cutmccn%3D%28organic%29%7Cutmcmd%3Dorganic%7Cutmctr%3D%28not+provided%29&_ga=GA1.2.777122877.1476469220&_gat=1&lang=en&rows=10&tpl=un

71 Dados da FISA in https://en.wikipedia.org/wiki/united_states_foreign_intelligence_surveillance_court#cite_note-7

72 O próprio Código Civil coloca esta ferramenta que é a da interpretação extensiva ao serviço do *Intelligence*, em todas as leis que necessitam de ampliação, assim cabe ao interprete/analista a verificação dos limites da norma.

Importa então distinguir uma escuta judiciária de uma escuta administrativa, esclarecer as suas delimitações e as suas extensões para que assim se possa legitimar a sua utilização no Sistema Integrado de Informações.

> *"10. The Assembly notes that the law in most States provides some protection for the privacy of their own citizens, but not that of foreigners. The Snowden files have shown that the United States NSA and its foreign partners, in particular among the "Five Eyes" partners (Australia, Canada, New Zealand, the United Kingdom and the United States), circumvent national restrictions by exchanging data on each other's citizens."* [73]
>
> *(Resolution 2045 (2015) Mass surveillance - European Parliamentary Assembly)*

SECURITY AGREMENT (UKUSA-FIVE EYES)

Este acordo de aliança técnico-política de segurança entre Estados tem como principal intuito criar um elo de ligação entre Estados com o objetivo de partilhar os frutos das interceções, concretizando uma corrente de trocas de informações em cadeia. Assim sendo, os diversos serviços (militares, segurança, justiça, ...) dos respetivos Estados têm uma forma privilegiada de concretizar os seus segmentos das informações.

Segundo o relatório Snowden, se por um lado os EUA vigiam os Italianos, os Canadianos escutam os Brasileiros e os Autralianos, os Indonésios, entre muitos outros. A título de exemplo, a Embaixada Americana em Itália intercetou 4 milhões de metadados telefónicos aos Italianos, em apenas dois meses, dezembro de 2012 e janeiro de 2013.[74]

A aliança UKUSA teve início em 1947 através de um *secret treaty* entre o UK e os USA, visando uma otimização das informações militares pelos serviços MI5 e MI6 contra o combate aos Soviéticos, só posteriormente apareceram os outros três aliados, transformando o UKUSA em *Five Eyes*, e apenas em 1976 este acordo foi tornado público.

73 Consultado em 15 de outubro de 2016, in https://ccdcoe.org/sites/default/files/documents/CoE-150421-MassSurveillanceRes2045.pdf

74 Reportagem do L`Espresso - Da qui ci spiano gli americani I documenti segreti di Edward Snowden rivelano come i servizi Usa hanno controllato le telefonate della leadership italiana dall'ambasciata di via Veneto a Roma. E smentiscono le rassicurazioni del governo Letta di Gleen Greenwald e Stefania Maurizi. Consultado em 05 de dezembro de 2016 http://espresso.repubblica.it/inchieste/2013/12/05/news/da-qui-ci-spiano-gli-americani-1.144421?refresh_ce

Os Five Eyes trabalham sobretudo de duas formas: a primeira intercetando mensagens, telegramas e chamadas telefónicas; já a segunda forma assegura o tratamento e a análise de dados através do Echelon.

> *"... antecipar que a vigilância eletrónica das comunicações continuaria a ser a forma mais importante dos serviços de informações no período do pós-guerra, tal como fora durante a Segunda Guerra Mundial."* [75]

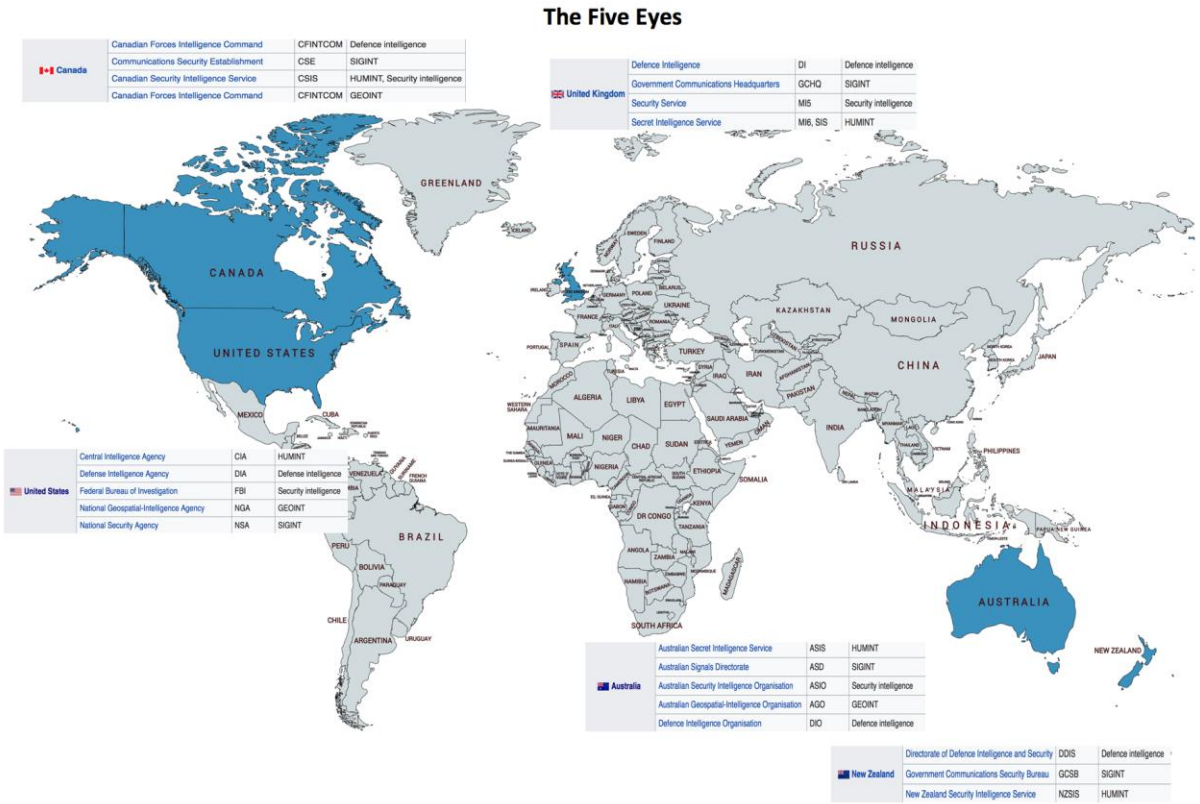

Figura 3 - Atribuições da UKUSA e respetiva distribuição de esferas entre entidades.[76]

Os Five Eyes cobrem o mundo inteiro através das atribuições de zonas de intervenção: o CSEC supervisiona a interceção de telecomunicações do Norte da Rússia e de parte da Europa; a ASD cobre a parte oriental do oceano Índico, o Sudoeste Asiático e o Pacífico Sul; a GCSB fica encarregue da região da Ásia e do Pacífico.

Na Nova Zelândia, mais propriamente na província de Waihopai, está colocada uma base cujo comando está sob a alçada do GCHQ e onde são aplicados anualmente 500 milhões de dólares, aí

75 Campbell, D. They`ve got it taped, somebody`s listening, New Statesman, 12 de agosto de 1988.
76 In, https://www.reddit.com/r/MapPorn/comments/7whd4u/the_five_eyes_and_the_major_agencies_involved_in/

trabalham mais de 15 mil operadores, sendo considerada *"... a maior componente do serviço de informações britânico",* [77] . Esta base tem capacidade para espiar a Europa, a África e a Rússia.

Em virtude desta mais valia por parte dos membros da Five Eyes, outros têm logrado da sua integração nesta aliança — são os casos da Noruega, da Dinamarca, da Suécia, da Coreia do Sul, da Turquia e, inclusive, da República Popular da China (por incrível que pareça), que faz parte desta aliança desde 1990 com uma base sino-americana na província de Uigir, em Xinjiang.

SPECIAL COLLETION SERVICE - SCS

Da SCS fazem parte a CIA e a NSA, estes serviços de informações, pese embora trabalhem separadamente as informações, partilham há muito informações, desde o tempo da Guerra Fria. Essa partilha de informação tornou-se ainda mais efetiva, quer pelo reforço de procedimentos no pós 11 de setembro quer pela necessidade real das missões diplomáticas fora dos EUA, a SCS permite aos EUA vigiar redes terroristas e do tráfico de droga.

Contudo, a vigilância eletrónica destes serviços faz com que seja possível vigiar e piratear as redes estrangeiras, esta vigilância eletrónica tem vindo a tornar-se primordial nos dias de hoje, quando se pretende uma verdadeira e totalitária supervisão eletrónica.

2.1.3 CENTRAL INTELLIGENCE AGENCY

O então presidente do EUA Frankelin D. Roosevelt, em 1946, decidiu criar uma nova agência de informações que estivesse fora das Forças Armadas (civil), muito pelo conteúdo do relatório de Harry Truman, que dizia *"...os serviços secretos norte-americanos eram esparsos, não comunicavam entre si, não eram centralizados..."* [78]

Ainda que nascida sem poderes, pois não podia efetuar operações de sabotagem e de contraespionagem, nem colher autonomamente informações, naquela altura, a CIA denominava-se de CIG – *Central Intelligence Group* — e esta limitava-se apenas a coligir, analisar, organizar e distribuir entre as diversas repartições militares e governamentais as informações que lhe tivessem chegado desses departamentos.

Mais tarde, em consequência da desorganização que pairava sobre os serviços de informações dos EUA, manifestou-se um aumento de poderes da CIG, alargando-os à espionagem e contraespionagem fora dos EUA, independente de qualquer relacionamento com a *National Intelligence*

77 Segundo Antoine Lefébure, historiador dos media e fundador da revista Interférences, em O Caso Snowden, p. 204
78 In CIA, p. 27.

Authority (Serviços de Informações das Forças Armadas). Nascia assim um serviço de informações para lá das guerras, com o objetivo de informar o que ia sucedendo no mundo, mas, à data, com relevância ao que se passava na URSS.

Ainda que em 1947 *"... metade de toda a informação sobre os soviéticos coletada pelos serviços de informação norte-americanos fosse completamente falsa."* [79] *, a* CIA não só tinha como missão saber o que os outros andavam a fazer, mas também impedi-los se necessário fosse.

Após a II Grande Guerra, a CIA questionou os seus advogados sobre a legalidade de uma possível intervenção da sua parte na tentativa de interferência nas eleições de Itália, pois a FIAT já havia acordado instalar-se na URSS caso Togliatti ganhasse as eleições. Os advogados confirmaram as ilegalidades, mas foram ignorados por Hillenkoetter e Angleton, diretor da *National Security Council* — NSC — e Coordenador do *Office of Special Operations*, respetivamente.[80]

A CIA fez nascer em Itália o *Special Procedures Group*, trazendo consigo a mais-valia da "negação plausível" da sua existência, por parte do Governo dos EUA, mais ainda, *"... os agentes da CIA conduziam, no mundo inteiro, operações clandestinas, por vezes arriscadas, para colocarem microfones, copiarem discos rígidos ou roubarem dados."* [81]

Seis anos passados da data de fundação da CIA, e agora sim uma CIA com poderes plenos, privava a recém criada NSA às suas informações de credenciação mais elevada.

Hoje a CIA tem como missão produzir informações de segurança nacional ao governo do EUA e congregar informações sobre governos estrangeiros, corporações e indivíduos.[82]

2.1.4 NATIONAL SECURITY AGENCY

A *National Security Agency* – NSA foi criada em 1952 [83] com o intuito de colmatar algumas falhas na recolha e tratamento das informações, durante a Guerra da Coreia, mais propriamente nas informações com origem eletromagnética, não só as informações externas aos EUA, mas também as informações que saíam dos EUA (doméstica), o que incluía vigiar os próprios cidadãos americanos. Este processo, à data, era altamente secreto e apenas alguns membros do Governo sabiam da sua existência. O processo em si passava pela recolha direta dos telegramas internacionais, nas redes de telégrafos americanas, cerca de 150 mil telegramas eram entregues mensalmente à NSA.[84]

79 Idem, p. 32
80 Idem, p. 37
81 Consultado em 26 de outubro de 2016 In https://www.yahoo.com/news/inside-secret-world-americas-top-eavesdropping-spies-174500519.html
82 CIA, About CIA, Mission, Consultado em 05 de junho de 2017 In https://www.cia.gov/about-cia/cia-vision-mission-values
83 NSA/CSS, History of The Insignia, Consultado em 05 de junho de 2017 In https://www.nsa.gov/about/cryptologic-heritage/center-cryptologic-history/insignia/nsa-insignia.shtml
84 In O caso Snowden como os EUA espiam o mundo, p. 125.

Desde 1967 que os EUA vigiam os próprios cidadãos, a comprovar tal facto a Operação *Minaret* e o Projeto *Shamrock*. A *Minaret* visava vigiar os grupos que se opunham à Guerra do Vietname, já o *Shamrock* visava vigiar os manifestantes dos Direitos dos Negros.[85]

A NSA começou por ter um papel de menor proeminência do que a CIA, assim nasceu uma crescente encrespação entre as agências e a ocultação mútua de comunicar informações Top Secret. A CIA usava como pretexto para tal o facto de o pessoal da NSA *"... não ser regularmente submetido a um teste de polígrafo."*[86], teste esse que hoje é obrigatório para ingressar nas agências de informações. Daí a preponderância ampliada da *Special Colletion Service* – SCS. [87]

A NSA dirigia vários projetos, entre outros, o *Project Wideband Extradiction* que intercetava ondas e frequências gigantes.

Com tantas interceções levadas a cabo pela NSA, por vezes ocorrem incidentes diplomáticos, tais como as supostas escutas à Chanceler Alemã Angela Merkel.

O procurador-geral da Alemanha, Harald Range, refere que existem provas de que as escutas teriam de facto sucedido, *"Informei a comissão parlamentar de assuntos jurídicos de que abri uma investigação preliminar sobre escutas ao celular da chanceler"* [88], o procurador referiu que não ia levar a cabo uma investigação sobre a interceção de comunicações eletrónicas de milhões de cidadãos alemães, tornados conhecidos pelos documentos confidenciais expostos por Snowden.[89]

Segundo o jornal Alemão DW, Obama pediu desculpas a Merkel e garantiu que elas não se repetiriam.[90]

O Sr. Eurodeputado Dr. Carlos Coelho, Presidente da Comissão Especial do PE (2000), descreve a NSA e o seu sistema da seguinte forma:

85 Idem
86 Ibidem, p. 155.
87 Ronald Kessler, Secret Service Agents Are Not Polygraphed, Consultado em 05 de junho de In http://www.newsmax.com/RonaldKessler/Secret-Service-polygraph-FBI/2012/05/07/id/438214/
88 Consultado em 17 de outubro de 2016, in http://www.dw.com/pt-br/justi%C3%A7a-alem%C3%A3-vai-investigar-den%C3%BAncia-de-que-celular-de-merkel-foi-espionado/a-17682922
89 O procurador-geral Harald Range informou que as "Investigações preliminares extensivas produziram evidência factual suficiente de que oficiais não identificados de inteligência dos EUA grampearam um telefone celular da chanceler Angela Merkel", aponta um comunicado do gabinete de Range. A investigação será feita contra "pessoas não identificadas" em vez de especificamente contra a NSA. Consultado em 11 de junho de 2017, in http://www.folhadelondrina.com.br/mundo/justica-alema-vai-investigar-espionagem-883302.html
90 Consultado em 17 de outubro de 2016, in http://www.dw.com/pt-br/justi%C3%A7a-alem%C3%A3-vai-investigar-den%C3%BAncia-de-que-celular-de-merkel-foi-espionado/a-17682922

" A mais secreta das agências americanas

40.000 agentes

3.5 mil milhões de dólares ano

90.000 agentes (Dados 2001 Body of Secrets)

Estatísticas em cada meia hora

1.000.000 mensagens recebidas

6.500 identificadas nos filtros

2.000 selecionadas na 2ª filtragem

20 selecionadas por técnicos

2 relatórios produzidos para o CNS"

2.1.5 DEFENSE INTELLIGENCE AGENCY

O Presidente dos EUA, John F. Kennedy, e o seu Secretário da Defesa, Robert McNamara, criaram a *Defense Intelligence Agency* – DIA, em 1961.

A estruturação da DIA foi elaborada pelo diretor designado da agência, o tenente-general Joseph Carroll, mas, para o Secretário da Defesa, Robert McNamara, a criação da agência tinha uma supervisão encapotada sobre a perspetiva global dos vários serviços de inteligência (militares), engendrada com o objetivo de analisar, produzir e disseminar informações militares para apoiar os decisores militares e políticos.

A DIA teve logo como missão observar as movimentações de operações, informações, pessoais e logísticas, levadas a cabo pela URSS, mais propriamente a conhecida crise dos mísseis em Havana – Cuba.

Em 1963, a DIA aumentou a sua capacidade com um *Automated Data Processing Center* e com o envolvimento do recurso a *Scientific and Technological Intelligence Diretorate*. Em 1965, a DIA já tinha uma escola de formação em Washington, onde lecionava cursos, tais como, *"Attache Staff Course"*, o que fazia com que, subsequentemente, colocasse os seus colaboradores em toda a parte do mundo, concebendo assim a *Defense Attache System* – DAS.[91]

À data, a tradução não era como agora, quase totalmente automatizada, mas sim manual, este facto levou a um aumento do pessoal especializado em tradução. Estes programas de tradução

91 In https://www.youtube.com/watch?v=P2U3lKY597U

automatizada, ainda que não tenham tantos linguistas/tradutores como nos anos 60, terão de ter sempre analistas que contextualizem toda a informação. [92]

As décadas de 60, 70, e 80 foram extraordinárias para o Intel: em 60, a Guerra entre o Vietname e os EUA, em 70 a invasão do Afeganistão pela União Soviética, em 1989 o DIA produziu um documento intitulado *Soviet Military Power*, distribuído por todos os Americanos para que estes tivessem em consideração a real ameaça.[93]

Os anos 80 conduziram ainda o Intel à China, à Nicarágua, a El Salvador. Estes dois últimos conduziram ao princípio de mais uma subagência de Intel, a *Central America Joint Intelligence Team*.

A já pródiga década de 80 teve ainda um revés para o Intel com o surgimento da 3ª onda do Terrorismo, também os Estados deixaram de fazer a Guerra pela Guerra, e passaram a atuar inopinadamente com ataques de terrorismo cirúrgicos, mais propriamente em 1985, com explosões e assassinatos, entre outros, nas seguintes ocasiões:

12 de abril em Madrid

13 de abril em Paris

19 de junho em Frankfurt

01 de julho em Madrid

08 de agosto na Base Aérea Americana perto de Frankfurt

03 de setembro em Atenas

16 e 25 de setembro em Roma

23 de novembro em Atenas

24 de novembro em Frankfurt

Em 1986, a DIA passa a ser uma fonte de suporte ao Estado-Maior das Forças Armadas Americanas.

Depois de 1989, após a queda do muro de Berlim e do colapso Soviético, a DIA direcionou o seu azimute para a "Operação *Desert Storm*", devido à invasão do Kuwait por parte do Iraque, juntamente a tudo isto soma-se o envolvimento da DIA, no Haiti, na Bósnia, no Kosovo, e em África

92 Na criminalidade organizada ou altamente organizada acontece com frequência a troca/codificação de palavra chaves tais como por exemplo: em vez de verbalizarem ou escreverem explosivos podem por exemplo chamar-lhes pipocas, e aqui por mais Inteligência artificial que possa existir a inteligência similar à humana exibida por mecanismos, nunca alcançará uma interpretação real, só ao alcance da mente humana.

93 A Soviet Military Power foi uma publicação de periodicidade ocasional levada a cabo pela DIA com o intuito de informar e alertar toda a população, sobre o conceito estratégico e as capacidades militares da URSS, esta publicação não servia só para os Americanos, mas também para outros países daí a sua publicação em outras línguas tais como Alemão, Francês Japonês e Italiano, países estes que atualmente fazem parte do atual G8. O conjunto do G8, segundo o Fundo Monetário Internacional (FMI), representa mais de 64% da riqueza líquida global, e são as economias mais avançadas do mundo.

pelas revoluções levadas a cabo pelas diferentes etnias. A DIA manteve sempre o seu foco nas potências da Líbia, Irão e Coreia do Norte.

Após o 11 de setembro, a DIA foi ampliada ainda mais, em toda a sua estrutura, foram atribuídas mais verbas, e centenas de analistas foram destacados para missões, entre outras, no Iraque e no Afeganistão.

A DIA liderou a inspeção ao Iraque em busca de Armas de Destruição Massiva – ADM.[94]

O modo diferenciado de subversão e insurgência levou a uma gigantesca transformação da DIA, assim a partir de 2006 a DIA foi redefinida nas repartições que se apresentam em seguida:

SOUTHCOM

CENTCOM

STRATCOM

NORTHCOM

TRANSCOM

AFRICOM

JFCOM

SOCOM

PACOM

Já em 2008, a DIA fundou mais uma subagência: a *Defense Couterintelligence and Humint Center*.[95]

94 In https://www.youtube.com/watch?v=FWU0s1Uvwk4
95 In http://www.dia.mil/

SUBCAPÍTULO 2. INSTITUIÇÕES NACIONAIS

2.2.1 SISTEMA DE INFORMAÇÕES DA REPÚBLICA PORTUGUESA

O SIRP tem como propósito produzir informações para apoio à tomada de decisão dos membros e órgãos do governo, principalmente em matérias que digam respeito aos segmentos de informação.

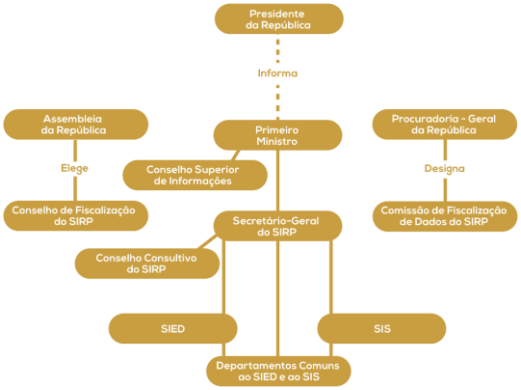

Figura 4 - Organigrama da estrutura do SIRP, onde se verifica a ramificação dos vários conselhos e comissões.[96]

A capacidade dos Estados democráticos, está hoje, mais do que nunca, perante uma nova ameaça: o excesso de informação. Devido aos elevados fluxos de informação, o SIRP obrigar-se-á a uma reforma profunda, quer devido à sua necessidade, quer devido à sua não proporcionalidade entre a segurança e a reserva da vida privada. À data, as garantias legais pendem mais para a hiperproteção da vida privada.

> *"Os Serviços podem recorrer a técnicas de natureza intrusiva como a interceção das comunicações, violação de propriedade privada, ações de vigilância, ...".*[97]

A teoria penal do inimigo vem também anuir o recurso a técnicas de natureza intrusiva tendo como alvo o *"indivíduo perigoso"*.[98] Esta teoria adere à quebra da garantia processual penal e à não

96 In https://www.sirp.pt/quem-somos/organograma-e-estrutura
97 Neste âmbito Pedro Esteves explica a dinâmica do SIRP, dos meios, dos fiscais políticos e judiciais, e a sua justificação comunitária e o interesse público da causa, em Estado e Informações: Uma perspetiva sistémica, in Informações e Segurança, p. 439, ss.
98 Jakobs. e Meliá, in Direito Penal do Inimigo, Noções e Críticas, p. 23.

reserva da vida privada, igual à dos indivíduos pró- sociais, considerando que a garantia processual deverá ser desigual na sua forma em função da perigosidade do comportamento.

Aos olhos da teoria penal do inimigo, fará sentido observar o código penal, recorrendo a uma interpretação sociológica, socorrendo-se de uma ponderação de valores nos crimes contra a reserva da vida privada, nomeadamente, no Artigo 190.º Violação de domicílio ou perturbação da vida privada; no Artigo 192.º Devassa da vida privada; no Artigo 193.º Devassa por meio de informática; e no Artigo 194.º Violação de correspondência ou de telecomunicações.[99]

Jorge Silva Carvalho, ex-diretor do SIED, foi a tribunal pela acusação de atividades ilegais (violação do segredo de Estado, acesso indevido a dados pessoais e abuso de poder) realizadas por agentes dos Serviços de Informações. Silva Carvalho disse em tribunal ser prática habitual este tipo de atividades e afirmou que o secretário-geral do SIED, Júlio Pereira, sabia das práticas ilegais cometidas por agentes das "secretas" e que inclusive estavam previstas num manual interno de procedimentos. Silva Carvalho mencionou ainda como conhecedores destas práticas: Rui Pereira, Teles Pereira, Margarida Blasco e Antero Luís, todos estes ex. diretores dos Serviços de Informações.[100]

A Constituição da República Portuguesa, para além de limitar as atividades ilegais acima descritas, circunscreve veementemente os SI na sua atuação, entre outras, na interceção de comunicações, garantindo fidúcia às seguintes inviolabilidades:

> *"1. O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis.*
>
> *2. A entrada no domicílio dos cidadãos contra a sua vontade só pode ser ordenada pela autoridade judicial competente, nos casos e segundo as formas previstos na lei.*
>
> *3. Ninguém pode entrar durante a noite no domicílio de qualquer pessoa sem o seu consentimento, salvo em situação de flagrante delito ou mediante autorização judicial em casos de criminalidade especialmente violenta ou altamente organizada, incluindo o terrorismo e o tráfico de pessoas, de armas e de estupefacientes, nos termos previstos na lei.*

99 Decreto-Lei n.º 48/95, de 15 de Março - Código Penal na sua última versão.
100 In Jornal SO,L Edição n.º 486, de 19 de dezembro de 2015, p. 37.

4. É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal." [101]

COMISSÃO DE FISCALIZAÇÃO

Os Estados verdadeiramente democráticos têm instrumentos consideráveis de fiscalização externa e de verificação, sendo estes últimos de exigência indispensável por influência maioritariamente social. Ao SIRP, derivado desta Comissão de Fiscalização, é lhe controlada toda a sua atividade discricionária, assim sendo a autoridade do SIRP abraça toda uma legalidade intangível.

Entre outros papéis, cabe à comissão delimitar ao SIRP a necessidade de conhecer informação sensível e minimizar as atividades cobertas, principalmente aquelas que tocam nas questões de licitude. Cabe também à comissão a sua ligação intrinsecamente direta ao fator conhecimento *vs* autorização.

Pedro Esteves sustenta ainda a não autonomia dos serviços muito por causa das *"... fugas de informações e escândalos público ...".* [102]

As estruturas formais dos SI, na generalidade dos Estados, contam com a intervenção do sistema político, maioritariamente de origem Governamental.

Para além do anteriormente referido, o Parlamento tem uma forte representatividade na responsabilização política, com as suas comissões parlamentares especializadas, particularmente a Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias.[103] Esta comissão tem caráter vinculativo e possibilidade de acesso a documentos independentemente do grau de credenciação (ver em 3.4).

2.2.2 SERVIÇO DE INFORMAÇÕES E SEGURANÇA

O Serviço de Informações e Segurança – SIS tem no campo de ação das suas tarefas específicas o desenvolvimento de forma regular, a pesquisa, a análise e o processamento de notícias e a difusão e arquivo das informações produzidas, tendo de, designadamente:

101 Artigo 34.º Inviolabilidade do domicílio e da correspondência, da Constituição da República Portuguesa.
102 In Informações e Segurança, p. 442, ss.
103 *"Exercemos atribuições legislativas e de fiscalização da atividade do Governo e da Administração, designadamente, no âmbito dos assuntos constitucionais, direitos fundamentais, justiça, administração interna, sistema prisional, imigração, asilo e refugiados, espaço de liberdade, segurança e justiça (no âmbito da integração europeia), assuntos institucionais e regimentais, exercício do mandato de Deputado, direitos humanos, legislação eleitoral, igualdade e não discriminação, e proteção das crianças e jovens em risco."* O Presidente da Comissão Pedro Carlos Bacelar de Vasconcelos, in http://www.parlamento.pt/sites/COM/XIIILEG/1CACDLG/Apresentacao/Paginas/default.aspx

" a) Acionar os meios técnicos e humanos de que tenha sido dotado para a produção de informações, desenvolvendo a sua atividade de acordo com as orientações fixadas pelo Primeiro -Ministro e no âmbito das instruções e diretivas dimanadas do Secretário -Geral;

b) Elaborar os estudos e preparar os documentos que lhe forem determinados;

c) Difundir as informações produzidas, de forma pontual e sistemática, às entidades que lhe forem indicadas;

d) Comunicar às entidades competentes para a investigação criminal e para o exercício da ação penal os factos configuráveis como ilícitos criminais, salvaguardado o que na lei se dispõe sobre segredo de Estado;

e) Comunicar às entidades competentes, nos termos da lei, as notícias e informações de que tenha conhecimento e respeitantes à segurança interna e à prevenção e repressão da criminalidade." [104]

Caso se verifiquem as alíneas d) e e), estaremos a falar de crimes, como tal, o âmbito da competência cairá na PJ, pois só esta é que é visada pela Lei 101/2001,[105] de 25 de agosto - Regime Jurídico das Ações Encobertas - RJAE, mas este regime de ações encobertas deixa uma abertura a todos os Serviços de Informações.[106]

"... o Serviço de Informações de Segurança não pode, como também se viu, proceder à interceção de comunicações nem, em geral, pôr em causa direitos, liberdades e garantias dos cidadãos." [107]

Já a Sra. Procuradora-Geral Distrital de Lisboa, Dra. Maria José Morgado, admite as escutas telefónicas, por parte dos Serviços de Informações, como medida preventiva, relembrando que é isso que acontece em França, onde são feitas escutas administrativas para garantir a segurança dos cidadãos.[108]

104 Artigo 33.º orgânica do Secretário -Geral do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa (SIED) e do Serviço de Informações de Segurança (SIS), Republicação da Lei n.º 9/2007, de 19 de fevereiro, em Diário da República, 1.ª série — N.º 155 — 13 de agosto de 2014 com a redação atual e demais correções materiais.
105 Ver a competência exclusiva para as escutas em matéria de investigação criminal no Subcapítulo 3.5.
106 No subcapítulo 3.5 iremos aprofundar a abertura deixada pelo RJAE.
107 O Professor Rui Pereira, em Os Desafios do Terrorismo: A Resposta Penal e o Sistema de Informações, in Informações e Segurança, p. 509.
108 Consultado em 11 de agosto de 2017 in https://www.rtp.pt/noticias/pais/maria-jose-morgado-defende-escutas-telefonicas_n53475

2.2.3 SERVIÇO DE INFORMAÇÕES ESTRATÉGICOS DE DEFESA

O Serviço de Informações Estratégicos de Defesa – SIED tem hoje uma abordagem para o exterior distintamente recomendável, com o intuito de desmistificar a missão e a forma de implementação dos Serviços de Informações, doutrinando a Sociedade Civil à Cultura de Informações dando a conhecer a dimensão e as balizagens de ação dos Serviços de Informações.

O SIED tem por missão produzir informações de salvaguarda da independência nacional, dos interesses nacionais e da segurança externa do Estado Português. Assegurando também as informações necessárias sobre as ameaças de origem externa à segurança interna. Neste quadro, o SIED contribui para a produção de informação privilegiada, tendo que, designadamente: [109]

> *" a) Acionar os meios técnicos e humanos de que tenha sido dotado para a produção de informações, desenvolvendo a sua atividade de acordo com as orientações fixadas pelo Primeiro -Ministro e no âmbito das instruções e diretivas dimanadas do Secretário -Geral;*
>
> *b) Elaborar os estudos e preparar os documentos que lhe forem determinados;*
>
> *c) Difundir as informações produzidas, de forma pontual e sistemática, às entidades que lhe forem indicadas;*
>
> *d) Comunicar às entidades competentes para a investigação criminal e para o exercício da ação penal os factos configuráveis como ilícitos criminais, salvaguardado o que na lei se dispõe sobre segredo de Estado;*
>
> *e) Comunicar às entidades competentes, nos termos da lei, as notícias e informações de que tenha conhecimento e respeitantes à segurança do Estado e à prevenção e repressão da criminalidade."* [110]

A par disso, incumbe também ao SIED avaliar a ameaça terrorista, alertar e identificar redes internacionais de crime organizado, nomeadamente as envolvidas em narcotráfico, facilitação da imigração ilegal e proliferação nuclear, biológica e química (NBQ). Ao mesmo tempo, o SIED monitoriza a segurança das comunidades portuguesas residentes no estrangeiro, o comprometimento

109 Artigo 26.º orgânica do Secretário -Geral do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa (SIED) e do Serviço de Informações de Segurança (SIS), Republicação da Lei n.º 9/2007, de 19 de fevereiro, em Diário da República, 1.ª série — N.º 155 — 13 de agosto de 2014 com a redação atual e demais correções materiais.

110 Também o SIED a par do SIS tem uma abertura deixada no RJAE, que será tratada no subcapítulo 3.5.

dos interesses nacionais em matérias políticas, sociais, económicas, energéticas e de defesa [111] que sejam prioritárias à estratégia do estado português.

2.2.4 CENTRO DE INFORMAÇÕES E SEGURANÇA MILITAR

Sun Tzu proferiu a seguinte frase *"... se quer a paz, prepare-se para a guerra ..."* e esta máxima assenta que nem uma luva ao Centro de Informações e Segurança Militar – CISMIL, que tem como missão assegurar a produção de informações e contrainformações e segurança necessárias ao cumprimento das missões das Forças Armadas e à garantia da segurança militar e, quanto às suas atribuições específicas, promover continuamente a pesquisa, a análise e o processamento de notícias e a difusão e arquivo das informações produzidas.

Cabe ao CISMIL dar apoio ao Chefe do Estado-Maior General das Forças Armadas – CEMGFA – nas missões e operações das Forças Armadas, muitas delas levadas a cabo através do Comando Conjunto para as Operações Militares – CCOM. Cabe também ao CISMIL a gestão da informação geoespacial e das células de informações militares.

> *"... Pode acontecer um atentado terrorista. (...) Também corremos riscos que resultam das nossas obrigações internacionais face às alianças a que pertencemos e à nossa posição estratégica (...) ameaças quer aéreas quer navais (...) A única forma de nos anteciparmos a um ataque daquele tipo é termos um serviços de informações capazes de ter notícias e conseguir infiltrar organizações dessas ..."* [112]

Os adidos de defesa ou militares acreditados em Portugal também são monitorizados, pelo CISMIL.

Ficam de fora das competências do CISMIL as matérias relativas à investigação criminal ou ao processo penal, tendo o CISMIL de comunicar às entidades competentes, nos termos da lei, as notícias e as informações de que tenha conhecimento e respeitantes à segurança do Estado e à prevenção e repressão da criminalidade.[113]

---

111 Relativamente à Defesa adverte-se que, o SIED anteriormente era SIEDM, no qual o M fazia referência a Militar mas, agora as Informações Militares relativas às Forças Armadas e necessárias ao cumprimento das suas missões especificas e à garantia da segurança militar são tratadas pelo Centro de Informações e Segurança Militar – CISMIL.

112 Entrevista do General Loureiro dos Santos, onde o especialista em Estratégia fala da sensação de insegurança, e da falta que faz as escutas, aos Serviços de Informações, in Diário de Notícias, em 07 de fevereiro de 2016, p. 14.

113 Alínea o) do N.2 do Art. 32º do Decreto-Lei 184/2014 de 29 de dezembro - Lei Orgânica do EMGFA.

Não resta qualquer dúvida que o *Intelligence* é uma ferramenta indispensável para as Forças Armadas, sucede que as estas recolhem muita das informações por via das Fontes Abertas, mas o novo *modus operandi* deixa aos comandantes militares uma dependência excessiva de informação.

Por norma, o Intel das FA ignora o salvaguardado na CRP no seu Artigo 41.º Liberdade de Consciência, de Religião e de Culto [114], pois, nas FA, a pesquisa objetiva de notícias nos seus domínios temáticos deve ter em conta prioritariamente os motivos étnicos, religiosos e rácicos, em virtude de o potencial dos conflitos ter, predominantemente, a sua origem natural nesses fundamentos, sobretudo no continente africano, na região dos Balcãs e na região Oriental.

> *"... a participação nos conflitos de outras fontes de poder social que não as militares, lançaram novos desafios no domínio do Intelligence. Produziu-se uma alteração, simultaneamente, quantitativa, qualitativa e temporal das necessidades de informação."* [115]

No continente africano, na região dos Balcãs e na região Oriental, não há novos assuntos, apenas os antecedentes sociais, os conflitos interétnicos e as relações esporádicas com o exterior.

Assim sendo, é fulcral monitorizar, para além das agitações religiosas e étnicas, os desenvolvimentos políticos, sociais e económicos nas regiões, bem como o acompanhamento das elites, grupos estes de interação e influência.

2.2.5 AUTORIDADE NACIONAL DE SEGURANÇA

A proteção e a salvaguarda da informação classificada é da competência exclusiva da Autoridade Nacional de Segurança – ANS.[116] Autoridade esta que se aplica simplesmente ao seu Diretor Geral. A ANS também administra o GNS.

---

114 Principalmente no ponto 4. onde diz que *"As igrejas e outras comunidades religiosas estão separadas do Estado e são livres na sua organização e no exercício das suas funções e cultos"*, este ponto só fará sentido quanto aos Estados que não utilizam a xaria (Direito Islâmico) como fonte de direito Primário, e que os seus governantes não sejam considerados Profetas. Em alguns países o Alcorão faz Jurisprudência, assim como a Suna.

115 Carlos Martins Branco descreve A ONU, o *Intelligence* e as Operações de Paz no Pós-Guerra-Fria. Oportunidades e Riscos, in Informações e Segurança, p. 161, ss.

116 O Decreto-Lei n.º 3/2012 de 16 de janeiro no seu artigo 4.º n.º1 diz que "O diretor-geral é, por inerência, a ANS", não se compreende aqui o facto de se atribuir uma designação de Autoridade Nacional a uma pessoa singular. Aqui argui-se o porquê de dois nomes GNS e ANS na mesma instituição. Bastando para isso conferir poderes de Autoridade ao Diretor-Geral. Argui-se no mesmo artigo, mas agora no n.2 a atribuição de tantas competências ao Diretor-Geral e não à instituição.

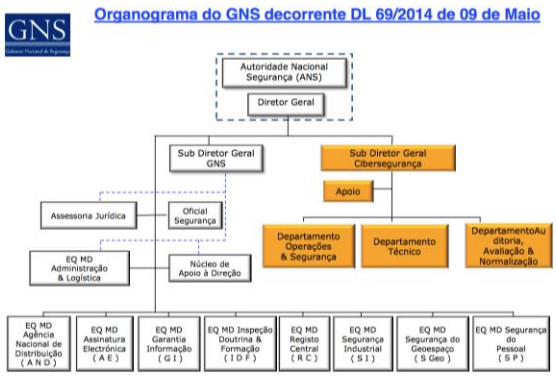

Figura 5 - Confere-se no topo que a ANS é só o seu Diretor Geral.[117]

GABINETE NACIONAL DE SEGURANÇA

O Gabinete Nacional de Segurança – GNS tem por missão a garantia da segurança. Ao GNS compete a autoridade de credenciação de pessoas e empresas para o acesso e manuseamento de informação classificada, fiscalização de entidades que atuem no âmbito do Sistema de Certificação Eletrónica do Estado. O GNS atua também no âmbito do Sistema de Certificação Eletrónica do Estado — Infraestrutura de Chaves Públicas (SCEE), como autoridade credenciadora e de fiscalização de outras entidades. O GNS é ainda o elo de ligação à OTAN para a Cibersegurança e Ciberdefesa.

Em virtude da revisão à Segurança da informação e após a Resolução do Conselho de Ministros n.12/2012 foi criado um Centro Nacional de Cibersegurança – CNC, presidido pelo diretor do GNS, Centro que foi implementado no sentido de dilatar a capacidade de proteção e defesa do Ciberespaço.[118]

SEGNAC 3 e 4

Em 1994, através da Resolução do Conselho de Ministros n.º 16/94 foram implementadas as instruções para a segurança nacional - Segurança das Telecomunicações, adiante designado por SEGNAC 3.[119]

Estas instruções só são válidas quando o conteúdo é transmitido por meios elétricos e eletrónicos.

O SEGNAC 3 também identifica os meios de telecomunicações não seguros, que são os seguintes:

117 In https://www.gns.gov.pt/organograma.aspx
118 In Estratégia da Informação e Segurança do Ciberespaço, IDN Cadernos n.12, p. 56, ss.
119 As Forças Armadas (Estado-Maior dos Ramos, Marinha, Exército e Força Aérea) ficam excluídas destas instruções, por isso só aplicáveis ao Estado, aos seus Ministérios, no qual se inclui o Ministério da Defesa Nacional, bem como todas as instituição civis. In ponto 1.1.2 do Capítulo I do SEGNAC 3.

" I) Intercomunicador;

II) Telefone;

III) Radiotelefone – telemóvel;

IV) Telecópia – fax;

V) Telex;

VI) Teleconferência;

VII) Correio eletrónico."[120]

O SEGNAC 3 vai ainda mais além, proibindo *"... a utilização de telefones não seguros para discussão e comunicação de matérias classificadas ..."* [121]

Em 1989, a Resolução do Conselho de Ministros n.º 5/90 demanda as instruções sobre a Segurança Informática, adiante designado por SEGNAC 4, e que, entre outros, atribuiu o Regime de Segredo aos Centros de informática do Estados ou privados que desempenhassem atividades com um dos três graus de segurança, e são eles *"... Muito secreto, Secreto e Confidencial ... ".*[122]

Não obstante a existência do Regime do Segredo de Estado da Lei Orgânica n.º 2/2014, de 6 de agosto, e as alterações subsequentes, o SEGNAC ficou salvaguardado pelo artigo 1.º, n.º 5 *"A classificação como segredo de Estado não prejudica a aplicação do quadro normativo respeitante à segurança das matérias classificadas, abreviadamente designado por SEGNAC, que comporta os graus de classificação «Muito secreto», «Secreto», «Confidencial» e «Reservado»".* [123]

120 Segurança das Telecomunicações - SEGNAC 3, Capítulo 2, Ponto 2.
121 Iden Ponto 2.2.4
122 Segurança Informática – SEGNAC 4, Capítulo 2, Artigo 11.º
123 Por interpretação lógica devemos olhar para o SEGNAC como sendo relativo à Segurança de Matérias Classificadas – SEGNAC 1; Segurança Industrial, Tecnológica e de Investigação – SEGNAC 2; Segurança das Telecomunicações – SEGNAC 3; e Segurança Informática – SEGNAC 4.

SUBCAPÍTULO 3. O SISTEMA DE INFORMAÇÃO CRIMINAL

2.3.1 A VISÃO DA COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS

Em Portugal, em 2014, foi implementada uma Plataforma para o Intercâmbio de Investigação Criminal - PIIC. A Comissão Nacional de Proteção de Dados participou nas reuniões de preparação, tendo até alguma intervenção ativa em matérias de caráter técnico, proferindo oficialmente um parecer relativo ao seu funcionamento contemplando todas as garantias legais.[124]

Após os vários atentados em Paris, o Sistema de Informação Criminal na UE entrou em velocidade supersónica, em consonância com a restrição dos Direitos Constitucionalmente Garantidos, por exemplo, através da declaração do Estado de Emergência proferida por François Hollande, Presidente da França.

Em França, o Frenchelon é em tudo semelhante ao Echelon (ver em 5.3.1), mas usado, como o próprio nome indica, pelo Estado Francês. Porém, subsiste uma colossal diferenciação: a França não faz parte do Five-Eyes[125] (ver em 3.2.2). O ataque ao Charlie Hebdo falhou também por isso, pois todos os assassinos estavam envolvidos entre si e tinham ligações ao Iraque, aos Jiadistas e, durante o tempo de pena cumprido nas prisões, alguns dos elementos tiveram a mentoria de clérigos, ligados e associados ao radicalismo, e mais ainda: alguns tiveram instrução militar no Yemen.

Importante será lembrar que milhares de pessoas estão envolvidas nas mesmas redes e com ligações de décadas.[126]

Em França existe uma poderosa Intel, mas esta só pode supervisionar comportamentos de forma intrusiva se o cidadão em causa já tiver sido acusado de um qualquer crime.

O grande desafio para este tipo de Intel é identificar precocemente quais os indivíduos que merecem mais atenção, com base em informações muito escassas. Neste tipo de Intel a polícia local tem um papel preponderante na referenciação dos *"inimigos da comunidade"*.

Os líderes com poder de decisão e de intervenção têm noção da necessidade de fazerem Autópsias Digitais constantemente, e não só em certos momentos, tais como o permitido quando decretado Estado de Emergência.

---

124 Conforme consta no Relatório de Atividades da CNPD 2013-2014, p. 10.
125 "... Yemen was a US priority, whereas American officials left it to French. France, it should be remembered, is not a member of the US-led Five Eyes intelligence aliance." In BBC Europe Charlie Hebdo attack: A French intelligence failure?
126 "... more than 1,000 French nationals (...) have travelled to Iraq and Syria ..." In BBC Europe Charlie Hebdo attack: A French intelligence failure?

> *"The Assembly recognises the need for effective, targeted surveillance of suspected terrorists and other organised criminal groups. Such targeted surveillance can be an effective tool for law enforcement and crime prevention. At the same time, it notes that, according to independent reviews carried out in the United States, mass surveillance does not appear to have contributed to the prevention of terrorist attacks, contrary to earlier assertions made by senior intelligence officials. Instead, resources that might prevent attacks are diverted to mass surveillance, leaving potentially dangerous persons free to act."*[127]

Sobre esta temática, a CRP refere que os cidadãos têm o direito de acesso aos dados informatizados.[128] Aqui discute-se o reconhecimento de quem possui determinados dados e onde estão armazenados.

A proliferação da informatização administrativa e judicial generalizou-se. Assim sendo, deveria estar também generalizado o garante do direito de retificação, como também generalizada a possibilidade de saber a finalidade a que se destinam os dados. Se assim não for, a proteção dos dados escorregará a grande velocidade ao domínio da sociedade. A par disso, o *"... tratamento automatizado, conexão, transmissão e utilização ..."*, ainda que consagrado no n.º 2 do Art. 35.º da CRP, não garante a proteção suficiente, tal como, já anteriormente foi referido.[129]

Para além dos Juízes de Ratão, também a Europa diz que não consegue assegurar a proteção de dados, bem como a sua livre circulação *"... mas podem, em razão da dimensão e dos efeitos da ação, ser mais bem alcançados a nível da União. Esta pode tomar medidas, em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia."* [130]

Se os SI são considerados incapazes de controlar e fiscalizar o uso abusivo de dados, e a Europa não garante a proteção de dados, então, provavelmente, pior será um controlo e fiscalização num serviço administrativo, como por exemplo as repartições das finanças, ou outro.

---

127 Resolution 2045 (2015) *Mass Surveillance*, Dot 11. Parliamentary Assembly – Council of Europe.

128 *"Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei."* In CRP Artigo 35.º Utilização da informática, n.1.

129 Logo na apresentação do problema desta tese no ponto 1.2 os *"... Juízes de Ratão (...) não viram os SI como uma entidade capaz de supervisionar e controlar e justificaram a sua inconstitucionalidade por também considerarem que não seria garantido de forma suficiente o uso não abusivo da recolha de metadados."*

130 In, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//PT#BKMD-6

Assim sendo, não só surge na UE o supervisor *European Data Protection Supervisor*, mas também legislação relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Por este motivo foi transposto para o ordenamento jurídico português, entre outros, a Dir. n.º 95/46/CE, do PE e do Conselho, 24/10/95, traduzindo-se na Lei n.º 67/98, de 26 de Outubro. [131]

O Tratado de Nice – Tratado da União Europeia de 26 de fevereiro de 2001 — tinha como fins concluir os objetivos não alcançados no Conselho Europeu de Helsínquia de 1999, tais como, preparar os novos Estados para a adesão. Sendo que dois dos países candidatos eram mais populosos do que a media dos Estados-Membros à altura, era de esperar que o peso político dos países com menos população registasse um aumento considerável. Logo, o fenómeno das migrações teria de ser controlado.

Quanto ao conteúdo, foi desenhada *"... uma cooperação reforçada mais flexível, o controlo do respeito dos direitos e valores fundamentais no seio da UE e ainda um reforço do sistema judicial da UE."* [132]

Já em 2019 Portugal promulgou a Lei n.º 58/2019 de 8 de agosto que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Assegura também a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

131 *"1 - A criação e a manutenção de registos centrais relativos a pessoas suspeitas de atividades ilícitas, infrações penais, contraordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias só podem ser mantidas por serviços públicos com competência específica prevista na respetiva lei de organização e funcionamento, observando normas procedimentais e de proteção de dados previstas em diploma legal, com prévio parecer da CNPD; 2 - O tratamento de dados pessoais relativos a suspeitas de atividades ilícitas, infrações penais, contraordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias pode ser autorizado pela CNPD, observadas as normas de proteção de dados e de segurança da informação, quando tal tratamento for necessário à execução de finalidades legítimas do seu responsável, desde que não prevaleçam os direitos, liberdades e garantias do titular dos dados".* In Lei n.º 67/98, de 26 de Outubro Lei Da Proteção De Dados Pessoais Artigo 8º. Suspeitas de atividades ilícitas, infrações penais e contraordenações.

132 In http://www.europarl.europa.eu/atyourservice/pt/displayFtu.html?ftuId=FTU_1.1.4.html

2.3.2 OS PROGRAMAS DA INTERPOL E DA EUROPOL

A Globalização Informacional não está pensada para as imperfeições do sistema, mas sim para a execução de programas baseados na perfeição estrutural de base e para a consciencialização da utilização pura da informática.

No âmbito criminal, a Globalização trouxe outras preocupações que não a privacidade de dados ou a segurança dos mesmos, mas sim os fenómenos da criminalidade transfronteiriça, como o branqueamento de capitais, o tráfico de droga, o tráfico de armas, de materiais nucleares, o tráfico de materiais tóxicos e perigosos e o terrorismo.

Estes três últimos são verdadeiramente o maior dos problemas da criminologia, mas também outras preocupações como os Direitos Humanos estão constantemente em causa nos crimes transfronteiriços, tais como o tráfico de seres humanos com vista à exploração de mão-de-obra ilegal, ao trabalho escravo, à produção de material pornográfico, à prostituição, ao tráfico de órgãos, entre outros fins.

Assim sendo, temos de olhar para as fronteiras externas não como as fronteiras limitadas fisicamente pelos próprios países, mas sim bem mais distantes para assim *"Combater as causas que estão na base do terrorismo, prevenir extremismos religiosos ou políticos, faz-se também com instituições democráticas, um bom sistema judicial e uma sociedade ativa."* [133]

A Europol tem sido a grande impulsionadora de programas sobre segurança, tais como, a Academia Europeia de Polícia, a Estratégia Europeia de Luta Contra a Droga, e também o Sistema de Informação de Schengen – SISc, parte integrante do Sistema de Informação Criminal.

133 Palestra Globalização e Terrorismo: Segurança vs Justiça, proferida pelo Sr. Eurodeputado Dr. Carlos Coelho, na Universidade Lusíada do Porto, em 04 de abril de 2003.

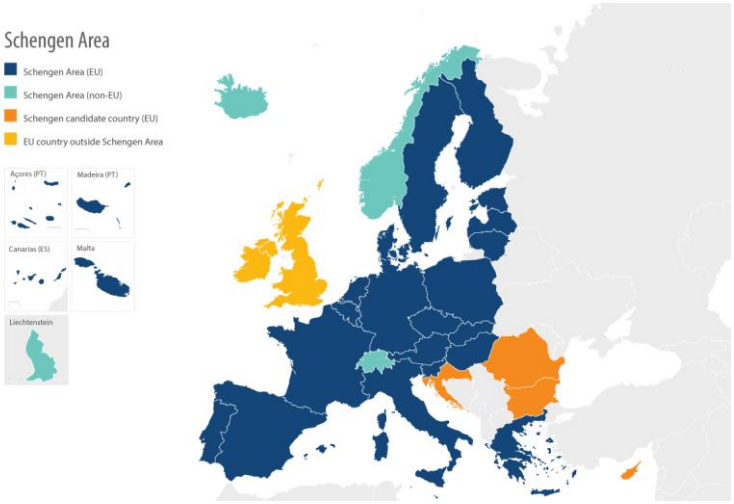

Figura 6 – Mapa da área Schengen[134]

As informações constantes no SISc são abastecidas pelos Estados membros do espaço Schengen e são trabalhadas pelas autoridades policiais e aduaneiras de outros Estados Schengen.

O SISc é a maior base de dados da Europa e tem como intuito a ordem pública e a segurança, atendendo à gestão do equilíbrio da livre circulação de pessoas e bens.

A Europol tem implementado, desde 25 de janeiro de 2016, o *European Counter Terrorism Centre*, maximizando o conceito operacional da troca de Intel, com especial enfoque no chamado Terrorismo Doméstico e com peculiar atenção ao Estado Islâmico, atendendo também ao evoluir do Cibercrime.

A Interpol, por seu lado, tem a sua estratégia atualmente programada para períodos de três anos, com quatro prioridades estratégicas:

> "1: Secure global police information system
> 2: 24/7 support to policing and law enforcement
> 3: Innovation, capacity building and research
> 4: Assisting in the identification of crimes and criminals" [135]

A primeira prioridade constitui-se em conectar e autorizar os trabalhos de Intel a que cada uma das instituições dizem respeito. Hoje existem 190 países, outras agências e parceiros estratégicos que têm acesso a dados.

134 In https://www.vistos.mne.pt/pt/vistos-schengen/informacao-geral/area-schengen
135 In https://www.interpol.int/About-INTERPOL/Priorities

Estas instituições terão também acesso, num futuro próximo, à mais-valia da interoperabilidade que se efetivará entre a Interpol e outros sistemas. A segunda prioridade consiste em assegurar um assistente permanente a operar o sistema, bem como responder de imediato em caso de crise de emergência. Neste sentido também se desenvolve, comanda e coordena a capacidade dos gabinetes de Intel das polícias do mundo inteiro. Já a terceira prioridade comporta a criação e desenvolvimento das capacidades técnicas dos analistas de informações, levada a cabo através do treino e assegurando a salvaguarda de riscos conexos. A última das prioridades consiste em assegurar a qualidade da base de dados e a melhor forma possível de consulta analítica. Entre outros dados contemplam-se *"... the identification, location and arrest of fugitives and cross-border criminals."* [136]

A Interpol vê a *Criminal Intelligence analysis* como uma componente essencial para a estratégia operacional da supervisão da Criminologia.[137] Esta estratégia passa por auxiliar os órgãos de polícia criminal, bem como os órgãos de decisão dos respetivos países. A par disso, a Interpol monitoriza também as ameaças.

O sistema analítico da Interpol divide-se nas seguintes componentes:[138]

> O apoio analítico operacional inclui:
>
> Identificação de ligações entre suspeitos e o seu envolvimento em crimes e actividades criminosas;
>
> Identificação das principais lacunas de investigação ou de informação;
>
> Preparação de perfis de criminosos conhecidos ou suspeitos.
>
> A análise estratégica inclui a identificação de:
>
> Modus operandi;
>
> Tendências e padrões de crime;
>
> Ameaças emergentes;
>
> O impacto potencial de factores externos como a tecnologia, demografia ou economia no crime.

136 Idem

137 "Criminologia é a ciência que estuda o fenômeno criminal, a vítima, as determinantes endógenas e exógenas, que isolada ou cumulativamente atuam sobre a pessoa e a conduta delinquente..." Gilzeda Santos sit. Fernandes Fernandes, in Dicionário de Criminologia, p. 58.

138 In https://www.interpol.int/INTERPOL-expertise/Criminal-Intelligence-analysis

Produtos analíticos:

Relatórios analíticos;

Avaliações de ameaças para regiões ou crimes específicos;

Avaliações de risco para um determinado evento;

Publicações de inteligência (boletins, relatórios mensais).

Após 2001, os Estados aumentaram o seu garante ao Princípio do Estado de Direito Democrático,[139] mesmo que para isso tenham de contemplar *"... a imposição de sanções aos Estados que apoiem o terrorismo, eficazes e graduáveis de acordo com a própria gravidade das suas atividades."* [140] — Ações contrárias aos Direitos, Liberdades e Garantias.

Cabe, assim, em última instância, aos Estados empregar as premissas oriundas do Conselho e das Comissões da EU [141], bem como socorrer-se dos meios de cooperação internacional dos Programas da Europol e da Interpol, ponderando o equilíbrio perfeito entre a Liberdade, a Segurança e a Justiça.

2.3.3 OS TRIBUNAIS E O MINISTÉRIO PÚBLICO

Hoje, mais do que nunca, existem vários tribunais e grande cooperação internacional, mas o mais relevante ao caso estudo é a exigência de julgamento em tribunais pela cooperação judiciária em estabelecimentos que impõem imperativos, o que leva por vezes a grandes erosões não só às Leis, mas também à CRP, a título de exemplo, a possibilidade de extradição de cidadãos portugueses.[142]

Os Tribunais Penais não têm uma diversidade na sua organização pelo simples facto de a criminalidade ser efetuada através do uso da informática, nem dispõem de uma forma processual penal diversa das restantes. *"Existem apenas algumas particularidades já assinaladas a propósito dos meios de obtenção de prova, extensivas aos casos de criminalidade altamente organizada."* [143], isto relativo às buscas e interceção de comunicações.

Quanto à informática, há dados cuja gestão escapa ao controlo das atividades de fiscalização, particularmente no que diz respeito ao COMINT (ver em 3.7).

---

139 "A República Portuguesa é um Estado de direito democrático, baseado na soberania popular, no pluralismo de expressão e organização política democráticas, no respeito e na garantia de efetivação dos direitos e liberdades fundamentais e na separação e interdependência de poderes, visando a realização da democracia económica, social e cultural e o aprofundamento da democracia participativa." Estado de direito democrático, Artigo 2.º da CRP.

140 In Informações e Segurança, p. 512.

141 Council of the European Union, 5855/15; European Parliament, 2015/2530; Council of the European Union, 12 February 2015, 56/15; Council of the European Union, 9951/15.

142 "A extradição de cidadãos portugueses do território nacional só é admitida, em condições de reciprocidade estabelecidas em convenção internacional, nos casos de terrorismo e de criminalidade internacional organizada, e desde que a ordem jurídica do Estado requisitante consagre garantias de um processo justo e equitativo." n.º3 do art. 33.º da CRP.

143 Segundo o Ex. Ministro da Administração Interna e Ex. Diretor-Geral do SIS, Professor Rui Pereira, em Os Desafios do Terrorismo: A Resposta Penal e o Sistema de Informações, In Segurança e Informações, p.511.

A estrutura jurídico, criminal e forense é em grande parte alimentada através das Tecnologias da Informação. Assim, o papel das comissões de fiscalização e dos magistrados do MP torna-se fulcral na credibilização do acesso, comando e controlo dos dados informáticos.

Portanto uma ação de interferência pelos órgãos de controlo transforma-se em elemento essencial para a reforma da política social aquando da observância de valores.

A cultura administrativa das Tecnologias da Informação prioritariza-se reflexamente dos interesses e da vontade política.

A título de análise, também os media têm um papel fundamental na interação com os tribunais, com o MP, com os OPC em asserção. Em última instância, os media são como que inspetores societários garantidores, pelo efeito que tem a divulgação noticiosa das atividades do Poder Judicial quanto à regência da informática. Os media são assim também mediadores no controlo da sociedade através da consciencialização dos vários acontecimentos.

Já o Ministério Público compreende, na área das Tecnologias da Informação, o Gabinete Cibercrime - GC que tem como intentos, entre outros, coordenar e formar magistrados do Ministério Público, interagir com o setor privado e com os órgãos de polícia criminal, e o Departamento Central de Investigação e Ação Penal - DCIAP que dirige a luta contra a criminalidade violenta, altamente organizada ou de especial complexidade, da seguinte forma:

Prevenção criminal

Investigação criminal

Coordenação nacional

Cooperação internacional

Compete ainda ao DCIAP garantir todas as diligências rogadas, por vezes, até ao DCIAP são impostas obstruções intransigentes à investigação.[144]

2.3.4 A PROCURADORIA GERAL DA REPÚBLICA E A POLÍCIA JUDICIÁRIA

A Procuradoria Geral da República que tem sobre a sua alçada, entre outros, o GC e o DCIAP tem também a seu cargo.

144 Em fase de julgamento, do designado 'Processo das Secretas', relacionada com escutas telefónicas, durante o inquérito foi extraída uma certidão que envolvia os Serviços de Informações da República Portuguesa em eventuais crimes de abuso de poder e de instrumentos de escuta telefónica, pela suposta adoção dos Serviços de Informação da República Portuguesa (SIRP) de procedimentos para interceções telefónicas de telefones fixos e móveis, registo de som ambiente, nomeadamente conversações, bem como interceção de e-mails, vigilâncias áudio e realização de fotografias de terceiros fora do espaço público.'', mas o primeiro-ministro, António Costa, não levantou o Segredo de Estado, e assim, face a este indeferimento, o Ministério Público viu-se impossibilitado de realizar outras diligências investigatórias, uma vez que, necessariamente, viriam a colidir com aquela classificação''. Consultado em 27 de setembro de 2017 In http://rr.sapo.pt/noticia/94292/costa_nao_levanta_segredo_de_estado_e_caso_secretas_acaba_arquivado

"... a cooperação judiciária internacional em matéria penal e de apostila (...) também entidade fiscalizadora do regime jurídico de incompatibilidades e impedimentos de titulares de altos cargos públicos, estando aí sedeada a Comissão de Fiscalização de Dados do Sistema de Informações da República Portuguesa." [145]

Não podemos falar de cooperação judiciária internacional sem falar no Sistema de Informação Criminal, nem podemos falar da Comissão de Fiscalização sem relevar o Regime Jurídico das Ações Encobertas – RJAE, levado também a cabo através das Tecnologias da Informação. Assim sendo, começaremos por aprofundar o RJAE, e a abertura que este dá a todos os Serviços que trabalham Informações. Vejamos pois o objeto deste regime, logo no ponto 2. do Artigo 1.º

"Consideram-se ações encobertas aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro atuando sob o controlo da Polícia Judiciária para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade."

Então o conceito será: qualquer elemento terceiro que atue sob o controlo da Polícia Judiciária poderá fazer Ações Encobertas.[146]

As orientações da Procuradoria Geral fortalecem ainda mais este conceito.

"As ações encobertas são sujeitas a controlo jurisdicional e têm um regime e tramitação legal específicos, que só consentem a respetiva abertura até ao termo do inquérito ou da investigação." [147]

145 In http://www.ministeriopublico.pt/pagina/procuradoria-geral-da-republica

146 A Ação Encoberta enquanto objeto Considera *"... ações encobertas aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro atuando sob o controlo da Polícia Judiciária para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade."* N.º 2 do Art. 1º Lei n.º 101/2001, de 25 de Agosto Ações Encobertas (versão atualizada). Já a Lei n.º 144/99, de 31 de agosto Lei da Cooperação Judiciária Internacional em Matéria Penal (versão atualizada) no seu n.º 1 Art. 160º - B Ações Encobertas refere que *"1 - Os funcionários de investigação criminal de outros Estados podem desenvolver acções encobertas em Portugal, com estatuto idêntico ao dos funcionários de investigação criminal portugueses e nos demais termos da legislação aplicável; 2 - A atuação referida no número anterior depende de pedido baseado em acordo, tratado ou convenção internacional e da observância do princípio da reciprocidade; 3 - A autoridade judicial competente para a autorização é o juiz do Tribunal Central de Instrução Criminal, sob proposta do magistrado do Ministério Público junto do Departamento Central de Investigação e Acão Penal (DCIAP)."*

147 Despacho n.º 3/2008 da PGDL e a Circular 6/2008 da PGDC.

Quanto à jurisprudência da pesquisa efetuada no que respeita às Ações Encobertas, estas só falam em agentes de Órgãos de Polícia Criminal e nunca em "terceiro". A acrescentar a tudo isto é de referir que um elemento dos Serviços de Informações quando esteja encoberto fisicamente pelas Tecnologias da Informação dificilmente poderá por si só ser apontado como agente provocador *"... As acções encobertas são um meio de investigação a usar com parcimónia e o modo como se desenvolvem deve ser objeto de aprofundado escrutínio...".* [148]

Ainda relativo às Ações Encobertas, *"os agentes informadores e infiltrados não participam na prática do crime, a sua atividade não é constitutiva do crime, mas apenas informativa, e, por isso, é de admitir que, no limite, se possa recorrer a estes meios de investigação".* [149]

Assim sendo, os elementos dos Serviços de Informações, quando atuarem como "terceiro", poderão efetuar ações encobertas aquando de uma operação conjunta entre os Serviços de Informações e qualquer Órgão de Polícia Criminal quando este último seja a entidade coordenadora.

Segundo a Mestre Ana Raquel, existe hoje a seguinte concertação:

> "... consagração de modernas técnicas de investigação criminal no domínio da cooperação. A constituição de equipas de investigação conjuntas, interceções de telecomunicações, investigações encobertas ou entregas vigiadas, são exemplos de métodos de combate à criminalidade organizada transfronteiriça." [150]

2.3.5 OS ÓRGÃOS DE POLÍCIA CRIMINAL

Segundo o Ministério Público, mais propriamente a Procuradoria Distrital do Porto, órgãos de polícia criminal são os seguintes:

> *"Entidades que cooperam com as autoridades judiciárias na investigação criminal, desenvolvendo atos de investigação em inquérito, concretamente solicitados ou com autonomia tática e técnica do próprio órgão. Os mais conhecidos são: Polícia Judiciária (PJ), Polícia de Segurança Pública (PSP),*

148Acórdão da Relação de Lisboa de 22-03-2011, Proc. 182/09.6JELSB.L1-5.
149 Sit. Germano Marques da Silva, in Acórdão do Tribunal da Relação do Porto, Proc. 8292/12.6TDPRT.P1.
150 In Escutas Telefónicas Regime Processual Penal, p. 62.

Guarda Nacional Republicana (GNR) e Serviço de Estrangeiros e Fronteiras (SEF).” [151]

Hoje em dia, grande parte dos Órgãos de Polícia Criminal têm divisões/núcleos de investigação criminal. Por essa razão, todos estes podem ter agentes portugueses ou estrangeiros e “terceiros” encobertos ou infiltrados.

As ações encobertas são admissíveis no âmbito da prevenção e repressão de alguns crimes.[152]

> *“O artigo 19.º da LC [Lei do Cibercrime] prevê a admissibilidade de recurso a ações encobertas no decurso de inquérito relativo a crimes previstos na presente lei, ou a crimes cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras, bem como os crimes contra obras protegidas por direito de autor...”*[153]

Nas ações encobertas não podemos esquecer a excecionalidade deste método para a produção de prova relativa à Criminalidade Grave.

---

151 Do que nos foi dado a conhecer não existe uma lista Oficial que diga quem são e quantos os Órgãos de Polícia Criminal existentes em Portugal, contabilizado por nós ultrapassa os (18) dezoito, Consultado em 22 de janeiro de 2017 in https://www.pgdporto.pt/proc-web/faq.jsf?ctxId=85&subCtxId=93&faqId=454&show=&offset=

152 *“a) Homicídio voluntário, desde que o agente não seja conhecido; b) Contra a liberdade e contra a autodeterminação sexual a que corresponda, em abstrato, pena superior a 5 anos de prisão, desde que o agente não seja conhecido, ou sempre que sejam expressamente referidos ofendidos menores de 16 anos ou outros incapazes; c) Relativos ao tráfico e viciação de veículos furtados ou roubados; d) Escravidão, sequestro e rapto ou tomada de reféns; e) Tráfico de pessoas; f) Organizações terroristas, terrorismo, terrorismo internacional e financiamento do terrorismo; g) Captura ou atentado à segurança de transporte por ar, água, caminho-de-ferro ou rodovia a que corresponda, em abstrato, pena igual ou superior a 8 anos de prisão; h) Executados com bombas, granadas, matérias ou engenhos explosivos, armas de fogo e objetos armadilhados, armas nucleares, químicas ou radioativas; i) Roubo em instituições de crédito, repartições da Fazenda Pública e correios; j) Associações criminosas; l) Relativos ao tráfico de estupefacientes e de substâncias psicotrópicas; m) Branqueamento de capitais, outros bens ou produtos; n) Corrupção, peculato e participação económica em negócio e tráfico de influências; o) Fraude na obtenção ou desvio de subsídio ou subvenção; p) Infrações económico-financeiras cometidas de forma organizada ou com recurso à tecnologia informática; q) Infrações económico-financeiras de dimensão internacional ou transnacional; r) Contrafação de moeda, títulos de créditos, valores selados, selos e outros valores equiparados ou a respetiva passagem; s) Relativos ao mercado de valores mobiliários.”*

153 O Professor Pedro Dias Venâncio critica ainda o facto de não estarem contemplados os crimes relativos à proteção das medidas de caráter tecnológico e das informações para a gestão eletrónica, in *Lei do Cibercrime Anotada e Comentada*, p. 122.

Assim sendo, as ações encobertas estão subsumidas no âmbito das escutas, nomeadamente na fase de inquérito, como um meio de obtenção de prova consagrada no nosso Código do Processo Penal. As escutas são só um instrumento para a obtenção de prova, mas terão sempre de obedecer às formalidades das operações segundo o Código do Processo Penal no seu artigo 188.º. [154]

A Constituição não concebe organizações terroristas ou associações armadas no ordenamento Português, mas garante a Liberdade de Consciência, de Religião e de Culto.[155]

O CPP, no n. 2 e 3 do Art. 135º, prevê a possibilidade de quebra do segredo profissional.[156] No que respeita à quebra de segredo, o disposto no n. 5 do Art. 135º não permite a sua aplicabilidade à religião. Daí que uma organização criminosa camuflada e albergada numa instituição religiosa terá logo à partida a proteção do Código do Processo Penal.

154 *"1 - O órgão de polícia criminal que efetuar a interceção e a gravação a que se refere o artigo anterior lavra o correspondente auto e elabora relatório no qual indica as passagens relevantes para a prova, descreve de modo sucinto o respetivo conteúdo e explica o seu alcance para a descoberta da verdade; 2 - O disposto no número anterior não impede que o órgão de polícia criminal que proceder à investigação tome previamente conhecimento do conteúdo da comunicação intercetada a fim de poder praticar os atos cautelares necessários e urgentes para assegurar os meios de prova; 3 - O órgão de polícia criminal referido no n.º 1 leva ao conhecimento do Ministério Público, de 15 em 15 dias a partir do início da primeira interceção efetuada no processo, os correspondentes suportes técnicos, bem como os respetivos autos e relatórios; 4 - O Ministério Público leva ao conhecimento do juiz os elementos referidos no número anterior no prazo máximo de quarenta e oito hora."*

155 *"... 3. Ninguém pode ser perguntado por qualquer autoridade acerca das convicções ou prática religiosa (...) 5. É garantida (...) a utilização de meios de comunicação social próprios para o prosseguimento das suas atividades ..."* do Art. 41.º da CRP.

156 *"3 – O tribunal superior àquele onde o incidente tiver suscitado, ou no caso de o incidente ter sido suscitado perante o Supremo Tribunal de Justiça, o pleno das secções criminais, pode decidir da prestação de testemunho com quebra do segredo profissional sempre que esta se mostre justificada, segundo o princípio da prevalência do interesse preponderante, nomeadamente tendo em conta a imprescindibilidade do depoimento para a descoberta da verdade, a gravidade do crime e a necessidade de proteção de bens jurídicos. A intervenção é suscitada pelo juiz, oficiosamente ou a requerimento."*

SUBCAPÍTULO 4. OPERADORAS E COMUNICAÇÕES

As operadoras de telecomunicações e os fornecedores do serviço universal desempenham um papel fundamental na partilha de informações relevantes para o Intelligence. Assim sendo, resta-nos esgrimir factos e argumentos que sustentem a parceria jurídica entre as empresas privadas e os órgãos formais de controlo social na difusão de matérias de âmbito privado e pessoal.

Em Portugal, as operadoras de telecomunicações têm um papel fulcral na investigação criminal, pois, ao contrário de outros países, como por exemplo os Estados Unidos da América e o Reino Unido, Portugal tem vindo a evoluir nas respetivas legislações para obrigar as operadoras e distribuidoras de serviço universal a fornecerem informações acerca dos seus clientes e por vezes atribuírem perfis para o uso das suas redes e bases de dados. As operadoras de telecomunicações nos EUA fornecem assim os dados por si só às instâncias de controlo, como por exemplo à CIA e ao FBI.[157] Os Estados Unidos chegam ao ponto de criar um grupo chamado Team Telecom dos quais fazem parte *"... membros do FBI, dos Departamento de Defesa e de Justiça e da Segurança Interna.".* [158] Em Portugal, instituições como o SIRP (SIS, SIED) ficam distantes desses dados, não obstante do entendimento do Parlamento Europeu.

> *"A Assembleia Parlamentar está profundamente preocupada com as práticas de vigilância em massa que têm sido divulgadas desde Junho de 2013 por jornalistas a quem um antigo contratante da Agência Nacional de Segurança dos Estados Unidos (NSA), o Sr. Edward Snowden, confiou uma grande quantidade de dados ultra-secretos que estabelecem a existência de vigilância em massa e práticas de intrusão em larga escala até agora desconhecidas do público em geral e mesmo da maioria dos decisores políticos.*
>
> *2. As informações divulgadas até agora nos arquivos da Snowden desencadearam um enorme debate mundial sobre a vigilância em massa pelos serviços de inteligência dos Estados Unidos e de outros países e a potencial falta de regulamentação legal e proteção técnica adequada a nível nacional e internacional, e/ou a sua efetiva aplicação.*

157 Aqui refere-se a adoção do Amendment Act por parte do FISA, onde se passou a conceder uma *"autorização de recolha global"*, in O Caso Snowden, p. 184.
158 In O Caso Snowden, p. 173.

3. As divulgações têm fornecido provas convincentes da existência de sistemas de longo alcance e tecnologicamente avançados postos em prática pelos serviços de inteligência dos Estados Unidos e seus parceiros em certos Estados membros do Conselho da Europa para coletar, armazenar e analisar dados de comunicação, incluindo conteúdo, localização e outros metadados, em larga escala, bem como medidas de vigilância direcionada que englobam inúmeras pessoas contra as quais não há motivo para suspeitas de qualquer ato ilícito". [159]

Independentemente da Recomendação do Conselho Europeu, existe um grande esforço por parte do Governo Português na elaboração de vários Projetos-Lei no sentido da autorização jurídica do acesso aos dados de telemóveis e contas bancárias por parte dos Serviços de Informações. O Conselho Superior da Magistratura – CSM tem chumbado sucessivamente a possibilidade de os Serviços de Informações terem acesso a esses dados. O CSM utiliza a expressão "inconstitucionalidade material", mais ainda, o CSM recorda um parecer de 2015 do Tribunal Constitucional que chumbou conteúdo muito idêntico, referindo que <<... a Constituição da República proíbe a "ingerência" das autoridades públicas nas comunicações "salvo nos casos previstos na lei em matéria de processo criminal">>.[160]

2.4.1 VERIZON, AT&T E SPRINT

Não se pode falar de operadoras nem de fornecedores de serviço universal sem se falar na Verizon, pois esta é a maior operadora de telecomunicações do mundo, contando, em 2013, com mais de 113 milhões de clientes.

Posteriormente, vamos verificar, no subcapítulo Recolha de Dados, que existe entendimento sobre a legalidade do fornecimento de metadados. O fornecimento dos metadados aos vários órgãos tem proveniência nas operadoras, assim sendo, também a NSA reúne todos os dias os registos telefónicos de milhões de assinantes da Verizon.[161] Edward Felton provou, através de documentos, que a NSA recolhia (nas três grandes operadoras referidas no subtítulo) *"... todos os metadados das chamadas telefónicas que entrassem, saíssem ou passassem pelos Estados Unidos."*[162]. Em 2011, só

159 Recommendation 2067 (2015) of The Parliamentary Assembly of the Council of Europe, In http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0yMTY5NCZsYW5nPUV O&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTIxNjk0

160 In Diário de Notícias de 19 de maio de 2017, Consultado em 30 de setembro de 2017 in https://www.dn.pt/portugal/interior/juizes-chumbam-acesso-das-secretas-a-dados-dos-telemoveis-8487444.html

161 NSA collecting phone records of millions of Verizon customers, In The Guardian, consultado em 19 de janeiro de 2017.

162 In O Caso Snowden, p. 188.

em Mainway, uma das principais bases de dados da NSA, eram recolhidos 1.1 mil milhões de gravações diárias com a ajuda da AT&T.[163]

Também a Sprint, durante a administração do Presidente dos EUA Barack Obama, gravava biliões de chamadas através de um programa de recolha de dados que, posteriormente, eram trabalhados pela NSA com o objetivo de Contra-Terrorismo. A Sprint, em 2010, era a terceira maior empresa fornecedora de serviço universal nos EUA.[164]

2.4.2 ENISA

A *European Union Agency for Network and Information Security* – ENISA é a grande coordenadora na UE entre as várias estratégias da gestão do ciberespaço. Esta entidade tem como função: o garante da segurança da informação das redes de comunicações na UE, a difusão de normas e regulamentos das melhores práticas a serem adotadas, quer pelos utilizadores quer pelas instituições público/privadas.

Toda esta gestão se traduz no melhoramento da qualidade dos serviços na aceleração das transações económicas, tais como, o e-commerce ou a disponibilidade permanente das redes móveis. A par disso, a ENISA também trabalha em conjunto com os diferentes Estados para aproximar as abordagens dos Estados às Tecnologias da Informação de forma semelhante entre eles.

A ENISA tem a seu cargo as seguintes atividades: Implementação de políticas; Recomendações; Cursos de formação. Esta última atividade traz aos formandos a possibilidade de se tornarem especialistas através da frequência dos seguintes cursos:[165]

- Análise de artefatos
- Ameaças Móveis e Tratamento de Incidentes
- Forense digital - Identificação e tratamento de provas eletrônicas
- Triagem e tratamento básico de incidentes - Teste do procedimento de tratamento de incidentes

A frequência destes cursos só está ao alcance de elementos que trabalhem sob a alçada do governo ou no sector público.

163 Idem, p. 193.
164 Ellen Nakashima, U.S. revealed secret legal basis for NSA program to Sprint, declassified files show, The Washington Post, Consultado em 27 de novembro de 2017, In https://www.washingtonpost.com/world/national-security/us-revealed-secret-legal-basis-for-nsa-program-to-sprint-documents-show/2014/05/14/f593612a-ce28-11e3-937f-d3026234b51c_story.html?utm_term=.cc12b679d948
165 In https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/training-courses

Uma das grandes preocupações da ENISA é a computação/informação através do uso da Cloud, assim a ENISA forma também analistas para integrar, entre outras, as equipas de Intervenção Imediata, que trabalham ininterruptamente e que já estão implementada em vários Estados da UE.

2.4.3 ANACOM

Em Portugal, a Autoridade Nacional de Comunicações (ANACOM) é a autoridade reguladora nacional (ARN) no âmbito das comunicações, para efeitos do disposto no direito da União Europeia e na legislação nacional, e sucede nas atribuições e competências da Comissão de Planeamento de Emergência das Comunicações. Esta Autoridade é funcionalmente independente, ainda que sob a tutela governamental.

A ANACOM regula todas as comunicações eletrónicas, entre outras, as radiocomunicações, eletromagnéticas e por satélite. [166]

A alusão ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas está na Lei n.º 46/2012, de 29 de agosto que, entre outros, aborda a garantia da inviolabilidade das comunicações eletrónicas e das proibições.[167]

Esta lei transpõe a Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009, que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas e o Regulamento (CE) n. 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor.

O acesso à informação armazenada, pela Lei n.º 46/2012, de 29 de agosto, impõe que só seja possível o seu acesso com o consentimento do assinante do Serviço Universal ou pela legitimidade da Lei de Proteção de Dados Pessoais.[168]

Quanto aos Dados de Tráfego, dependendo da necessidade destes, a lei refere explicitamente a sua eliminação ou o seu anonimato pelo n.º 1 do Art. 6.º da Lei n.º 46/2012, de 29 de agosto.

---

166 *"A ANACOM tem por missão a regulação do setor das comunicações, incluindo as comunicações eletrónicas e postais e, sem prejuízo da sua natureza, a coadjuvação ao Governo no domínio das comunicações, nos termos dos presentes estatutos e da lei.",* n.º 2 do Art. 1º do Estatutos da Autoridade Nacional de Comunicações.

167 *"É proibida a escuta, a instalação de dispositivos de escuta, o armazenamento ou outros meios de interceção ou vigilância de comunicações e dos respetivos dados de tráfego por terceiros sem o consentimento prévio e expresso dos utilizadores, com exceção dos casos previstos na lei."* N.º 2 do Art. 4º da Lei n.º 46/2012, de 29 de agosto.

168 *"1 - O armazenamento de informações e a possibilidade de acesso à informação armazenada no equipamento terminal de um assinante ou utilizador apenas são permitidos se estes tiverem dado o seu consentimento prévio, com base em informações claras e completas nos termos da Lei de Proteção de Dados Pessoais, nomeadamente quanto aos objetivos do processamento."* Artigo 5.º Armazenamento e acesso à informação da Lei 46/2012, de 29 de agosto.

No que se refere à limitação de tratamento de Dados de Tráfego, a presente Lei divide esta especificidade em duas partes: a primeira diz respeito aos Colaboradores e a segunda aos Tribunais/Autoridades.[169]

Quanto a Dados de Localização, o seu tratamento só poderá ser sob a forma de anonimato pelo n.º 1 do artigo 7.º da presente lei. A única exceção só se verifica no n.º 2 do mesmo artigo em chamadas de emergência e para efeitos de resposta a essas chamadas.

Se a Lei n.º 46/2012, de 29 de agosto tinha como grande finalidade estabelecer a correlação entre as empresas prestadoras de serviço universal e os seus assinantes, já a Lei 32/2008, que transpõe a Diretiva da Retenção de Dados relativa à conservação de dados das comunicações eletrónicas, está mais vocacionada para a relação entre utilizadores e as autoridades com o objetivo principal de *"... investigação, deteção e repressão..."* de crimes graves.[170]

No Ordenamento Jurídico Português e Internacional, existe uma tendência para desresponsabilizar o fornecedor do serviço universal, como coautor isentando-o da parte civil e criminal dos danos causados pelo assinante/utilizador.

Assim sendo, só existe interesse público no conhecimento efetivo de quem produziu a ilicitude.

A Lei n.º 5/04, de 10 de fevereiro — Lei das Comunicações Eletrónicas versou a especificação das definições e do seu entendimento (ver em Anexos - Definições). Estas definições tornam-se muito importantes na utilização das definições para fins jurídicos.

Portanto, no que respeita à responsabilidade do Estado, esta tem sempre lugar, independentemente da autonomia, do tipo de informação transferida, da interconexão ou interligação entre redes públicas/privadas de telecomunicações. Também a Lei n.º 91/97, de 01 de agosto — Lei de Bases das Telecomunicações trata da atribuir responsabilidades de Tutela, no seu artigo 5.º trata da Tutela das telecomunicações.[171]

---

169 *"6 - O tratamento dos dados de tráfego deve ser limitado aos trabalhadores e colaboradores das empresas que oferecem redes e ou serviços de comunicações eletrónicas (...) restringindo-se ao necessário para efeitos das referidas atividades. 7 - O disposto nos números anteriores não prejudica o direito de os tribunais e as demais autoridades competentes obterem informações relativas aos dados de tráfego..."* Artigo 6º da Lei 46/2012 de 29 de agosto.

170 *"1 - A conservação e a transmissão dos dados têm por finalidade exclusiva a investigação, deteção e repressão de crimes graves por parte das autoridades competentes. 2 - A transmissão dos dados às autoridades competentes só pode ser ordenada ou autorizada por despacho fundamentado do juiz, nos termos do artigo 9.º 3 - Os ficheiros destinados à conservação de dados no âmbito da presente lei têm que, obrigatoriamente, estar separados de quaisquer outros ficheiros para outros fins. 4 - O titular dos dados não pode opor-se à respetiva conservação e transmissão."* Artigo 3.º Finalidade do tratamento da Lei 32/2008 de 17 de julho.

171 *"1 - Compete ao Estado a definição das linhas estratégicas e das políticas gerais, a aprovação da legislação aplicável ao setor, a superintendência e a fiscalização das telecomunicações e da atividade dos operadores de telecomunicações. 2 — Na prossecução das atribuições do Estado, compete ao Instituto das Comunicações de Portugal, enquanto entidade reguladora do sector e sem prejuízo de outras atribuições cometidas por lei: a) A gestão do*

Com toda esta conjuntura e conexões legais conduz-se a uma Hierarquia Constitucional pelo Interesse Público, assim, teremos de harmonizar a ponderação de valores, analisar limites e definir intervenções, que estimulem o papel da justiça.

> "Com efeito, a compatibilização do desenvolvimento das novas Tecnologias da Informação com respeito pelos direitos fundamentais dos cidadãos é uma tarefa tanto mais complexa quanto é certo que se encontram tantas vezes em conflito interesses, direitos e deveres de indiscutível relevância e, por vezes, de similar dignidade jurídico-constitucional.". [172]

2.4.4 VODAFONE, TMN, MEO/PT E NOS

As operadoras em Portugal são impelidas por Lei a conservar a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas colectivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, detecção e repressão de crimes graves por parte das autoridades competentes.[173]

A conservação de dados que revelem o conteúdo das comunicações é permitida ainda que muito limitada.[174]

A Lei 38/2008 categoriza os dados a conservar, entre eles, destacamos, identificar a fonte e o destino de uma comunicação, bem como, data, a hora e a duração da mesma.

As operadoras tem obrigatoriamente que preservar esses dados durante um ano após a comunicação.

Estes dados só são transmitidos pelas operadoras às entidades competentes após ser autorizada, por despacho fundamentado do juiz de instrução.

---

espectro radioelétrico e das posições orbitais; b) A normalização, aprovação e homologação dos materiais e equipamentos de telecomunicações, de acordo com a legislação aplicável; c) A fiscalização das telecomunicações e do cumprimento das respetivas disposições legais e regulamentares relativas à atividade, bem como a aplicação das correspondentes sanções; d) A definição das condições de interligação de redes e serviços de telecomunicações de uso público explorados por operadores com posição significativa nos mercados." Artigo 5º - Tutela das Telecomunicações da Lei n.º 91/97, de 01 de agosto.

172 In Direito da Informática, p. 147.

173 Lei 38/2008 de 17 de julho.

174 *"2 – A conservação de daos que revelem o conteúdo das comunicações é proibido, sem prejuízo do disposto na Lei n.º 41/2004, de 18 de agosto, e na legislação processual penal relativamente à intercepção e gravação de comunicações."* Artigo 1.º da Lei 38/2008 de 17 de julho.

CAPÍTULO 3. AS PRÁTICAS DOS SISTEMAS DE INFORMAÇÃO E OS DIREITOS LIBERDADES E GARANTIAS

3.1 TEORIA E PRÁTICA DOS SISTEMAS DE INFORMAÇÃO

No estudo da estratégia operacional há que reter primordialmente dois aspetos: primeiro, a prospetiva estratégica e, segundo, as ameaças e desafios.

A prospetiva inclui um estudo das causas técnicas, científicas, económicas e sociais que aceleram a evolução do mundo moderno e a previsão das situações que poderiam derivar das suas influências conjugadas, analisando proativamente todo o seu processo, bem como a sucessão de acontecimentos.

Quanto às ameaças, o estudo incide sobre a vitalidade dos seus desafios, evoluindo para a conjuntura nacional e internacional como um só.

Assim, a gestão de um Estado passa muitas vezes pela elaboração de um plano estratégico, ao caso, o plano para os Sistemas e Serviços de Informações (SSI), tendo em conta a noção de Direitos Fundamentais como princípio basilar da estrutura do plano operacional e geopolítico.

Para encetar a estratégia operacional, começamos por reportar que os membros da Assembleia da República estão no SSI representados pelos membros do Conselho de Fiscalização (CF), que têm sobre a sua alçada o controlo do SIRP nos termos do art. 8.º, n.º 1, da Lei-Quadro do Sistema de Informações da República Portuguesa (LQSIRP), esse CF tem como intuito acompanhar e fiscalizar a atividade do Sr. Secretário-Geral dos Serviços de Informações e do CISMIL nos termos do art. 34.º da mesma Lei-quadro.[175]

A par do CF, existe também um Conselho Consultivo (CC) do SIRP, que é composto por: diretor-geral de Política de Defesa Nacional do Ministério da Defesa Nacional, diretor-geral de Política Externa do Ministério dos Negócios Estrangeiros, responsável pelo organismo de informações militares, comandante-geral da Guarda Nacional Republicana, diretor nacional da Polícia de Segurança Pública, diretor nacional da Polícia Judiciária e pelo diretor-geral do Serviço de Estrangeiros e Fronteiras. Fazem parte também do CC do SIRP os diretores e os diretores-adjuntos do SIS e do SIED.

175 *"... são aplicáveis às atividades de produção de informações das Forças Armadas."* os objetivos, as finalidades, o limite das atividades dos serviços de informações, as delimitações do âmbito de atuação, o acesso a dados e informações, impostos pela Lei-Quadro do Sistema de Informações da República Portuguesa – Lei n.º 30/84 de 5 de setembro.

Estes são os principais mediadores oficiais das Informações e do apoio à tomada de decisão do Estado, mas os fluxos e as informações dentro de todos os Estados são influenciados (manipulados) muitas vezes pela sociedade, e muitas respostas importante são oriundas também desta.

Os fluxos de informações podem vir através do grupo, isto é, das elites económicas, dos *mass media* ou através dos líderes de opinião (comentadores e cronistas dos media), sem esquecer a Religião e, em alguns locais do mundo, as Castas.

O Estado Português delega funções e competências nos Srs. Diretores-Geral da rede de informações: (SIRP, SIS, SIED, CISMIL e Ministérios) fazendo com que estes, por sua vez, não possam ficar à espera de uma qualquer solicitação por parte dos órgãos de soberania, muito pelo contrário, estes, por vezes, têm de tomar a iniciativa própria, o mais oportunamente possível, que vise o melhoramento e funcionamento (desenvolvimento) do Estado e da sua população.

Os desconhecedores dos serviços do Intel muitas das vezes tratam a rede de informações por serviços secretos, o que é por si só é uma incongruência, pois o que seria da partilha de informações se existisse na realidade um secretismo, e o que seria feito dos fiscalizadores (CF) que são escolhidos pelos membros da AR, e o que seria da nossa economia se os empresários não tomassem contra medidas para prevenir a espionagem industrial?

Assim, por tudo o que foi sendo enumerado, discrimina-se o que aparentam ser os três princípios obrigatórios para uma boa estratégia no dirigismo de qualquer entidade: Cooperação, Coordenação e Comunicação. Se o primeiro traduz o trabalho em simultâneo das instituições, já o segundo princípio serve para planear, organizar e orientar o trabalho das instituições para que não haja duplicação de tarefas, nem as possíveis contendas. Por último, nada disto poderá funcionar sem o princípio da comunicação que é a garantia de que todos os elementos têm conhecimento dos objetivos e das funções a desempenhar.

Quando verificados os três princípios, poder-se-á dizer que existe uma verdadeira organização no sentido mais estrito da palavra.

Só existe um verdadeiro comando e controlo se à Intel for dada a devida importância. Quer em alvos de cariz nacional ou transnacional, devem então os gestores estar preparados para um atentado de qualquer tipo: económico, informático, ou das já famosas armas de destruição massiva, entre outros.

Trocar informações entre Estados aliados é fulcral na direção e gestão de um Estado, dominar a ideologia e a especificidade das Informações é ter uma verdadeira política estratégica, de reconhecimento, podendo, assim, desmontar-se todos os enigmas a jusante do ato.

O único conceito que não pode ser desmontado é quando um Estado vê outro Estado preso nas suas próprias paranoias.[176]

Para gerir um cenário que englobe atividades de grupos de terroristas, basta gerir e seguir todos os elementos logísticos necessários à prática do crime em preparação. Pois *"...prevention is so intelligence intensive".*[177] Traduz-se isto então em que o trabalho feito a montante é muito mais difícil, pois aí teremos de encontrar a peça que falta no desconhecido, o que é uma atividade muito morosa e, por vezes, chega a ser necessário organizar reuniões de grupos de pensamento estratégico, fazendo a posteriori suposições conjuntas. Sendo que, por vezes, aparecerá a completa ausência de prova, o que não significa que não existam em processo os atos preparatórios.

Assim, por vezes, os operacionais têm de recorrer ao seu instinto e às dicas no período da efetivação do trabalho de campo, e este tipo de input só se consegue alcançar com este tipo de sentimentos (trabalho intelectual), mesmo não tendo qualquer caráter científico por detrás deste input, e muito menos pode esse instinto ser verificável dentro de um programa tecnológico.

A posteriori, as tarefas, os materiais, os equipamentos e as facilidades farão parte de um processo extensivo e de avaliação. Pela sua importância, repare-se no terrorismo biológico, não será necessariamente obrigatório o controlo do grupo terrorista? Para isso, basta monitorizar a coleção de materiais requisitados por esse grupo para se chegar a uma avaliação final. Como refere Treverton (2007), existem três características a observar: Importância, Raridade e Detetabilidade. Este tipo de abordagem traz um conjunto de probabilidades.

A título de exemplo: *"O terrorista Anders Behring Breivik, que matou 77 pessoas em ataques na Noruega em 22 de Julho, comprou no site de leilões eBay o enxofre e outros materiais que usou para fazer os explosivos usados nos ataques... "*[178] Sabendo que um dos produtos utilizados no ataque foi o enxofre em pó (massa atómica de 32,066 e que serve para sulfatar as videiras), uma das respostas jurídicas do Estado Português em relação ao ataque converge com a Lei n. 26/2013, que regula as atividades de distribuição, venda e aplicação de produtos fitofarmacêuticos para uso profissional e de adjuvantes de produtos fitofarmacêuticos e define os procedimentos de monitorização à utilização dos produtos fitofarmacêuticos.[179]

176 Treverton retratando o pensamento de Moscovo no tempo da guerra fria em *Threat Converge and intelligence*, p.154.
177 Id, p. 155.
178 www.tvi24.iol.pt, Consultado em 28 de novembro de 2017 In http://www.tvi24.iol.pt/tecnologia/noruega/breivik-comprou-materiais-para-os-ataques-no-ebay
179 *"Artigo 10.º Registos da venda 1 - Nos estabelecimentos de venda, o vendedor dos produtos fitofarmacêuticos deve registar, incluindo no documento comprovativo de venda, o número de autorização de exercício de atividade, a data, o nome do comprador, o nome comercial e o número de autorização de venda do produto, as respetivas quantidades e os lotes e, se for o caso, o número de identificação do aplicador especializado."* e no Artigo 11.º Registos da distribuição 1 - As empresas distribuidoras devem registar, incluindo no documento comprovativo de distribuição, o seu número de autorização de exercício

Assim sendo, esta resposta jurídica veio simplificar o trabalho de campo dos Serviços que trabalham Informações, pois, permite identificar qual o item a explorar e a identificação do comprador, o que se traduz numa boa gestão da quantidade de sinergia a ser gasta, e na redução do esforço de empenhamento na tarefa.

3.2 O *INTELLIGENCE* NA ESTRATÉGIA

A estratégia passa por combinar a meditação com um ato (ação/omissão), provocado pelo intelecto na influência do ato, ora, em suma, o Intel é a inteligência de definir uma estratégia. Então, na gestão de um Estado, este terá de conceber um plano estratégico assente em modelos e sistemas que apoiem uma decisão, servindo-se para isso dos Sistema e Serviços de Informações (SSI).

O Sr. General Loureiro dos Santos retrata as informações como uma comunicação de dois tipos: informal e formal [180], mas isto só pode acontecer nas sociedades modernas (democráticas).

Na Estratégia de um Estado democrático, para que se possa validar o *Intelligence* levado a cabo pelas Tecnologias da Informação, será necessário analisar o sistema formal de controlo social português e internacional, bem como as suas regras e os seus princípios constitutivos de âmbito legislativo e territorial.

Os princípios-base são a política e o processo, no entanto, há que ter em conta, numa fase anterior e mais a jusante, princípios tais como a universalidade, a ubiquidade e a territorialidade, num tempo onde os assuntos jurídicos, criminais e forenses jorram na comunidade. Também a teoria de prevenção geral positiva aflora na sociedade, efetivando esse intento através da ameaça da punição, para assim prevenir a prática de ilícitos através da coação.

O Código Penal – CP Português prevê como princípio geral a aplicação da lei no espaço, em todos os factos praticados em território português, a bordo de navios ou aeronaves portugueses.[181] O CP prevê ainda, como lugar da prática do facto, tanto o local onde é totalmente ou parcialmente praticado, ou onde o resultado se tiver produzido, sendo que a tentativa também é punível.[182]

---

de atividade, a data, a denominação e o número de autorização de exercício de atividade da empresa distribuidora ou do estabelecimento de venda recetores dos produtos fitofarmacêuticos, o nome comercial e o número de autorização de venda daqueles produtos, as respetivas quantidades e os lotes; 2 - As empresas distribuidoras devem, igualmente, proceder ao registo dos produtos fitofarmacêuticos fornecidos por prestadores de serviços de distribuição de produtos fitofarmacêuticos que operem nos termos do n.° 3 do artigo 4.°, nomeadamente a data de fornecimento, a identificação do distribuidor, o nome comercial e o número de autorização de venda daqueles produtos, as respetivas quantidades, os lotes e o armazém de proveniência; 3 - As empresas distribuidoras devem manter os registos referidos nos números anteriores por um período mínimo de cinco anos." da Lei 26/2013.

180 O Sistema de Decisão Nacional, in Incursões no domínio da Estratégia, p. 40.

181 Código Penal da Lei n. ° 110/2015, de 26 de agosto, no seu Artigo 4. °.

182 Iden, Artigo 7.°.

O *Intelligence* tem como finalidade a produção de informações necessárias à preservação da segurança interna e externa, bem como à independência e interesses nacionais e à unidade e integridade do Estado.

As Tecnologias da Informação são cada vez mais usadas como o *locus delicti* por excelência. Então, quem tem por estratégia o uso do *Intelligence* na preservação da segurança e independência deve olhar as TI como o local do *iter criminis* na prática dos atos preparatórios.[183]

Os sucessivos atentados terroristas levaram a um endurecimento sancionatório, tal como a uma revisão do conceito de organizações terroristas, além disso, levaram também ao endurecimento sobre quem recompensar ou louvar nessas mesmas organizações ou similares.[184]

A defesa dos interesses nacionais passa não só por assegurar o Princípio da Nacionalidade bem como o Princípio da Territorialidade, nada fácil aos olhos das Tecnologias da Informação. A par disso, o Princípio da Convivência Internacional tem de sobreviver aos anteriores princípios.

Relativamente ao Interesse Nacional, o Professor Jorge de Figueiredo Dias releva a importância da nacionalidade da vítima.[185]

Também a proteção dos bens jurídicos se aproxima a nível internacional pela conexão entre leis de diferentes Estados.

> *"... o Estado em cujo território o crime foi praticado pode não se encontrar em condições de perseguir os infratores (em virtude, v.g., de graves conflitos internos), ou pode mesmo não ter vontade de o fazer (porque apoia, implícita ou explicitamente necessários à defesa própria dos seus interesses essenciais."* [186]

Este conflito de interesses por parte do Estado pode impossibilitar o Estado em perseguir, ou querer perseguir, os infratores.

---

183 O Professor Figueiredo Dias em *Direito Penal*, p. 213, defende que os atos preparatórios devam ser vistos de forma mais estrita, contudo deixa abertura à dogmática-criminal, a punibilidade, tendo em conta a proteção dos interesses nacionais.

184 O pós 11 de setembro levou à Decisão Quadro n.º 2002/475/JAI, do Conselho, de 13 de junho, relativa à luta contra o terrorismo, bem como ao surgimento da Lei n.º 52/2003 de 22 de Agosto da Lei dos Atos de Terrorismo, enaltecendo a sua Quarta alteração, criminalizando a apologia pública e as deslocações para a prática do crime de terrorismo, Lei n.º 60/2015, de 24 de junho.

185 *"... relavante é a nacionalidade da vítima, não a do agente (...) |necessidade| sentida pelo Estado português, de proteger os cidadãos nacionais (...) proteção de nacionais perante factos contra eles cometidos por estrangeiros no estrangeiro e, neste sentido a proteção de interesses nacionais ..."* In *Direito Penal*, Parte geral, Tomo I, 9º Capítulo, 19, p. 216, ss.

186 Basta observarmos a proteção dos interesses nacionais, contudo sem declinar a incriminação das organizações de atos terroristas, entre outros. Figueiredo Dias, *Direito Penal*, Parte Geral, Tomo I, 2ª edição, Coimbra Editora, 2007, p. 224, ss.

O *ius puniendi* nacional vê-se assim, em determinados momentos, com o problema de conflito de interesses com certos Estados.

No plano estratégico, os moderadores oficiais e os grupos têm de pensar os objetivos e os interesses nacionais, as aspirações e as obrigações assumidas no âmbito das parcerias internacionais, das decisões quadro, tratados ou convenções.

No que se refere aos objetivos de Estado, estes devem subdividir-se em três momentos: imediatos, intermédios e de longo prazo. Em todos eles deverá ser levado em conta um conjunto de fatores: logísticos, financeiros, pessoais e doutrinários.

Quanto aos modelos tipo, estes podem ser: preventivos ou interventivos. Se no primeiro o intuito é antecipar um acontecimento, já no segundo é atuar prontamente quando um ato surge. Estes modelos devem ser acompanhados (controlados) pelos CF e CC, assumindo estes o seu papel de Direção, Comando e Controlo das organizações com poder decisor e de supervisão da gestão das informações.

> *"Aquele que se distingue na resolução de dificuldades fá-lo antes de elas se erguerem. Aquele que se distingue na conquista dos seus inimigos triunfa antes de as ameaças se materializarem."* [187]

Os Estados têm assim na sua missão uma das principais tarefas de garante do Estado, o triunfo do bem (segurança) contra o mal (insegurança).

3.3 A SEGURANÇA DA INFORMAÇÃO

Hoje, mais do que nunca, a sociedade deve evitar os possíveis riscos, mas só através de uma análise pode evitá-los e preveni-los.

Nesta temática, ao contrário de muitas outras, existe quase uma fidelização de ideias por entre os mais diversos autores, não há divergência de objetivos, nem causas sem razão. Pode dizer-se que a maioria dos autores preconiza que a Avaliação e a Análise do Risco é um dos métodos auxiliares para apoiar a tomada de decisões relativamente às situações futuras, de forma tão acertada quanto possível, tendo também em conta um conjunto de dados quantitativos e qualitativos, transformando-se assim numa estimativa.

187 Griffith sita Tu Mu em Sun Tzu A Arte da Guerra, 2005, p. 115.

Então o Risco é, nada mais nada menos, do que uma incerteza que origina uma suposição.

Em todos os setores de atividade, os analistas então interessados em antecipar e detetar eventuais erros. Para medirmos o risco, podemos considerar três situações: Risco Certo; Risco Incerto ou Risco.

Com tais divisas bem definidas, só resta acrescentar que todas as variáveis do Risco podem ser observadas com a gestão (prudência) de uma boa análise, decompondo todo o emaranhado em dados compreensíveis, através da aplicação das disciplinas das ciências do conhecimento, criando assim uma conceção precisa do método vindouro a utilizar.

A necessidade de inspecionar e de fiscalizar a atividade da Administração Interna, tendo como referência uma rigorosa superintendência e toda uma retidão exigível a tal Instituição levou a que, em 1995, fosse criada a Inspeção-Geral da Administração Pública (IGAI).

O IGAI, como infraestrutura |fiscalizadora dos fiscalizadores|, tem à partida em mãos uma responsabilidade acrescida, pois nas suas fileiras terão de ter assento pessoas da mais alta credibilidade e largamente qualificadas.

O facto de existir um Sistema de Controlo das Forças de Segurança (GNR e PSP) leva a que uma instituição como o IGAI tenha de ser isenta e imparcial e que usufrua de autonomia técnica e administrativa.

Pese embora todas as estruturas de caráter policial tenham como supervisores extrínsecos o Provedor de Justiça, o Parlamento, o Procurador da República e os respetivos Tribunais, o IGAI traz com ele toda uma estrutura organizada para os serviços de inspeção e fiscalização onde inclusive detém um Departamento de Assuntos Internos, com a missão de observar e controlar o funcionamento das atividade policiais, regendo-se pelo Regulamento das Ações Inspetivas e de Fiscalização – RAIF.[188]

Este RAIF tem também por finalidade garantir uma cordial e correta aplicação do erário público, garantindo a prática do plano de atividades e regulando os recursos humanos. O IGAI tem *«obrigação e preocupação permanente do seguimento "follow up"»*[189]

A principal ação preventiva por parte do IGAI é defender os Direitos Fundamentais dos cidadãos, assegurada pelo Código deontológico das Forças de Segurança (GNR e PSP).

Apesar de todas estas competências do IGAI perante a GNR e a PSP, fica excluída a investigação criminal, pois esta é da competência exclusiva da PJ quando se refere a atos de investigação sobre a PSP e da competência exclusiva da PJM nos atos investigatórios relativos à GNR.

188 Regulamento n°10/99, aprovado pelo MAI de 21 de dezembro.
189 In Controlo Externo da Atividade Policial, 2002, IGAI, p. 75.

Com a envolvência de tantas instituições, o Princípio da Legalidade está mais do que assegurado, bem como uma total imparcialidade.

> *"Em vários países, um enorme "complexo vigilância-industrial" tem evoluído, fomentado pela cultura de sigilo que envolve as operações de vigilância, a sua natureza altamente técnica e o facto de tanto a gravidade das alegadas ameaças como a necessidade de contra-medidas específicas e os seus custos e benefícios serem difíceis de avaliar para os decisores políticos e orçamentais sem contar com a contribuição dos próprios grupos interessados. Existe o risco de que estas estruturas poderosas possam escapar ao controlo democrático e à responsabilização e ameaçar a natureza livre e aberta das nossas sociedades".*[190]

Quanto ao segredo nas matérias de segurança, este demonstra uma carência e leva-nos a realçar a inquietação quanto à proteção das fragilidades na troca de informações entre os diferentes membros dos Comités do Intel. A desconfiança desmorona a pureza da publicitação de informação nas relações internacionais.

3.4 MATÉRIA CLASSIFICADA

O acesso à informação classificada passa por objetivos de defesa e segurança, mas também por objetivos das áreas económicas e sociais, pelo que os funcionários de instituições ligadas ao Intel têm obrigações de restrição de liberdade e de garantia do bom manuseamento da informação classificada.

Os EUA permitem que múltiplos funcionários e agentes possam aceder aos documentos mais secretos *TOP SECRET* (cor de laranja). Esta credencial é habitual nos EUA, após o preenchimento de um questionário de 127 páginas, de uma entrevista de três horas por um investigador, e posterior teste do polígrafo. Ainda assim, estamos a falar de 5 milhões de pessoas com esse grau de credenciação, mas esse número cresce se falarmos de documentos *SECRET* (cor vermelha), *CONFIDENCIAL* (cor azul), ou *SCI* (cor amarela).[191]

Em Portugal as informações classificadas têm os seguintes níveis:

190 Resolution 2045 (2015) Mass Surveillance, Dot 9. Parliamentary Assembly – Council of Europe.
191 In O caso Snowden, p. 182.

- TRÈS SECRET UE/EU TOP SECRET: informações e material cuja divulgação não autorizada possa prejudicar de forma excecionalmente grave os interesses essenciais da UE ou dos seus Estados-Membros;

- SECRET UE/EU SECRET: informações e material cuja divulgação não autorizada possa prejudicar seriamente os interesses essenciais da UE ou dos seus Estados-Membros;

- CONFIDENTIEL UE/EU CONFIDENTIAL: informações e material cuja divulgação não autorizada possa prejudicar os interesses essenciais da UE ou dos seus Estados-Membros;

- RESTREINT UE/EU RESTRICTED: informações e material cuja divulgação não autorizada possa ser desfavorável aos interesses da UE ou dos seus Estados-Membros;

A informação classificada também pode e deve exibir a marca que designe a entidade, a atividade, identifique a entidade de origem, limite a distribuição, restrinja a utilização ou indique a comunicabilidade.[192]

Portugal difere muito da forma como os EUA dispõem as informações, pois o controlo de acesso a documentos é uma matéria muito meticulosa, pelo que a possibilidade da sua consulta deverá obedecer à classificação que é conferida ao seu consultante, ainda assim, podem excetuar-se os casos de possibilidade de análise e consulta de documentos quando este consultante estiver revestido do exercício de funções investigativas (órgãos de polícia criminal) e quando devidamente autorizado pelas chefias e legitimamente autorizado.

Ao Estado cabe decidir, através da sua organização, estabelecer as delegações de competências, a forma de ação e o alcance do acesso a documentos, ficando assim outros investidos de legitimidade de competências e poderes funcionais, conceptualizando o livre acesso a documentos.

A partilha de informações traz sempre consigo uma certa resiliência dos serviços na troca de fluxo de informação.

O acesso a uma informação do género da que se encontra plasmada no ponto 3.30 do Anexo IV, e que diz respeito a matéria muito relevantes sobre a economia portuguesa, poderá originar uma catástrofe ou hecatombe económica sem precedentes.

192 Decisão 2013/488/UE de 23 de Setembro (Relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE, revoga a Decisão 2011/292/UE)

"3.30. O Governo vai acelerar o seu programa de privatizações. O plano existente, elaborado até 2013, abrange os transportes (Aeroportos de Portugal, TAP e ramo de carga da CP), energia (GALP, EDP e REN), comunicações (Correios de Portugal) e seguros (Caixa Seguros), bem como um conjunto de empresas de menor dimensão. O plano visa receitas antecipadas de cerca de [5,5] mil milhões de euros até ao final do programa, estando apenas previsto o desinvestimento parcial para todas as grandes empresas. O Governo compromete-se a ir ainda mais longe, prosseguindo um rápido desinvestimento total das acções do sector público na EDP e na REN, e espera que as condições de mercado permitam a venda destas duas empresas, bem como da TAP, até ao final de 2011. O Governo irá identificar, até ao momento da segunda revisão, mais duas grandes empresas para privatização, até ao final de 2012. Até Março de 2012 será preparado um plano actualizado de privatizações". [193]

Não obstante esse facto, acresce que a panóplia burocrática dos serviços a que ainda assistimos traz consigo uma classificação excessiva de documentos cuja matéria é classificada.

A liberdade de informação é também *"...o direito à informação e o direito de acesso aos arquivos e registos administrativos."* [194]

A Lei nº 65/93, de 26 de agosto, veio vislumbrar e configurar o regime legal de acesso aos documentos da Administração, a qual confere um conjunto de garantias (acesso) às entidades que tratam os assuntos de segurança interna e externa e da investigação criminal.

Para que o exercício dessas garantias (acesso) seja verificável, terá a Administração Pública de ter uma atitude ativa na desburocratização dos expedientes, cooperando mutuamente entre órgãos com a garantia do cumprimento de toda a ordem jurídica do direito geral de acesso (a própria pessoa e os autorizados).

Para entendermos o Segredo de Estado, temos de entender primeiramente o Princípio da Necessidade e a respetiva observação deste, tendo como contraponto o Princípio da Administração Aberta.

193 Portugal: Memorandum Of Understanding On Specific Economic Policy Conditionality 3 May 2011, 13:40 in http://economico.sapo.pt/public/uploads/memorandotroika_04-05-2011.pdf

194 In Controlo Externo da Atividade Policial e dos Serviços Tutelados pelos MAI, IGAI, 2001, Lisboa, p. 447.

A confidencialidade da informação e as restrições ao acesso dos arquivos está sempre assegurada quando estiver em razão a Investigação Criminal, a Intimidade das Pessoas e também quando estiver em causa os serviços do SIRP (Serviços de Informação da República Portuguesa).

A Segurança Nacional, no que se refere ao acesso às informações, é assegurada pelo SEGNAC (ver 2.2.5) através Resolução do Conselho de Ministros com instruções para a Segurança Nacional, visando proteger os países no que se refere às informações. Sendo que este SEGNAC é de âmbito Nacional, ainda assim este tem de respeitar os Princípios da Excecionalidade e Necessidade, entre outros.

O regime excecional obsta limitar a divulgação percecionado o Risco de acesso por parte das pessoas não autorizadas, ainda assim consegue integrar os princípios legalmente assegurados, tais como o Segredo de Estado e os condicionalismos da sua exigibilidade.

Sendo que só quatro entidades têm competência para tornar matérias em Segredo de Estado: Presidente da República, Presidente da Assembleia da República, Primeiro-Ministro e Ministros.

A proteção de informação e a sua acessibilidade pode facilmente ser controlada com a classificação de documentos (autorização) e pode também ver a sua proteção ainda mais fortalecida quando se registem todos os acessos de entrada para que se controle o quem e o quando, sabendo-se à partida que todos os funcionários e agentes de Estado têm como especial dever o sigilo.

O IGAI, com toda a sua legalidade e legitimidade ao direito à Administração Aberta, englobou também os seus dirigentes, os inspetores e o pessoal do apoio técnico das Forças de Segurança, ao caso a GNR e PSP, quando devidamente autorizados e no exercício das funções.

Assim, reconhecer o esforço das instituições na implementação de interpretação de interesses evitará os conflitos internos e externos no sentido positivo.

A temática da matéria classificada não poderia ficar concluída sem antes confirmar que existe ainda um nível de classificação mais elevado do que TOP SECRET.

3.5 TÉCNICAS ANALÍTICAS PARA ANÁLISE DE INFORMAÇÃO

A análise de informações e as tarefas do analista laboram sobre diferentes paradigma e pensamentos críticos diversificados

As técnicas analíticas divagam em vieses cognitivas e de taxonomia dos métodos analíticos. Pensar o futuro. Introdução às técnicas analíticas estruturadas.

A utilização destas técnicas analisam, entre outros: checklist, fitas do tempo e cronologias; lista de prioridades; matrizes; análise de redes; mapas conceptuais, mapas mentais, mapas dinâmicos.

Geralmente estas técnicas dirijam processos de ideias tais como: *"1. brainstorming estruturado; 2. virtual; 3. diagrama estrela - who, what, how, where, when, why; 4. matrizes de impacto estruturado; 5. análise morfológica"*[195]

Estas técnicas analíticas permitem a elaboração de cenários como método de criação de hipóteses.

Análise de hipóteses em competição:[196]

Avaliações de causa/efeito: 1. Role playing; 2. Red Hat Analysis; 3. "Outside-in thinking". O caso da análise contraterrorista; 4. Modelo de previsão política; 5. Prediction markets.

Challenge analysis: 1. análise premortem;

Autocrítica estruturada: 1. HILP; 2. What-if; 3. Advogado do diabo; 4. Red team analysis; Método Delphi

Apoio à decisão: 1. Gestor de complexidade; 2. SWOT

3.6 FONTES ABERTAS E FECHADAS (DIGITAIS)

O Intelligence tem como propósito a obtenção de informação procedente de dois tipos de fontes: a aberta e a fechada (coberta), sendo que ambas podem ser recolhidas nas Tecnologias da Informação. Antigamente, o Intelligence tinha como alvo Estados, atualmente, com a mudança de protagonistas, tais como, os Quase Estados, ou os Lobos Solitários, entre outros, há uma necessidade e inevitabilidade do uso do Intel.

As operações dos Serviços que trabalham informações passaram não só a ter de conhecer informações relativas aos Estados, mas também à sociedade e aos seus aspetos étnicos e religiosos, proibidos de investigar pela Constituição.[197]

---

195 In, https://guia.unl.pt/pt/2019/novaims/program/4971/course/400032
196 Iden
197 *"Ninguém pode ser perguntado por qualquer autoridade acerca das suas convicções ou prática religiosa, salvo para recolha de dados estatísticos não individualmente identificáveis, nem ser prejudicado por se recusar a responder."* - Liberdade de consciência, de religião e de culto, Artigo 41.º da CRP.

Assim sendo, o Intel enfrenta grandes obstáculos na articulação dos conjuntos de dados que correlacionam o espaço, o tempo e o cenário de ação. Importa também salientar a vantagem da respetiva análise de informações, em função dos objetivos institucionais permanentes, essa análise deverá ser efetuada pela divulgação da informação facultada pelas comunicações globais. Esta divulgação é que leva o analista a percecionar alguns comportamentos reveladores de atividades ilícitas, que tem muitas vezes origem através da pesquisa e da recolha de informações por meio das fontes. As informações dessas fontes têm de ser organizadas para serem posteriormente contextualizadas, depois de serem limpas as impurezas pelo seu caráter bruto.

Estas fontes dividem-se em dois grandes campos de ação: fontes abertas e fontes fechadas.

> "... 80-90% das informações são obtidas por via aberta e 10-20% por via coberta. E muitas vezes tal é utilizado como argumento para salientar a importância dos operacionais relativamente aos analistas: os primeiros correndo riscos, inclusivamente de vida, para obter segredos; os segundos sentados confortavelmente nos gabinetes a «tirar partido» sem esforço desses mesmos riscos." [198]

As fontes persistem até aos dias de hoje como conteúdo fundamental para o Intel. A recolha de informações recorre a técnicas (meios e processos) tais como as referidas na análise seguinte OSINT, SIGINT, COMINT, ELINT, FISINT, IMINT, e MASINT.

Já sabemos que as Fontes se classificam em abertas e fechadas e, segundo Rogério Bravo, a fonte fechada

> *"... envolve a obtenção de uma autorização judicial, ou de uma forma de autorização de alto nível, ainda que possa ser de carácter administrativo e não o judicial. Na prática, a caracterização de uma fonte como "fechada" fá-la ficar fora dos limites legais de recolha de informação por iniciativa própria da polícia. Pretende-se com isso manter a privacidade do cidadão, evitar a inadmissibilidade da utilização da informação assim obtida na investigação*

198 In Borges Graça, Pedro – Informações e Segurança, Prefácio, 2004, Metodologia da Análise nas Informações Estratégicas, p. 429, ss

criminal e, no limite, evitar que sobre o agente policial ou a Organização para a qual trabalha, possa recair responsabilidade civil, disciplinar e criminal ..." [199]

O Ciberespaço é, por tendência, uma gigantesca fonte aberta, pois os cibernautas disponibilizam de forma livre a informação ali difundida. Neste sentido, o investigador Rogério Bravo em "Open Sources" na Investigação do Cibercrime: conceito e implicações deixa uma achega ao Direito relativamente à definição de fonte aberta utilizando a frase "totalmente acessível", referindo que um agente policial ao aderir a um formato sujeito a autorização (fórum) na obrigatoriedade de ter de preencher algum dado como (username e password). Este Ciberespaço continua a ser publicamente acessível, admitindo que possa também ser usado um "user" e uma "password".

Na falta de uma definição jurídica de espaço público, apelamos ao campo multidisciplinar da arquitetura para assim, por analogia, consertarmos, uma base de ciberespaço público *vs* espaço público.[200]

Já quanto à definição de ciberespaço, as definições encontradas eram tão diferenciadas e de tamanho colossal que, resumidamente, se considera ciberespaço tudo aquilo que implica o uso da internet através do uso das Tecnologias da Informação.

Assim sendo, as matérias recolhidas oriundas das fontes abertas desfruta da licitude, pois os motores de busca ou o uso de plataformas cujo emprego não esteja vetado por lei poderão e deverão ser utilizadas para recolha de informação em fontes abertas.

Portanto, não faz sentido para a tese desenvolver profundamente a destrinça entre fonte aberta (digital) e fonte fechada (digital) e os programas usados em cada qual, pois a grande diferença entre fonte aberta e fechada é basicamente a quebra de uma qualquer barreira (programação) técnica. A título de exemplo, o IMINT em tempos era usado exclusivamente pelas Forças Armadas, Serviços de Informações e Polícia pelo uso de fonte fechada. Atualmente, o notável programa google maps também recolhe informação através de imagens de satélite e de fotografia aérea/terrestre em fonte aberta.

---

199 *"Open Sources" na Investigação do Cibercrime: conceito e implicações* R. Bravo Lisboa 2014, In https://www.academia.edu/5906230/O_Conceito_de_Fontes_Abertas_na_Investigação_do_Cibercrime

200 A Arquiteta Filipa Antunes dos Santos define como espaço público urbano *"... o lugar onde se manifesta a vida e animação urbana e onde se desencadeia o encontro das pessoas que fazem parte do quotidiano da cidade. É o lugar onde se processa grande parte da socialização urbana, constituindo assim um reflexo da sociedade e um retrato da cidade..."* in, *Características físicas e sociais do espaço público Nove casos de estudo sobre as vivências urbanas no centro histórico de Lisboa*, p. 2.

Figura 7 – Imagem de um Parque de Obúses de Artilharia, onde se observa claramente as Bocas de Fogo.[201]

3.7 INVESTIGAÇÃO OPERACIONAL

Presentemente, as unidades operacionais que curam das informações são constituídas em grande parte por analistas (peritos) informáticos em virtude da crescente utilização da tecnologia para a comunicação interpessoal, derivado das características particulares do ciberespaço que são as seguintes:[202]

Caráter Dinâmico
Custo irrelevante de acesso
Enorme potencial de crescimento
Alta capacidade de processamento
Caráter assimétrico
Anonimato
Alta capacidade para produzir efeitos físicos
Transversalidade

Tendo em conta todas essas características a *guerra*, hoje é multidimensional evoluindo para formas que não indicam as armas tradicionais, não obstante, as Transmissões nas forças armadas portuguesas serem consideradas uma arma e não um serviço.

201Esta imagem devia ter um nível de classificação de segurança elevado e estar salvaguardada em fonte fechada, mas pelo contrário foi recolhida pelas Tecnologias da Informação em fonte aberta, In https://www.google.pt/maps/place/Santa+Margarida+da+Coutada/@39.4237706,-8.2929218,128m/data=!3m1!1e3!4m5!3m4!1s0xd18688ce6f14919:0x500ebbde4910000!8m2!3d39.388317!4d-8.2760021

202 Segundo o *IDN Caderno n.º 12* (2013) Estratégia da Informação e Segurança no CiberEspaço, p. 8, ss.

As Transmissões/Comunicações utilizam a esfera digital no espectro das operações e informações. Pelo que no conceito de investigação operacional iremos incluir as ações de pesquisa, recolha e análise de informações individuais ou coletivas cujas ações se poderão constituir eventualmente como atividades ilícitas.

Vários ilícitos abundam nas Tecnologias da Informação a título de exemplo: os Crimes de Guerra, tais como *"...incitar o ódio contra um povo, com intenção de desencadear uma guerra..."*[203]; os Crimes de Incitamento à guerra, tais como *"... incitamento do ódio (...) com intenção de guerra..."*[204]; os Crime de Terrorismo, tais como *"Quem (...) louvar outra pessoa, grupo, organização ou associação..."*.[205] ; ou os Crimes contra a Realização do Estado de Direito, tais como *"Quem publicamente incitar habitantes (...) à guerra civil..."*.[206]

Assim no que respeita ao Computer Network Operations – CNO, ou operações e informações no ciberespaço, estes incluem ações estratégicas através das redes de computadores que são as seguintes:[207]

Computer Network Defense – CND
Computer Network Attack – CNA
Computer Network Exploitation – CNE

Este último *"...integra as capacidades de recolha de informações (intelligence) levadas a cabo através do uso de redes de computadores para recolher dados das redes de comunicações e dos sistemas de informação de um potencial adversário."* [208]

Este tipo de exploração ganha forma cooperativa na OTAN e na UE, muito em virtude das ameaças provenientes do Ciberespaço. Muita da doutrina de operações de informação tem como base o Departamento de Defesa dos EUA.

Os estrategas das informações têm, entre outros métodos, o do contra-terrorismo que tem a capacidade de intercetar as comunicações e de geolocalização. Estas operações são muitas vezes levadas a cabo por militares, polícias e, ultimamente, tem-se recorrido a engenheiros informáticos, programadores e gestores de sistemas altamente especializados.

203 Artigo 38.º da Lei n.º100/2003, de 15 de novembro do Código de Justiça Militar.
204 Artigo 17.º da Lei n.º 31/2004, de 22 julho da Lei da Violação do Direito Internacional.
205 N. 8 Artigo 4º da Lei N.º 60/2015, de 24 de junho da Lei de Combate ao Terrorismo.
206 Artigo 325.º da Lei N.º 59/2007, de 4 de setembro do Código Penal.
207 Joint Chiefs of Staff - DoD Information Operations (2006).
208 Ciberespaço: Conceito e Âmbito em segurança e Defesa, in IDN Caderno n.º12 (2013) do Instituto da Defesa Nacional, p. 12.

A Era da Informação alargou o espectro das operações de informação, fazendo com que a atividade de exploração das transmissões recaia em grande parte nos grupos de risco que têm atividades supostamente perigosas. A esta atividade dá-se o nome de «vigilância em massa», perturbadora de algumas garantias supostamente pessoais e garantidas constitucionalmente.

Embora os tempos atuais tenham a alcunha de "Era da Informação", já desde o tempo em que Lord Curzon era Chefe de Gabinete da Comissão dos Serviços Secretos Britânicos (1919) que se trabalha (aquisição, análise e interpretação) no Intel com origem em Comunicações através de Sistema de Informação. Também entre 1939 e 1945 este tipo de Intel foi alvo de intensa atividade, mais propriamente em Buckinghamshire, já nessa data eram cerca de 10 mil pessoas, entre Ingleses e Americanos, que trabalhavam nas escutas e informações de origem eletromagnética. [209]

A atividade do *Intelligence* abrange tradicionalmente informações de questões políticas e militares, informações essas que conduzem à compreensão do opositor. A generalidade das pessoas fala em espionagem quando se fala em recolher prioritariamente dados económicos de nações amigas ou de concorrentes industriais. Os Serviços de Informações abrangem um vasto leque de capacidades de recolha de informações.

O Intel usa especialmente duas áreas: Humana e Tecnológica.

- Humana:

Human Intelligence (HUMINT)

- Tecnológica:

Open Source Intelligence (OSINT)

Signals Intelligence (SIGINT)

Communications Intelligence (COMINT)

Electronic Intelligence (ELINT)

Foreign Instrumentation Signals Intelligence (FISINT)

Imagery Intelligence (IMINT)

Measurement and Signature Intelligence (MASINT).

209 Keith Jeffrey e Alan Sharp, Secret Intelligence at Lausanne, p. 79, ss.

HUMINT

O *HUMINT* é o método de recolha de informações mais antigo, pois usa o ser humano como instrumento e fonte de informação, assim sendo, como está fora do teor desta tese, não será abordado, será apenas referido para mero enquadramento do Intel.

OSINT

É um método de recolha de informação através de fontes livremente acessíveis a todos podendo ter os mais variados formatos digitais, tais como: jornais, revistas, rádio, televisão, internet (sites foruns, deep web, redes sociais tais como *twitter, facebook*, etc.). Os sites especializados também são fundamentais pelo facto de o objeto de estudo estar concentrado no respetivo site, bem como pelo facto de os seus utilizadores serem mais restritos e em alguns sites até verificável o seu estado on/off-line.

Utilizando ferramentas extras disponíveis nos navegadores, tais como *screengrab*, vídeo, *downloaderhelper* e *scrapbook,* e efetuando pesquisas através de motores, tais como *Google, bing, yandex, baidu, duckduckgo, wolframalpha,* etc., com possibilidades de *tracking, anonymizing proxy* e tor, o processo OSINT tem a sua estrutura assente, além da identificação e exploração, em requisitos da informação relevantes através de palavras-chave ou expansão semântica. Este processo permite ao analista de informações fazer relatório analítico a através de uma *situation awareness* utilizando um *Mind Map.*

A exploração das potencialidades de pesquisa da OSINT poderão ser ainda intensificadas através de métodos mais intrusivos.[210]

SIGINT

O *SIGINT* depende da interceção de transmissões individuais ou coletivas recolhidas pelo método *COMINT, ELINT*, e *FISINT*.

O SIGINT pode ser usado em variadas plataformas e pode ser rastreado mesmo nos meios de transporte, tais como aviões ou navios. Muito devido ao facto de o *SIGINT* conseguir monitorizar transmissões a partir de comunicações de satélite ou terrestres, tem particular importância nas transmissões transoceânicas.

210 Curso de Fontes Abertas (OSINT) Direção de Formação, Escola das Armas, Exército Português.

O SIGINT com origem nos EUA inclui o *"... International Maritime Satellite system (INMARSA T), the International Telecommunications Satellite system (INTELSA T),and the European Satellite system (EUROSA T) (...) ".*[211] O SIGINT é por norma o pai das interceções eletromagnéticas *"... intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems. SIGINT provides a vital window for our nation into foreign adversaries, capabilities, actions, and intentions."* [212], mas existem três tipos principais de transmissões do SIGINT: COMINT, ELINT e FISINT.

COMINT

Entre os três tipos de transmissões, o COMINT é de longe o mais importante, pois esta técnica interceta comunicações rádio tanto militares como civis, veja-se, por exemplo, o caso da "missão Gupy" de que foram alvos os altos dirigentes do Kremlin. Este tipo de técnica poderá ser usada na contra-informação, pois, *"Antes de colocar uma bomba, o sinal de rádio deve ser testado e, se os serviços de escuta conseguem captar o sinal, podem, pirateando-o, fazer explodir a bomba prematuramente."* [213]

O COMINT debruça-se no texto falado e escrito transmitido por vídeo, código Morse, ou mensagens simbólicas. O COMINT compila Intel originária de ondas de frequência, cabo, fibra ótica, entre outros.

ELINT

Já a ELINT é uma técnica de interceção e análise também de não comunicações (simples localização), como radares que identificam e georreferenciam objetos, e não a usual transmissão entre emissor/recetor. A ELINT é também destinada a satélites e mísseis, o que inclui sinais de aquisição, como os que usam os dados telemétricos como o FISINT.

FISINT

O FISINT inclina-se para a interceção telemétrica principalmente de sistemas de armas, o que inclui informações sobre as características técnicas, devido a este tipo de informações, o FISINT é usado frequentemente no estudo de protótipos.

211 Intelligence threat handbook - Operations security (OPSEC), p.26, in https://fas.org/irp/nsa/ioss/threat96/part02.htm
212 Informação recolhida no site da NSA https://www.nsa.gov/sigint/ em 25 de novembro de 2015.
213 Conforme escreveu Géné em Contre services secrets britanniques, in O caso Snowden, p. 199.

IMINT

A Imagery Intelligence — IMINT — está relacionada inteiramente com a recolha de informação através de imagens de satélite e de fotografia aérea.

MASINT

O Measurement and Signature Intelligence – MASINT — depende em grande parte do IMINT e do RADINT

Existem ainda formas de recolha de informações envolvendo outras técnicas meios e processos diversos dos anteriores, tais como GEOINT, STRATINT, CYBINT, RADINT e UMBRA.

GEOINT

A Geoespacial Intelligence – GEOINT — relaciona-se totalmente com vigilância, aquisição de objetivos e navegação. Neste processo, as estratégias, metodologias e instrumentos de gestão de informação geográfica passam pelo exame de quesitos de interesse.

A diversidade da forma de administração no delinear, supervisionar e simular fenómenos geográficos, estratégicos, militares, demográficos e ambientais em diversas conjunturas, diminui os graus de dúvida relacionados com os intentos dos quesitos de interesse da informação a relevar. Esta administração é auxiliada por sistemas e tecnologias que cuidam das carências organizacionais de informação geográfica, tais como o SIG (ver em 4.1.5).

Este tipo de recolha de imagens (GEOINT) estreou-se primordialmente através do uso de aviões pelos anos 20 do século passado, atualmente são levadas a cabo através de Drones ou de Satélites.

STRATINT

O Strategic Intelligence, pese embora não seja um meio de recolha de informações, trata antes do processo em si, antecipando os perigos e prevendo o futuro, incorporando todos os multifatores acessíveis e válidos tendo em conta o objetivo. O STRATINT não pensa só o processo de aquisição das tecnológicas, mas pensa também o processo de interpretação humana. Este pensamento estratégico faz conjeturar um entendimento até chegar ao conhecimento.

CYBINT

O Cyber Intelligence – CYBINT — tem apoio nas atividades de HUMINT e SIGINT, mas, ao contrário destas atividades do Intel, o CYBINT requer estar assente no tempo real e incluir a Technical Intelligence (TECHINT), identificando e fiscalizando o desenvolvimento das atividades à sua volta, sejam estas económicas, militares ou outras. O CYBINT tem a capacidade de penetrar e de neutralizar ameaças. Estes desafios requerem muito conhecimento e constantes interações como, por exemplo, controlar infraestruturas críticas e apoiar a indústria tecnológica.

O CYBINT disponibiliza a um Estado uma quantidade de informação que lhe vai proporcionar uma vantagem.

RADINT

O Radar Intelligence – RADINT — é uma técnica da interceção dos sinais de radar.

> *"... coleta, análise, processamento, integração, avaliação, análise e interpretação das informações disponíveis sobre nações estrangeiras, forças ou elementos hostis ou potencialmente hostis, ou áreas de operações reais ou potenciais. O termo também é aplicado à atividade que resulta no produto e às organizações envolvidas em tal atividade".* [214]

Esta técnica foi muito usada pelo Intel nos anos 20 e 40, atualmente é uma disciplina do MASINT.

UMBRA

Todas estas formas de recolha são elaboradas através da seleção de informação veiculada pela troca de comunicações entre sistemas digitais.

> *"Conhecendo os grupos de terroristas sobre as formas de Intel utilizada pelos serviços de informações, eles irão utilizar cada vez menos esses meios detetáveis e voltarão às velhas técnicas de comunicação."* [215]

214 In https://definedterm.com/a/definition/239199

215 A Socióloga da Polícia Judiciária, Núria Amaral, fazendo alusão à retroatividade das formas de comunicação por parte dos terroristas, na sua tese de mestrado – *O Papel dos Serviços de Informações no Combate ao Ciberterrorismo: O Caso Português,* p. 58, ss.

Assim sendo, este tipo de recolha de informação não aparece só na forma de combate aos crimes, mas também como forma de prevenção criminal. Pois, atualmente, de que outra forma poderá comunicar, a título de exemplo, um grupo terrorista que esteja geograficamente descentralizado...

Não poderíamos deixar de referir que a partilha de informações de outros serviços de informações também é considerada uma fonte.

3.8 ESPIONAGEM, AUDITORIA FORENSE E GOVERNANCE

A (contra) espionagem, a auditoria forense e o *governance* assumem uma função social/empresarial de proatividade, no sentido de proteger e salvaguardar a informação enquanto bem jurídico autónomo. Estes serviços funcionam como observatórios permanentes sobre a segurança tecnológica, enquanto ferramenta das comunicações, reconfigurando a manutenção das infraestruturas dos sistemas.

A prevenção e Análise do Risco passa também por ter um sistema de modelo de fiscalização e controlo. No caso da GNR e da PSP, esse (modelo) fiscalizador é o IGAI, que circunscreve um conjunto de ações, visto ser dotado de autonomia administrativa e ser um serviço público. Podendo, assim, dominar a política de gestão destas estruturas.

O IGAI tem capacidade para avaliar, controlar todos os procedimentos dessas Forças Policiais, através de auditorias internas, pois o IGAI tem ainda poder de inspeção do funcionamento. A par disso, quer o Comando Geral da GNR quer a Direção Nacional da PSP têm modelos de inspeção interna, dependendo diretamente do seu Comando e Direção. Desta forma, o Risco poderá ser diminuído através da Análise (auditoria) e de forma Preventiva, modernizando, racionalizando e simplificando os modelos de gestão. Por outro lado, a Análise pode também levar a cabo a forma Repressiva de controlo de risco quando dá início aos atos investigatórios.

> *"Na apreciação de queixas, reclamações e denúncias, instauração de processos de averiguações, realização de sindicâncias e inquéritos e instrução de processos disciplinares determinados pelo Ministério."*
>
> Controlo Externo da Atividade Policial (IGAI) 2002

O Risco pode também ser combatido com uma Instrução Doutrinária rigorosa e com um planeamento organizado, obedecendo às metodologias de formação especializadas com planos

preventivos de controlo do Risco, articulando o Comando da GNR e a Direção da PSP com o IGAI, pese embora toda a hierarquização esteja ligada diretamente ao Ministério.

ESPIONAGEM

As fontes aparecem de forma diversa e apresentam três padrões de serviços: *Friendly/Enemy/Neutral*. Há autores que defendem que a Espionagem só aparece entre nações inimigas, tese que será veementemente impugnada nos parágrafos que se seguem.

A troca de informações processa-se através de reuniões, por troca, ou a pedido. Aqui saem favorecidos os serviços que entre si partilhem de vinculações, tais como, políticas, culturais, geográficas, estratégicas, entre muitas outras.

A base da espionagem está no recurso ao Intel, na busca de informações de relevo, tais como as que a NSA recolheu antes da 5.ª Cimeira das Américas, usufruindo assim de uma compreensão mais profunda das intenções dos participantes e trazendo consigo uma vantagem desleal para com os outros intervenientes na cimeira. Nessa altura, foram analisadas 80.000 mensagens pela agência NSA sobre documentos *Top Secret*, com especial enfoque sobre as informações relativas à avaliação das reservas de petróleo offshore a partir de amostras extraídas do mar levadas a cabo pela Petrobras.[216]

Neste caso, os EUA espionaram um suposto Estado *Friendly*, pelo menos é o que aparenta das relações entre os EUA e o Brasil.

Já na contraespionagem, o uso de portas insonorizadas, "Gaiolas de Faraday", é uma das técnicas que serve para bloquear as ondas de rádio, que através de uma superfície condutora eletrizada, que não tem qualquer campo elétrico, evita as interferências eletromagnéticas nos equipamentos eletrónicos.

AUDITORIA FORENSE

Reconhecer os riscos proeminentes e a fiscalização das Tecnologias da Informação – TI – é o principal objetivo da Auditoria Forense, bem como os alicerces indispensáveis para a concretização de procedimentos de boa auditoria interna/externa de TI.

Ajustar as conceções das TI assenta em grande parte na arquitetura de Sistemas de Informação nos mais favoráveis moldes (*Standards* e *frameworks*) e na atribuição de cargos e obrigações ao grupo de auditores das TI. Administrar as TI passa também por uma favorável gestão e organização das TI, determinar as políticas e procedimentos a adotar através da elaboração de um

216 Lefébure cita, a fonte globo.com, em *O Caso Snowden*, pag. 115 relativa aos documentos sobre a espionagem a Dilma presidente do Brasil.

planeamento estratégico reconhecido por todos e para todos os colaboradores, assente na separação de funções dos diversos colaboradores. A preparação da auditoria às TI baseia-se em grande parte na observação do risco *vs* benefícios. Assim sendo, todo o processo de auditoria deverá ser incorporado tendo em conta a definição de prioridades e dos objetos a auditar.

Quanto à segurança de sistemas e bases de dados, esta deverá ser garantida da seguinte forma:[217]

> *" Política de Segurança da informação*
> *Gestão de acessos*
> *Segurança aplicacional, sistema operativo e base de dados*
> *Revisão de acessos, perfis e privilégios*
> *Segregação de funções*
> *Segurança física e ambiental*
> *Auditoria ao processo de gestão de desenvolvimento "*

Uma das conceções de controlo do risco é elaborar o risco de processamento tendo em conta o ciclo calculado da aplicação dos sistemas e Tecnologias da Informação.

Quanto à operação das TI, esta deverá ser garantida da seguinte forma:[218]

> *" Funções e responsabilidades*
> *Riscos e controlo de backups e armazenamento de dados*
> *Planeamento e controlo de processos batch*
> *Gestão de incidentes e problemas*
> *Auditoria de Plano de Continuidade e Recuperação de Negócio"*

Uma Auditoria Forense levanta uma questão muito relevante que é a definição legal de entidade jurídica às Auditoras Forenses e a relação cliente-fornecedor em colisão com a licitude e o dever de informar.[219]

---

217 PWC Auditoria em Sistemas e Tecnologias de Informação, Consultado em 05 de dezembro de 2017, In https://www.pwc.pt/pt/formacao/portefolios/curso-gest/lisboa/auditoria-interna-gestao-de-risco/auditoria-em-sistemas-e-tecnologias-de-informacao.html

218 Iden

219 Recordamos a título de exemplo o Relatório da Auditora PwC ao Grupo Espírito Santo – GES, em que na Comissão de Inquérito da AR, o Sr. deputado Duarte Marques classificou de "... espécie de assassínio financeiro ..." aquilo que se passou com o investimento da PT no GES. Já o Presidente da PWC, à altura Dr. José Alves, explicou que "A definição dos termos de um trabalho como este é feito entre cliente e fornecedor (...) | ainda assim referiu que o

GOVERNANCE

A noção de *Governance*, na sua generalidade, é entendida como um modelo de gestão de uma qualquer entidade (Estado, empresa, etc.). Este conceito segundo a College of Arts and Sciences at Webster University tem enfoque especificamente na eficácia do poder executivo do governo.[220]

O modelo de gestão *Governance* mistura as instituições formais e informais de controlo social. Este modelo consente à sociedade a prática do poder, da autoridade, de forma a influenciar as decisões de políticas de interesse público.

Um |bom| governo acarreta assim um alto nível de eficácia organizacional em relação às políticas realmente seguidas, particularmente na orientação da política económica e do seu contributo para o crescimento, estabilidade e popular Bem-estar. O |bom| governo também implica responsabilidade, transparência, participação, abertura e estado de direito. Representa igualmente a propagação de organizações de base e organizações não governamentais, como associações de agricultores, cooperativas e grupos de mulheres.

O *Governance* tem em consideração quesitos de natureza constitucional que estabelecem as regras da conduta política.

Para terminar, a conceção de *Governance* é assim uma ferramenta de administração de assuntos de interesse e domínio público e conjuntamente reverteu-se a uma edificação analítica e por vezes de ordem política comparativa.[221]

3.9 ATAQUES INFORMÁTICOS

A Sociedade de Informação vive diariamente entre ataques (vírus) e proteções (antivírus), vive também com a desmedida capacidade de dissimulação, com potencialidades incalculáveis das ameaças.

As Tecnologias da Informação são famosas pela sua simplicidade e alta sofisticação, sendo esta última ponderável determinante, pois, se por um lado possibilita o anonimato dos indivíduos/máquinas, por outro permite o rastrear das pegadas digitais.

---

relatório| não passou a incluir juízos de valor que, volto a referir, valeriam, que eram de uma entidade jurídica (...) |uma qualquer conclusão| pode ser chegada por qualquer outra análise jurídica". José Alves assegurou, que a PwC comunicou ao Banco de Portugal, mediante a auditoria de dezembro de 2001, das "suspeitas" em relação aos créditos autorizados pelo BES, que poderiam ser investimentos do próprio banco. Aqui também o supervisor da banca releva para os factos de ilicitude algum do conhecimento que lhe vier a ser dado ainda que de proveniência de uma Auditoria Forense.

220 Consultado em 05 de dezembro de 2017, In http://www.webster.edu/arts-and-sciences/academics/history-politics-international-relations/comparative-and-regional-governance.html

221 In Democracy, Governance and Economic Policy Sub-Saharan Africa in *Comparative Perspective* in John Healey and Mark Robinson Overseas Development institute, p. 47, ss.

As ações físicas podem afetar a arquitetura das Tecnologias da Informação, tais como os efeitos, *"Shut Down"* que desliga todo o sistema e só inicia à ordem, *"Broken Wall"* que quebra as barreiras de segurança ou "*I'm In"* entrar dentro da arquitetura das TI.

Há ataques que, embora informáticos, *"... são dirigidos contra o cérebro humano, utilizando os meios da infraestrutura, como é o caso das técnicas de propaganda, de deceção, de desinformação ou a ação psicológica"* [222]

Figura 8 – Imagem de um Vídeo onde se finge um atentado terrorista – Málaga 24h TV.[223]

O vídeo acima enunciado reporta a elaboração de um falso atentado terrorista que se tornou viral na internet. A explosão não tem na realidade qualquer vítima, mas serve para manipular a opinião pública. Neste vídeo vê-se toda uma sequela teatralizada, num bairro do Iraque, onde se vê um homem a aproximar-se de um carro e a colocar um artefacto explosivo no seu interior, de seguida o homem abandona o lugar noutro veículo. Quando a bomba rebenta, a rua encontra-se completamente vazia, não há sangue, não há ferimentos ligeiros e muito menos vítimas mortais, passados alguns segundos, o local é invadido por figurantes caraterizados com roupas rasgadas e manchas vermelhas para simular um atentado com numerosas vítimas mortais, chega mesmo a haver uma carrinha que simula o auxílio de transporte de feridos, tudo isto impecavelmente sincronizado. Para ainda dar maior semblante a este autêntico teatro, os atores simulam estar a pedir ajuda, tudo isto decorre tendo como pano de fundo o carro que explodiu continuamente a arder.

A própria agência de notícias Reuters, tão prestigiada pelo seu trabalho, também caiu no engodo, chegando a divulgar as imagens.

222 In de Jesus Bispo, António – *Informações e Segurança*, Prefácio, 2004, A Função de Informar, p. 97.
223 Falso terrorismo: o vídeo que prova que nem todos os atentados são verdadeiros, Málaga 24h, Consultado em 30 de abril de 2018 in, https://youtu.be/UPfMbT8JCRw

Este tipo de vídeos de propaganda tem como fins o ataque a uma ideologia, à política, ao Estado, logo podemos assim estar na presença de um crime de falsidade informática. [224]

3.10 SECURITY AFFAIRS

O padrão de crescimento das Tecnologias da Informação nas suas mais variadas formas de comunicação é incomensurável, assim também o deveriam ser os aspetos relacionados com a segurança.

As infraestruturas críticas padecem em muito desta insegurança, pela possibilidade de sabotagem a uma qualquer estrutura de construção civil, à produção de bens e serviços ou, no âmbito de elementos tecnológicos, impossibilitarem o tráfego de informações, entre muitos outros.

> *"Neste âmbito, se considerarmos o funcionamento da Rede Nacional de Emergência (112), do sistema de distribuição de águas ou mesmo do sistema de distribuição de energia elétrica, verificamos que se geram "cascatas de interdependências" decorrentes das suas interações e do funcionamento dos seus subsistemas. A quebra dos fluxos de informação, necessários ao funcionamento de qualquer um destes sistemas, poderá ter consequências catastróficas."* [225]

As questões de segurança sofrem assim um problema de proteção jurídica, será necessária então um imputação jurídica similar em diversos Estado em virtude do *Lex loci rei sitae*.[226]

Atribuir responsabilidades e funções aos diversos Estados membros difunde uma visão securitária que se justifica também pelo aumento circunstancial do risco, garantindo a segurança interna e externa, bem como a segurança a que cada um se reconhece.

Aqui a segurança pode e deve ser confundida também com a cidadania, assim o papel regulador do Estado torna-se de dimensão universal com formulação de políticas de segurança pública.

O Dr. Nuno Silva afirma que os fins do Estado assentam em três vertentes: "... a "segurança" – externa e interna; a "justiça" – cumulativa e distributiva e o "bem-estar" – económico e social."[227]

---

224 "1 - Quem, com intenção de provocar engano 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." Artigo 3.º - Falsidade informática - Lei n.º 109/2009 de 15 de Setembro - Lei do Cibercrime.

225 Cor Doutor Viegas Nunes, *Mundos Virtuais Riscos Reais: Fundamentos para a Definição de uma Estratégia da Informação Nacional,* no I Congresso Nacional de Segurança e Defesa, p. 487, ss.

226 Em virtude do lugar onde os bens estão situados e a lei vigente segundo a localização destes para os efeitos de conflito legislativo.

227 In, *Cidadania e Segurança: Uma Análise Prospetiva*, no I Congresso Nacional de Segurança e Defesa, p. 551, ss.

O mesmo autor propõe uma reflexão a uma participação ativa na implementação das políticas públicas de segurança.

O conceito de segurança tende assim a alargar-se a outros âmbitos, ao caso estudo às Tecnologias da Informação.

A construção de uma análise compreensiva relativa ao *Intelligence* traduz-se assim, por razões securitárias, na aceitação das Autópsias Digitais às Tecnologias da Informação, ultrapassar e desconsiderar a devassa da vida privada mesmo que por meio informático[228], em detrimento de uma busca a lugar (digital) por motivos de segurança. Até porque não há uma intenção de devassa, a real intenção é a de prevenção.

3.11 CRIPTOGRAFIA (PRETTY GOOD PRIVACY) E DESCODIFICAÇÃO (NUCLEON)

A tarefa árdua de salvaguardar a vulnerabilidade dos sistemas digitais levou a uma prevenção criativa perante os novos desafios pelo uso de redes de transmissões de dados, mais ainda quando se trata do acesso às bases de dados. Os engenheiros informáticos têm de ultrapassar os novos desafios tecnológicos, ao caso, as sucessivas reinvenções da codificação ou encriptação, o secretismo das mensagens levou à conceção de instrumentos que resguardassem mensagens ou ficheiros.

O emprego de uma linguagem codificada para transmissão, chamada esteganografia, disfarça dados em ficheiros que incluem som e/ou imagem.

O programa de codificação Pretty Good Privacy – PGP, segundo fontes do FBI, é muitas vezes utilizado pelas associações terroristas ou por criminosos altamente organizados para disfarçar comunicações.

O PGP é um programa de computador com funções de encriptação e desencriptação de dados (textos, e-mails, arquivos, diretórios e partições inteiras de disco) que fornece autenticação e privacidade criptográfica para comunicação de dados via e-mail.[229]

A NSA, através da descodificação de operações da rede de cartões bancários, intercetou a rede SWIFT, georreferenciando transferências intercambiais, mais propriamente num serviço chamado *Follow the Money*.[230]

---

228 Artigo 192.º Devassa da vida privada 1 - Quem, sem consentimento e com intenção de devassar a vida privada das pessoas, designadamente a intimidade da vida familiar ou sexual: a) Intercetar, gravar, registar, utilizar, transmitir ou divulgar conversa, comunicação telefónica, mensagens de correio eletrónico ou faturação detalhada;
Artigo 193.º Devassa por meio de informática 1 - Quem criar, mantiver ou utilizar ficheiro automatizado de dados individualmente identificáveis e referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada, ou a origem étnica, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias. (...), ambos os artigos do Código Penal.

229 Conforme descreve Paulo Rebelo em *O PGP é sistema de segurança avançado para o correio eletrónico*, in http://tecnologia.uol.com.br/segurança/ultnot/2009/02/09/ult6065u8.jhtm

No que respeita à interceção de chamadas telefónicas, existe um programa que tem por nome Nucleon e que tecnicamente filtra palavras-chave faladas, esta ferramenta é utilizada também pela agência NSA. Esta prática filtra assim informação relevante por amostragem.

Segundo McCullagh, sobre o modo como o Departamento de Justiça Norte Americano vê o programa Nucleon, este refere que a NSA *"... interpretou as leis federais de vigilância, de maneira a permitir a milhares de analistas de base escutarem as chamadas telefónicas ..."* [231]

Após as revelações de Snowden, os EUA passaram por uma crise de moral, isto levou a que o Presidente dos EUA Barack Obama aparentemente forçasse a que se objetivasse os limites das escutas só a pessoas que representassem uma potencial ameaça terrorista.[232]

Esta crise levou o FISC a decretar a desclassificação de documentos e a torná-los públicos.

O General James Clapper, Diretor do Serviço Nacional de Informações (2010-2017), expôs o seguinte *"... devemos restaurar a confiança do público e dos seus representantes ..."* [233]

O Engenheiro e Criptógrafo Bruce Schneier, em virtude da quebra de contrato social pelos abusos por parte dos SI na hipervigilância e intrusão maciça e no funcionamento da internet, em carta aberta, apelou aos Engenheiros e Programadores informáticos que vendessem e criassem programas de armazenamento de dados que combatessem todos os dias como se de um ato de revolta se tratasse. Bruce sugeriu também criar uma Internet Engineering Task Force – IETF, o que veio a acontecer, e trouxe consigo uma revisão ética de segurança no controlo da internet, englobando routers, redes, as tecnologias encriptadas, bem como os sistemas da cloud.

Os abusos levados a cabo pela NSA como que legitimam os que são praticados por outros Estados, menos democráticos, tais como a China, a Rússia e o Irão, entre outros.

> "O apelo do Parlamento Europeu para promover o amplo uso da criptografia e resistir a quaisquer tentativas de enfraquecer a criptografia e outros padrões de segurança da Internet, não apenas no interesse da privacidade, mas também no interesse das ameaças contra a segurança nacional colocadas por Estados desonestos, terroristas, ciberterroristas e criminosos comuns". [234]

---

230 Lefébure cita, Laura Poitras et Al, através da fonte Der Spiegel, de 27 de agosto de 2013, em *O Caso Snowden*, p. 161.
231 NSA spying flap extends to contentes of U.S. phone calls, in news.cnet.com
232 Pelo facto de ter sido veiculado pelos Media que a NSA teria escutado no mínimo 35 chefes de Estado, em *O caso Snowden*, p. 342.
233 Sobre a decisão do FISC relativa à desclassificação de documentos, que até à data tinham uma classificação de grau elevado, em *O caso Snowden*, p. 344.
234 Resolution 2045 (2015) Mass Surveillance, Dot 17.2 Parliamentary Assembly – Council of Europe.

3.12 SERVIÇOS DE GESTÃO DE SEGURANÇA E RISCO DA TECNOLOGIA (BOOZ ALLEN HAMILTON)

Existem empresas cuja atividade principal é a prestação de serviços de consultoria, gestão, tecnologia e segurança. Estas empresas, por norma, prestam serviço para empresas de segurança, paramilitares, de defesa e até mesmo para os Serviços de Informações Estatais.

Estas empresas dedicam-se à Estratégia Operacional, e têm como principal função o apoio à tomada de decisões dos comités de Informação e Decisão (ver 2.1.1).

BOOZ ALLEN HAMILTON

É uma das muitas empresas de consultoria e gestão, com sede nos Estados Unidos, e conta com mais de 80 escritórios. Esta empresa dispõe de funcionários civis com acesso a matérias classificadas e com acesso aos documentos mais secretos *TOP SECRET* (ver 3.4). Um desses funcionários era o Analista de Sistema Edward Snowden, que disponibilizou documentos *TOP SECRET* em fonte aberta, através dos jornais *The Guardian* [235] e o *The Washington Post* [236], o seu conteúdo era relativo ao Intel e seus programas.

Esta empresa não só integra softwares, como também desenvolve e utiliza ferramentas para a interação de uma diversidade de programas informáticos. A mesma anuncia ser prestadora de serviços tais como *"... Consulting, Analytics, Digital Solutions, Engineering, Cyber ..."* a instituições de diversas áreas tais como *"... Civil Government, Commercial, Defense & Intelligence, International, Energy, Resources & Ulitities, Financial Services, Helth, Homeland Security & Law Enforcement, Transportation ..."* [237]

Esta empresa é perigosamente global, pelo uso intensivo de Tecnologias da Informação que a levam a uma posição dominante no mercado e em todos os setores de atividade, sejam eles no setor primário (atividade extrativa da natureza), no secundário (transformação), ou no setor terciário (serviços). Esta empresa fica em posição de supervisão de todos os fluxos inerentes às mais diversas interações.

Se uma empresa como a Booz Allen Hamilton tivesse atividade sediada em Portugal, no mínimo teria de ser fortemente supervisionada pela Autoridade da Concorrência – AC e pela Comissão de Mercado de Valores Mobiliários – CMVM, por possível posição dominante e pela prática restritiva da

235 In https://www.theguardian.com/us-news/the-nsa-files
236 In https://www.washingtonpost.com/opinions/edward-snowden-doesnt-deserve-a-pardon/2016/09/17/ec04d448-7c2e-11e6-ac8e-cf8e0dd91dc7_story.html?noredirect=on&utm_term=.4bb73fee81ef
237 In https://www.boozallen.com

concorrência, em virtude de poder dispor de um ou mais mercados, ou porventura pelo abuso de posição dominante pela utilização indevida do seu poder de mercado, explorando talvez outros agentes económicos ou até mesmo a sua exclusão de concorrentes do mercado.

Quanto a uma possível imputação da Booz Aleen, teríamos de correlacionar, entre outras, com a tutela jurídica da Lei da Concorrência. [238]

3.13 INVESTIGAÇÃO DIGITAL

Não se pode levar a cabo uma investigação digital, sem triturar um conjunto de princípios constitucionalmente salvaguardados, argui-se então metodologias jurídicas que possibilitem uma licitude à tal trituração de princípios.

Sendo hoje em dia o formato digital uma forma de «expressão humana elevada» e também uma das mais utilizadas dando encaminhamento ao vasto fluxo informacional que abunda na sociedade virtual, terá de existir uma correspondência que inclua a forma de comunicação falada/oral e a escrita/digitada.

Segundo José Costa, a informática trouxe *"a possibilidade de a palavra não ser escrita, nem falada, estar virtualmente visível em um écran", podendo até "ser criada, recriada, transformada..."* [239]

A esta valoração conclusiva teremos de contrapor a valoração institucional do peso dos valores jurídicos adjacentes aos SI.

A perceção problemática dos costumes do «jogo da intel» levar-nos-á a calcular ponto a ponto a parte, e não o todo, da humanidade, assim fazendo jus aos apelidados "perigosos dissimulados" [240]

3.14 DIVULGAÇÃO (PINTAURA)

A distribuição dos resultados das autópsias digitais às Tecnologias da Informação é levada a cabo de forma automatizada através de softwares, ao caso de estudo, o (Pintaura), *"... a partir daí é atribuído um novo nome aos dados: P1 para a Microsoft, P2 para a Yahoo!, P3 para a Google, P4 para o Facebook, P5 para a Paltalk, P6 para o Youtube, P7 para o Skype, P8 para a AOL, e PA para a Apple."* [241]

238 "... 1 — É proibida a exploração abusiva, por uma ou mais empresas, de uma posição dominante no mercado nacional ou numa parte substancial deste." Art. 11° - Abuso de posição dominante - Lei n.° 19/2012 de 8 de maio - Regime Jurídico da Concorrência.
239 Costa, p. 152.
240 É a partir do conceito de "perigosos dissimulados" que Gunther Jalobs sustenta em grande parte a sua teoria do direito penal do inimigo.
241 Top Level Telecommunications, Prism as part of the Blarney program.

Este software absorve o Intel através das colossais bases de dados das empresas de internet, e para isso basta só dar-lhe pontos de referência, tais como, "nome", assunto e endereço de e-mail.[242]

Alguma desta informação resultante de Autópsia Digital está interdita à NSA, mas disponível para o FBI, tal e qual o caso Português que interdita as Autópsias Digitais ao SIRP, mas autoriza à PJ (ver 2.3.4).

A divulgação de documentação sensível poderá ser muitas vezes restrita, e para isso basta que o documento seja intitulado com marcas *Special Access Programs* (SAP), assim, o controlo passa a ser por camadas. Passa a ter de haver uma premissa que é a "necessidade de conhecimento".

Estas marcas designam-se e prescrevem-se da seguinte forma:[243]

> *"NOFORN – (não deve ser comunicada a estrangeiros)*
>
> *NOCONTRACT – (não deve ser comunicada a prestadores de serviços externos)*
>
> *ORCON – (difusão controlada pelo autor mediante numeração dos exemplares)*
>
> *EYES ONLY – (informações da NSA)"*

Os metadados recolhidos pela NSA são armazenados durante um ano em duas bases de dados e é possível saber o tráfego dos alvos, o histórico de consulta e as atividades das redes sociais.[244]

3.15 INTEROPERABILIDADE DOS SISTEMAS

Em Portugal, a permuta de informações criminais entre Forças e Serviços de Segurança funciona através de uma Plataforma para o Intercâmbio de Informação Criminal – PIIC, que pretende juntar numa só plataforma os diversos sistemas de investigação criminal de todos os parceiros, de modo a que todos os analistas credenciados possam, legalmente, utilizar toda a informação existente na PIIC para a sua investigação criminal. Tal como o nome indica, a PIIC permitirá o intercâmbio da informação entre PSP, GNR, Polícia Judiciária, Serviço de Estrangeiros e Fronteiras e Polícia Marítima, sempre no estrito cumprimento da legislação em vigor, nomeadamente em termos de controlo e regras de acesso à PIIC.

242 Todo este Intel embora pareça um dado adquirido necessita sempre do aval do Foreign Intelligence Surveillance Act – FISA por solicitação do Governo Americano, In *O Caso Snowden*: Como os EUA espião o mundo, p. 180.
243 Top Level Telecommunications, The US classification system.
244 BALL, James, NSA stores metadata of millions of web users for up to a year, secret files show.

Esta PIIC começou a ser pensada após os ataque de 11 de setembro de 2001, mas só a partir de 2013 se começou a verificar a sua real implementação, com Workshops da PIIC.[245]

Atualmente, *" ... o Secretário-geral do SSI é o órgão de natureza executiva, com competência decisória, em diversos níveis (...) coordenação (...) direção (...) controlo (...) comando operacional ...* ".[246] Já o Gabinete Coordenador de Segurança – GCS é o órgão especializado de assessoria e consulta para a coordenação técnica e operaciona[247], criando-se assim condições para uma melhor interoperabilidade entre as FSS, através de mecanismos de cooperação importantes, como a Plataforma para o Intercâmbio de Informação Criminal (PIIC), o Ponto Único de Contacto para a Cooperação Policial Internacional e a melhoria da operacionalização da Unidade de Coordenação Antiterrorismo (UCAT), entre outros.

Segundo Antero Luís, *"... Inicialmente, 300 analistas vão poder estar, ao mesmo tempo, a fazer pesquisas na PIIC, mas a plataforma vai ter capacidade para que 3.000 possam fazer consultas em simultâneo (...) o sucesso da plataforma vai depender dos sistemas de informação dos Órgãos de Polícia Criminal (OPC). "Quanto melhor forem os sistemas de informação dos OPC, melhor será o resultado final da plataforma",* sustentou Em matéria de investigação, a plataforma deteta toda a informação, mesmo aquela que está em segredo de justiça. Nestes casos, os OPC podem aceder à informação sempre que forem autorizados por um magistrado do Ministério Público ou juiz de instrução.[248]

Esta PIIC é supervisionada pelo conselho de fiscalização, composto por elementos de todos os OPC e do gabinete do secretário-geral do SSI, e pela Comissão Nacional de Proteção Dados (CNPD).

A interoperabilidade de informações não se faz somente através da utilização da PIIC, pois existe bastante diversidade de cooperação bilateral entre muitas instituições Estatais, entre outros, o Sistema de Informação de Schengen (ver Fig. 6), a título de exemplo, a Cooperação entre a PJ, a Direção-Geral dos Impostos e a Direção-Geral das Alfândegas e dos Impostos Especiais, que cria condições de acesso e análise, em tempo real, da informação pertinente para a investigação dos crimes tributários pela Polícia Judiciária e pela administração tributária.[249]

245 Workshop da PIIC – Plataforma de Intercâmbio de Informação Criminal, Consultado em 30 de maio de 2018, http://www.amn.pt/Media/Paginas/DetalheNoticia.aspx?nid=65

246 In Direito da Segurança, p. 569, ss.

247 Artigo 21.°, n.°1, da Lei 53/2008 de 29 de agosto – Lei de Segurança Interna

248 Consultado em 30 de maio de 2018, In https://www.jn.pt/seguranca/interior/plataforma-de-partilha-de-dados-de-policia-criminal-arranca-em-marco-3035682.html

249 "1 – A troca de informações efetuada (...) processa-se através do Grupo Permanente de Ligação." Artigo 4.° do Decreto-Lei n.° 93/2003 de 30 de abril.

3.16 O ESTRATEGO ANALISTA DE INFORMAÇÕES

O estratego analista de informações desenvolve nas informações o trabalho operacional e também a estafa documental. O estratego efetua a sua análise de dois modos: Passivo (Processamento de dados) e Ativo (Produção de Relatórios). A produção de relatórios requer a criação de cenários de forma a fomentar uma indagação criativa.

A metodologia do estratego analista tem *"... cerca de 50 técnicas e tipos de relatórios de análise"*. [250] A análise na sua arquitetura tem como reação aos modelos a Teoria na aquisição de conhecimento, a observação dos núcleos de poder e de fatores-chave.

Os relatórios (cenários) tendem entre o "MUITO PROVÁVEL" e o "IMPROVÁVEL", tendo em conta a possibilidade (probabilidade) de cenários e subcenários. Os relatórios devem ser precisos e escritos de forma descomplicada, incluir conceitos técnicos e representações limpas intuitivas e céleres. Já os relatórios especiais, segundo Pedro Graça, devem ser *"... mais extensos, para enquadrar assuntos novos e/ou complexos."* [251]

Nasce assim o *"empowerment"* que frui do *Intel*.

As entrevistas aos analistas visam condensar a apreciação autêntica dos vários analistas de informações dos vários OPC a todo o sistema em rede para que se possa academicamente fazer uma análise aos factos (prós e contra) sentidos pelos operacionais do terreno.

QUADRO RESUMO **DAS ENTREVISTAS EM %**			
ÁREAS CLASSIFICADAS			
SEGURANÇA DAS TECNOLOGIAS DA INFORMAÇÃO			
MEDIDAS DE DESEMPENHO	SIM	NÃO	N/A
A proteção das informações classificadas é adequada em função da classe de segurança a que cada pertence?	0	100	0
Existe controlo de acesso às Tecnologias da Informação?	100	0	0
Existe uma política de recolha de documentos classificados no final do dia de	0	100	0

250 Conforme descreve Pedro Borges Graça in *Metodologia da Análise nas Informações Estratégicas*, p. 435, ss.
251 Idem

serviço?			
O Sistema das Tecnologias da Informação possui controlo fora do horário de serviço?	0	100	0
O Sistema está organizado por camadas com os regulamentares graus de segurança consoante a matéria classificada existente?	100	0	0
	40	**60**	**0**
ÁREAS CLASSIFICADAS			
SEGURANÇAS DAS TECNOLOGIAS DA INFORMAÇÃO			
PROCEDIMENTOS			
MEDIDAS DE DESEMPENHO	SIM	NÃO	N/A
O acesso às Tecnologias da Informação é alterado com frequência (6 em 6 meses)?	100	0	0
Existe uma relação nominal do pessoal autorizado (código)?	100	0	0
Existe um registo de abertura (GDH, identificação e rubrica)?	0	100	0
Existe um registo de existências?	0	100	0
Existe um indicador de aberto/fechado?	0	100	0
	40	**60**	**0**
ÁREAS CLASSIFICADAS			
ARMÁRIOS E FICHEIROS			
ROBUSTEZ/PROCEDIMENTOS			
MEDIDAS DE DESEMPENHO	SIM	NÃO	N/A
Possuem condições de segurança de acordo com os regulamentos em vigor em concorrência com a matéria que guardam?	0	100	0
As chaves (código) estão apenas na posse de um responsável?	0	100	0
As chaves (código) são entregues no final do serviço ao responsável pelo chaveiro (com assinatura do livro de entrega/receção)?	0	100	0
	0	**100**	**0**
TRATAMENTO DO MATERIAL CLASSIFICADO			
GENERALIDADES			
PROCEDIMENTOS			
MEDIDAS DE DESEMPENHO	SIM	NÃO	N/A

O custódio/informático é conhecedor de todos os procedimentos inerentes ao tratamento de material classificado?	100	0	0
	100	**0**	**0**
TRATAMENTO DO MATERIAL CLASSIFICADO			
RECEÇÃO DE DOCUMENTOS			
PROCEDIMENTOS			
MEDIDAS DE DESEMPENHO	SIM	NÃO	N/A
Existe uma norma que regule o fluxo de receção de todos os documentos classificados?	0	100	0
Existe uma entidade autorizada para abrir a correspondência MUITO SECRETO?	0	100	0
Existe uma entidade autorizada para abrir a correspondência SECRETO?	100	0	0
Existe uma entidade autorizada a abrir a correspondência CONFIDENCIAL?	100	0	0
	50	**50**	**0**
TRATAMENTO DO MATERIAL CLASSIFICADO			
REGISTO DE ENTRADA/EXPEDIÇÃO /ENCAMINHAMENTO DE DOCUMENTOS			
PROCEDIMENTOS			
MEDIDAS DE DESEMPENHO	SIM	NÃO	N/A
Existe um responsável pelo registo de entrada e expedição de documentos/informações?	100	0	0
O responsável é conhecedor da norma superiormente aprovada para a elaboração do registo de entrada e expedição de documentos/informações?	100	0	0
O seu encaminhamento é controlado através de Protocolo/Folha de Circulação/Certificado de Transferência?	0	100	0
	66	**33**	**0**
TRATAMENTO DO MATERIAL CLASSIFICADO			
MANUSEAMENTO/ARQUIVO DE DOCUMENTOS			
PROCEDIMENTOS			
MEDIDAS DE DESEMPENHO	SIM	NÃO	N/A
Existe uma norma que identifique a entidade que autoriza o seu manuseamento?	100	0	0

Interno	100	0	0
Externo	0	100	0
Existe uma norma que identifique a entidade que autoriza o seu arquivo?	0	100	0
É verificado e encerrado o Protocolo/Folha de Circulação aquando da entrega para arquivo?	0	100	0
Existe um registo atualizado de documentos arquivados?	100	0	0
Existem arquivos separados para documentos classificados de MUITO SECRETO, SECRETO e CONFIDENCIAL?	0	100	0
Existe nomeado um responsável pela salvaguarda/manutenção do seu inventário físico?	100	0	0
Existe uma relação nominal de pessoas com acesso ao arquivo?	100	0	0
	60	**40**	**0**

Figura 9 – Quadro resumo das entrevistas a analistas de informações.

SELEÇÃO DA AMOSTRA E ANÁLISE DE DADOS

O contexto e o detalhe das visões antagónicas dadas na entrevista, foram apresentados com imparcialidade, com os múltiplos pontos de vista em evidência, para melhor clarificar a verdadeira situação e analise critica em forma de resumo as ocorrências mais relevantes.

Todas as entrevistas apresentam-se de forma anónima, assim sendo para a Tese os dados mais relevantes são os seguintes:

- 60% dos analistas dizem que não há segurança nas TI;
- 60% dos analistas dizem que não há segurança de procedimentos;
- 100% dos analistas dizem que a robustez não é suficiente;
- 100% dos analistas conhecem os procedimentos sobre as matérias classificadas;
- 50% dos analistas dizem que o fluxo de informação é suficientemente controlado;
- 66% dos analistas dizem que é confiança na expedição;
- 60% dos analistas dizem que a robustez do armazenamento/arquivamento é suficiente.

Relembramos que ainda sobre a temática dos analistas fica também explanada a insuficiência legislativa, ainda que constantemente alterada a Lei n.º 30/84, de 05/09. Estas alterações revelam-se

parcamente insuficientes para uma boa sustentação jurídica das informações, bem como insuficiente possibilidade de conduta positiva dos seus analistas.[252]

252 *Artigo 4.º Delimitação do âmbito de atuação 1 - Os funcionários ou agentes, civis ou militares, dos serviços de informações previstos na presente lei não podem exercer poderes, praticar atos ou desenvolver atividades do âmbito ou competência específica dos tribunais ou das entidades com funções policiais. 2 - É expressamente proibido aos funcionários e agentes, civis ou militares, dos serviços de informações proceder à detenção de qualquer indivíduo ou instruir processos penais.*

Artigo 5.º Acesso a dados e informações 1 - Os funcionários e agentes, civis ou militares, que exercem funções policiais só poderão ter acesso a dados e informações na posse dos serviços de informações desde que autorizados por despacho do competente membro do Governo, sendo proibida a sua utilização com finalidades diferentes da tutela da legalidade democrática ou da prevenção e repressão da criminalidade. 2 - O funcionário ou agente, civil ou militar, que comunicar ou fizer uso de dados de informações com violação do disposto no número anterior será punido com prisão até 3 anos, se pena mais grave não lhe for aplicável, independentemente da medida disciplinar que ao caso couber. Lei n.º 30/84, de 05 de Setembro - Sistema de Informações da República Portuguesa.

CAPÍTULO 4. *INTELLIGENCE*: PROGRAMAS, MODELOS E SISTEMAS

SUBCAPÍTULO 1. DEFINIÇÃO

4.1.1 SISTEMAS E PROGRAMAS

Elucidar a definição de sistemas e programas informáticos atravessará primeiramente as definições encontradas nos dispostos legais. Assim sendo, um sistema informático é um dispositivo que executa programas.[253] Já a tão necessária definição de programa informático desapareceu do nosso ordenamento jurídico, que subsistiu entre 1991 e 2009 na Lei n.º 109/91 de 17 de agosto – Lei da Criminalidade Informática, esta última revogada pela Lei 109/2009 de 15 de setembro – Lei do Cibercrime, e que esclarecia que programa informático era as instruções inseridas numa máquina.[254]

Ora, se a base das Tecnologias da Informação são os computadores, como poderia ter sido sonegada a indispensável definição de programa informático do nosso ordenamento jurídico, mais ainda quando o Relatório Anual de Segurança Interna – RASI nos diz que a criminalidade informática subiu 21,8% e que *"Os crimes informáticos mantêm a tendência de subida."* [255]

	Arguidos constituídos		Detidos		Prisão preventiva	
Tipo de crimes	Ano 2016	**Ano 2017**	Ano 2016	**Ano 2017**	Ano 2016	**Ano 2017**
Acesso ilegítimo ou indevido	39	**43**	3	**1**	0	**0**
Intercepção ilegítima	0	**1**	0	**0**	0	**0**
Burla informática e nas comunicações	330	**367**	31	**26**	3	**8**
Viciação/Dano relativo a dados ou programas informáticos	0	**2**	0	**0**	0	**0**
Devassa por meio informático	8	**5**	1	**0**	0	**0**
Falsidade informática	16	**25**	0	**0**	0	**0**
Reprodução ilegítima de programas protegidos	5	**4**	0	**0**	0	**0**
Sabotagem informática	4	**3**	0	**0**	0	**0**

Figura 10 – Análise dos Inquéritos – arguidos constituídos, prisão preventiva e detidos.[256]

Estes dados poderão ser facilmente atrapalhados, pois os crimes de burla informática ou de pornografia, entre outros, podem ser incluídos também noutras classificações por serem crimes comuns que podem ser praticados com recurso à tecnologia informática.

4.1.2 BIG DATA E O INTELLIGENCE (MATRIX)

253 *«Sistema informático», qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção,* alínea a) do Art. 2.º da Lei n.º 109/2009 de 15 de setembro – Lei do Cibercrime.

254 *Programa informático - um conjunto de instruções capazes, quando inseridas num suporte explorável em máquina, de permitir à máquina que tem por funções o tratamento de informações indicar, executar ou produzir determinada função, tarefa ou resultado,* alínea c) do Art. 2.º da Lei 109/91 de 15 de setembro – Lei da Criminalidade Informática.

255 In Relatório Anual de Segurança Interna (2017), p. 32.

256 In Relatório Anual de Segurança Interna (2017), p. 31.

O Big Data tem especial relevo na sociedade atual pelo armazenamento de grandes dados a grande velocidade e que hoje edifica em grande parte a comunidade humana informático-digital, operando com grande flexibilidade toda a informação. Assim uma disforme "vitrificação"[257] de dados poderá causar uma incerteza social dos valores a defender, Segurança em detrimento da Privacidade ou vice versa.

A violação do bem jurídico da reserva da vida privada pede uma reflexão profunda e especial na construção qualitativa da sua profanação ou da simples ameaça da violação deste, assim, tem sido o comportamento do Intel, mais propriamente na devassa por meio informático.

Pelo que o legislador legitimou restringir o domínio de procedimentos danosos criando um tipo legal de crime Art. 193.º do CP [258], onde o legislador restringe os ficheiros de dados individualmente identificáveis e relativos a convicções políticas, religiosas ou filosóficas referentes também a filiações partidárias ou a sindicalismos, à vida privada ou origem étnica.

Quanto à legislação especial, refere-se a Lei n.º 109/2009, de 15 de setembro, que aprova a Lei do Cibercrime, que transpôs para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativo a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, onde no seu art. 12.º possibilita a obtenção e armazenamento de dados informáticos num sistema, incluindo o tráfego, quando seja necessária a produção de prova decorrente de um processo. Ora, aqui teremos um problema juridicamente imposto aos SI devido ao conceito e formas de produção de informação, pois, o legislador refere que só poderão ser preservados de forma expedita dados "Se no decurso do processo..." [259] — quando se fala em processo o legislador quis transmitir a ideia de processo penal, mais quando no n.º 2 do art. 12º da LC , se obrigam os órgãos de polícia criminal a transmitir o relatório (resumo das investigações levadas a cabo) previsto no artigo 253.º do CPP.

Assim, fica juridicamente claro que a LC deixa de fora o Intel, bem como os SI, no que concerne à preservação expedita de dados.

Perante este facto normativo, facilmente se compreende que a reserva da vida privada e a intimidade (devassa por meio informático) só poderão ser triturados pela investigação criminal.

257 A apelação a um ponto de equilíbrio entre o público e o íntimo, COSTA, José, *Direito Penal da Comunicação*, 1998, p. 67.

258 1 - Quem criar, mantiver ou utilizar ficheiro automatizado de dados individualmente identificáveis e referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada, ou a origem étnica, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias. 2 - A tentativa é punível.- Devassa por meio de Informática.

259 Art. 12.º da Lei N.º 109/2009 de 15 de setembro.

Considerando que a intimidade é quando «o eu», para se desenvolver harmonicamente, crie espaços onde o «outro» só pode penetrar quando aquele, o «eu», em atitude de autorrealização, o permita."[260]

Aderindo a este conceito de "autorrealização" há então que estabelecer a separação do espaço físico propriamente dito, do privado e do público, (Ver nota de rodapé 202).

Neste último, incluo as redes sociais como fontes abertas (Ver em 3.6) dos «eu`s» onde a inexistência de privacidade impera.

Quanto ao Big Data e ao Intel, a autoridade judiciária pode ordenar a quem tenha disponibilidade e controlo, designadamente ao fornecedor de serviço, que preserve os dados, conforme previsto no art 12.º da LC.[261]

Relativamente ao *Intelligence*, a NSA, desde 2008, que levava a cabo, no Afeganistão e no Iémen, ataques por Drones tendo por base 60% das informações operacionais pela interceção de dados (mensagens e geolocalização) de suspeitos. Esse dispositivo dava pelo nome "Disposition Matrix" e tinha a listagem de pessoas a eliminar.[262]

A NSA depende em muito da autorização da FISA, mas essa autorização pode ser renovada todos os anos e referente a uma "... autorização de recolha global ..."[263]. Nesta matéria também a NSA, tal como os nossos |Portugueses| Serviços de Informações foi considerada *"... incapaz de coordenar os seus softwares (...) 1935 interseções legais (Reasonable, articulable suspicion), contra 15.900 ilegais ..."*.[264]

A própria NSA interceta, através de um programa que dá pelo nome de Muscular, *"... seus dados através da pirataria das suas redes de fibra ótica privadas (...) intercetando 181280466 trocas nos servidores da Yahoo!, e da Google ..."*.[265]

Também o GCHQ criou um programa de vigilância da Internet e das comunicações, intercetando, armazenando e vigiando em tempo real, e que dá pelo nome de Mastering the Internet – MTI.[266]

260 José Costa escrutinando o conceito de intimidade, p.70.
261 Pedro Dias Venâncio em *Lei do CiberCrime: Anotada e comentada* argui que podem ser dados informáticos, tais como, documentos eletrónicos, programas de computador, dados pessoais, dados de tráfego ou dados de localização, p. 98.
262 In *O Caso Snowden*, p. 162.
263 Idem, p. 184, ss.
264 Idem.
265 Idem, p. 187.
266 Idem, p. 209.

4.1.3 BUSINESS INTELLIGENCE

> *"Também está preocupado com a coleta de grandes quantidades de dados pessoais por empresas privadas e com o risco de que esses dados possam ser acessados e utilizados para fins ilegais por atores estatais ou não estatais. Neste contexto, deve ser sublinhado que as empresas privadas devem respeitar os direitos humanos nos termos da Resolução 17/4 sobre direitos humanos e empresas transnacionais e outras empresas comerciais, adoptada pelo Conselho dos Direitos Humanos das Nações Unidas em Junho de 2011".* [267]

As Tecnologias da Informação também prosseguem na área da economia e empresarial, e porventura estas áreas serão as que congregam os maiores investidores nas inovações tecnológicas (Intel), mais quando o andamento geral da atividade económica gera grandes impulsos sociais.

Assim sendo, os principais efeitos disso são os seguintes:

> *"1) a inconsciência das perceções; 2) a volatilidade dos comportamentos; 3) a sobrefocagem no imediato; 4) a incapacidade de visão estratégica; 5) o risco (acrescido) de erros de decisão (mais ou menos gravosos); 6) a vulnerabilidade em termos de compreensão atempada de ameaças e/ou desatenção a novas oportunidades; e 7) sobretudo o risco de enfraquecimento ou eliminação da posição no mercado ..."* [268]

No que respeita aos campos de atuação estes delimitam-se dentro dos seguintes parâmetros:

> *"1) a questão das fontes a montante; 2) os modos de processamento; 3) a diferenciação nos procedimentos; 4) as razões empresariais para a utilização; 5) a questão das condições de financiamento; 6) a lógica teórica da atividade de informações na atividade económica; e 7) a explicitação da chave fundamental que a informação estratégica constitui."* [269]

---

267 Resolution 2045 (2015) *Mass Surveillance*, Dot 6. Parliamentary Assembly – Council of Europe.
268 In, Informações e Segurança, p. 222, ss.
269 Idem, p. 226.

O Intel serve então para melhor alicerçar e aprontar a atuação do Business fazendo-o prosseguir nas suas conveniências (económicas) e nos seus intuitos (enriquecimento).

4.1.4 WEB ANALITICS (MEDIA)

Analistas, investigadores, civis, militares e académicos de diversas áreas intervêm e dissecam intensamente a produção dos media na autêntica volumetria, ainda que tenham fortes limitações técnicas, logísticas e humanas. Estes intervenientes habitualmente trabalham com base em informações em segunda mão, analisando-as muitas vezes em tempo real e esbarrando por vezes com conveniências e óticas divergentes.

Os *"... avanços tecnológicos (...) |abrem| novas oportunidades, mas |geram| igualmente outras limitações e instrumentos de manipulação."* [270]

Assim, analistas, investigadores, civis, militares e académicos têm de ponderar, confirmar e contextualizar todas as notícias, assim não sendo, poderão ser induzidos no engodo dos media muito pelas causas de lógica comercial/política muitas vezes orientadora dos media.[271]

As grandes fontes de informação[272] obtêm imediatamente um feedback e anotações dos intervenientes catalisando à partida todo o processo do pensamento crítico na medida em que não deixam espaço à valoração e à configuração de uma controvérsia.

Nos media tradicionais (rádio, TV) o recetor era somente isso, já nos media modernos (internet) o recetor é agora participante, emissor de opinião, e as suas atitudes são muitas vezes dúbias de justeza e oriundas de meadas políticas, pela escolha dos interesses a envolver na informação.[273]

Os media vivem hoje, mais do que nunca, da notícia impacto. Levando o recetor a respostas irracionais e emotivas. Também as pressões comerciais e políticas manipulam o recetor das mais diversas formas.

As Tecnologias da Informação são hoje veiculadores universais de informação ampliando a intensidade de interpenetrabilidade da informação, isto é, uma notícia aqui será veiculada nos mesmos moldes da veiculada em qualquer outra parte do mundo. Assim, surge a multiplicação de acontecimentos não confirmados deturpando muitas vezes os reais eventos, surgem similarmente as

270 Carlos Santos Pereira cita Katz dizendo que muitas vezes o Jornalista tem a função de intérprete, In *Informações e Segurança Media e Militares na Gestão de Conflitos Internacionais . Da Desconfiança à cumplicidade*, p. 203.

271 Já na década de 80 o Jornalista Francês François-Henri de Virieu apelidava o poder exercido por determinadas organizações da sociedade sobre os media de "mediacracia". In Jornal de Notícias de 02 de novembro de 2015, p.32.

272 "A CNN atinge (...) três por cento da população mundial – quatro quintos dessa população nem sequer tem acesso a um aparelho de televisão" , In *Informações e Segurança*, p. 207.

273 O grupo Anonymous declarou guerra |digital| à Al-Qaeda e ao estado islâmico após o ataque à redação do Charlie Hebdo, prometendo invadir os seu sites, "nós vamos encontrar-vos (...) a cada um de vocês e vamos matar-vos". Joana Marques Alves, Jornal Sol – Internacional, de 09 de janeiro de 2015.

mensagens mediáticas pré-fabricadas dos poderosos, numa promiscuidade institucional obtendo assim uma consonância homogénea da informação fornecida, como tal, não garantindo a multiplicidade de informação nem diversidade informacional.[274]

4.1.5 SISTEMAS DE INFORMAÇÃO GEOGRÁFICA

Os Sistemas de Informação Geográfica (SIG) são sistemas de informação auxiliares à tomada de decisão através da Geografia.

Os SIG permitem uma análise de forma muito eficaz, pois refletem num mapa os dados previamente recolhidos, esses dados podem ser representados sobre diferentes formas e conter elementos diferenciados convergentes ou divergentes entre si, dependendo do modo como o seu utilizador os queira ver representados, mais ainda, os SIG tem a capacidade de fazer interagir os diferentes elementos entre si.

> *"Num SIG, a informação sobre o mundo real é armazenada na forma de um conjunto de camadas temáticas ligadas pela Geografia e que contêm elementos semelhantes, como redes viárias, ferroviárias e de telecomunicações, infraestruturas de saneamento e de abastecimento de água ou eletricidade, os espaços verdes e equipamentos coletivos."* [275]

Assim, as representações de padrões e tendências podem ser mais facilmente percecionadas pelo utilizador/gestor para supor antevisões económicas, sociais ou culturais, e então, antecipar os futuros fenómenos comportamentais que serão adotados por humanos.

A inteligência artificial é assim uma das formas contemporâneas *"para as organizações compreenderem o nosso mundo"*, foi assim que Rui Sabino, CEO da Esri Portugal, descreveu a missão dos sistemas SIG quanto à sua utilização por parte da sociedade.[276]

Quanto ao Geoprocessamento, os SIG são coletas de informação sobre a distribuição geográfica de recursos, levados a cabo pelos conhecimentos da matemática e computacionais entre as

274 José Manuel Diogo, especialista em Media Intelligence, diz que "depois de um acontecimento se tornar mediático, ou viral, como agora se diz, os seus protagonistas serão afetados por ele para sempre." In, Jornal de Notícias de 02 de novembro de 2015, p. 32.
275 Sistemas de Informação Geográfica pela empresa ESRI Portugal, no dossiê especial do Jornal Expresso da edição n.º 2239 de 26 de setembro de 2015.
276 Idem.

áreas da cartografia, análise de recursos naturais, transportes, comunicações, energia e planeamento urbano e regional. Os SIG permitem assim análises complexas.

Quanto aos tipos de dados, estes podem ser temáticos, cadastrais, de redes, de modelos numéricos de terreno (altimetria, projetos de estradas e barragens, declive e exposição), imagens (satélites, fotografia aéreas ou scanners).

Relativamente à tecnologia e à sua visão geral, as grandes tecnologias do SIG são:
GIS desktop, com interfaces amigáveis e crescente funcionalidade; Gerenciadores de dados geográficos, que armazenem os dados espaciais em ambiente multiusuário;
Componentes GIS, ambientes de programação, que fornecem insumos para que o usuário crie o seu próprio aplicativo geográfico; Servidores Web de dados geográficos, utilizados para publicação e acesso a dados geográficos via internet.

Os benefícios da utilização de SIG potenciam todos os setores de atividade e conectam de forma aguerrida a probabilidade à probabilidade posteriori.

Pelo que o conhecimento geográfico estará então cada vez mais à disposição da sociedade e em permanente interação com a atividade humana, integrando a sociedade como um todo.

4.1.6 SOCIAL NETWORK INTEL (AGATHA)

O Intel no segmento social é extraordinariamente intrincado e de organização mínima o que torna o Intel no domínio social mais penoso e mais original podendo levar a lapsos consideráveis.

A Social Network tem um resultado efetivo e outro aparente.[277] Este segmento leva a desvios pela impossibilidade de uma apreciação em circunstâncias razoáveis.

A sociedade digital subordina-se de redes eletrónicas e aos processos informatizados, expondo-se assim às atividades criminosas.

O cibercrime não tem fronteiras e pode ser classificado em três grandes grupos:[278]
- Crimes específicos da Internet: tais como, ataques contra os sistemas de informação ou *phishing* (por exemplo, sites bancários falsos de forma a aceder às contas bancárias das vítimas).
- Fraude e Falsificação online: esquemas de fraude em grande escala podem ser cometidos online através de instrumentos como o roubo de identidade, *phishing, spam* e código malicioso.

277 Ernâni Rodrigues Lopes apelidou-o de "Image Building" em Informações e Segurança, p. 224.
278 In http://www.poci-compete2020.pt/noticias/detalhe/Proj-18022-Agatha

- Conteúdo online ilegal: inclui material de abuso sexual de menores, incitação ao ódio racial, incitamento de atos terroristas e glorificação da violência, terrorismo, racismo e xenofobia.

Entre as práticas que suscitam maior preocupação, envolvendo crime organizado, encontram-se o tráfico de mercadorias e animais, ou mesmo a formação de redes complexas e bastante organizadas para tráfico de seres humanos e a distribuição de pornografia ilegal, incluindo a pornografia infantil. Ultimamente, os atos de terrorismo reivindicados por organizações transnacionais, com reconhecido desempenho político, económico e religioso, apresentam uma organização complexa e de muito difícil controlo.

As Tecnologias da Informação têm criado novas formas de interação e comunicação social, comunicações estas que poderão ser camufladas passando assim inobservadas. O Estado tem então de criar e adaptar novas ferramentas com a habilidade de fiscalizar e prevenir o crime, e também alguns excessos que podem ser meramente considerados ilícitos, tais como, o abuso de posição dominante.279 Este tipo de ilícitos é praticado em todo o mundo, a título de exemplo, na Alemanha onde *"... trade officers are collecting economic intelligence through open-source analysis."* [280]

Assim nasce o projeto "AGATHA" - Sistema inteligente de análise de fontes de informação abertas para vigilância/controlo de criminalidade, que é uma plataforma dirigida às polícias de investigação criminal e serviços de inteligência, facilitadora na recolha de indícios de práticas criminosas ao utilizar a informação disponível em fontes abertas, analisando-as automaticamente. Esta recolha incide sobre fontes de informação.[281]

O projeto "AGATHA" é um sistema que terá a capacidade de analisar grandes quantidades de informação e extrair dela relações implícitas, padrões e intervenientes, entre outros, através de módulos dedicados à análise de vídeo e imagem, áudio e texto em diversas línguas, compostos por algoritmos de *crawling and data mining*, para a recolha dos conteúdos de forma seletiva e direcionada.

Esta obtenção de dados - *web crawler*, criará cópias dos conteúdos a analisar e processar, indexando-os segundo o formato, fonte ou endereço, etc.. para otimização das pesquisas. Estes dados obtidos através do crawler serão guardados na sua forma original (dados Brutos) numa base de dados

279 O abuso de posição dominante é uma prática restritiva da concorrência que decorre da utilização ilícita por parte de uma empresa (ou de um conjunto de empresas, no caso de se tratar de posição dominante coletiva) do poder de que dispõe(m) num determinado mercado. In http://www.concorrencia.pt/vPT/Praticas_Proibidas/Praticas_Restritivas_da_Concorrencia/Abuso_de_posicao_dominante/Paginas/Abuso-de-posicao-dominante.aspx

280 Operations security (OPSEC) Intelligence Threat Handbook, In https://fas.org/irp/nsa/ioss/threat96/part02.htm

281 Consideram-se fontes de informação: as redes sociais, fóruns, imagens, informação da blogosfera e demais fontes de informação presentes na web, incluindo fontes de áudio e vídeo. In http://www.poci-compete2020.pt/noticias/detalhe/Proj-18022-Agatha

dedicada/repositório. Serão ainda criadas duas bases de dados adicionais, numa das quais será guardada a mesma informação, mas na forma normalizada, e na outra os dados resultantes da análise de conteúdos efetuada aos dados.[282]

O projeto "AGATHA" - Sistema inteligente de análise de fontes de informação abertas para vigilância/controlo de criminalidade, representará deste modo uma mais-valia fundamental para as equipas de investigação criminal ao criar esta plataforma, que deverá:[283]

- Suportar análise multilingue colaborativa de conteúdos audiovisuais e informações biométricas, através da aplicação de metodologias de *Visual Analytics* e tecnologias de *data mining*;

- Integrar tecnologias de base de dados ETL (Extract, Transform and Load), modelação semântica e *machine learning* de forma a explorar os vários dados a serem recolhidos.

De modo a que o seu desenvolvimento se baseie na:

- Aquisição de dados: recolha de informação a partir de fontes abertas, através de algoritmos de *crawling, data mining* e ferramentas de ETL;

- Análise de vídeo e imagem: extração de características de ficheiros de vídeo, a delimitação automática de momentos e cenas, deteção de padrões e respetiva segmentação;

- Análise de áudio e voz: desenvolvimento de tecnologias com capacidade de obter, automaticamente, informações a partir de fontes de dados de áudio recolhidas pelo módulo de aquisição de dados;

- Análise biométrica: extração de modelos de face 3D de alta qualidade com origem em ficheiros de vídeo de baixa qualidade, que serão depois utilizados para obter imagens 2D desses rostos para aplicações de reconhecimento facial com foco especial para utilização forense. Será explorada a biometria de voz. Conjugados os dois classificadores (identificação de rosto e de voz), o erro inerente a cada uma das técnicas de identificação é minimizado;

- Análise de texto multilíngue: tradução automática para utilização de informação em diferentes línguas, bem como técnicas de processamento de língua natural (NLP) para extrair conhecimento de forma automática.

---

282 Este é um projeto de investigação estratégico para a Compta BS, inserido no desenvolvimento de competências na vertente de Segurança da Sociedade em que estamos ativamente envolvidos. O projeto Agatha foi apoiado pelo COMPETE 2020 no âmbito do Sistema de Incentivos à Investigação e Desenvolvimento Tecnológico Empresarial na vertente de Co-promoção, com um Investimento elegível de 2.354 mil euros o que resultou num Incentivo FEDER de 1.386 mil euros. Para a implementação do projeto estabeleceu-se um consórcio liderado pela Compta Business Solutions, S.A. – (empresa de inovação tecnológica); Voiceinteraction S.A. – (empresa de base tecnológica); Associação C.C.G. – (entidade qualificada pelo Sistema Científico e Tecnológico Nacional (SCTN) para a Prestação de Serviços de Investigação e Desenvolvimento Tecnológico e para Consultoria e Serviços de Apoio à Inovação às empresas); Universidade de Évora | Centro de Inovação em Tecnologias da Informação (CITI) - unidade interdepartamental da Escola de Ciências e Tecnologia da Universidade de Évora, traz ao consórcio competências na área das Interfaces e Sistemas de Processamento de Língua Natural. É de realçar que os recursos alocados possuem vasta experiência no desenvolvimento de projetos nas áreas da inteligência artificial, recuperação de informação, análise de sentimentos e web semântica.

283 In http://www.poci-compete2020.pt/noticias/detalhe/Proj-18022-Agatha

- Classificação e segmentação semântica: segmentação e indexação dos conteúdos permitirão maior facilidade de navegação no conteúdo e o cruzamento de informação entre as diferentes bases de dados e repositórios.

- Base de Dados e Repositórios: armazenar numa Base de Dados Estruturada toda a informação proveniente dos diferentes módulos (áudio, vídeo, imagem, texto, biometria), devidamente indexada facilitará a sua referenciação e/ou correlação pelas restantes funcionalidades da solução a desenvolver.

- Gestão, organização e visualização de dados: definir regras para o processamento de pedidos de informação do utilizador, para recuperação da informação da base de dados do sistema, utilizando metodologias de pesquisa semântica, implementada através de uma componente de Visual Analytics (VA) que permitirá a análise visual de grandes quantidades de dados.

- Interface com o utilizador: desenvolver a interface de utilização que garanta todas as medidas de segurança que impossibilitem o acesso a utilizadores que não se encontrem devidamente credenciados.

É inequívoco que o projeto AGATHA ostenta um produto inovador ao nível tecnológico, acarretando consigo um auxílio às polícias de investigação criminal e serviços de inteligência, mas, não obstante toda essa inovação tecnológica, ao longo da elaboração deste capítulo, em momento algum conseguimos constatar a abordagem jurídica de tal projeto.

4.1.7 CRYPTO LAW SURVEY

A codificação de texto e/ou imagem através da programação criptográfica é crucial para o direito à privacidade e liberdade de expressão, mas este direito coadjuva paralelamente a dissimulação da criminalidade e dos comportamentos desviantes.

Este tipo de programação ao nível informático é efetuada de forma idêntica em todo o mundo, a grande diferença coloca-se nas distintas posições legais que cada Estado sustenta, ainda que a maioria dos Estados tenha adotado o Wassenaar Arrangement / COCOM (Coordinating Committee for Multilateral Export Controls). Este comité, formado por um conjunto de organizações internacionais, foi criado com o intuito, entre outros, de controlar o software criptográfico.

"O principal objetivo dos regulamentos do COCOM era evitar que a criptografia fosse exportada para países "perigosos" - geralmente, os países

pensavam em manter laços amigáveis com organizações terroristas, como Líbia, Iraque, Irã e Coréia do Norte. A exportação para outros países é geralmente permitida, embora os Estados muitas vezes exijam uma licença para serem concedidos. (...)

O COCOM foi dissolvido em março de 1994. Enquanto se aguarda a assinatura de um novo tratado, a maioria dos membros do COCOM concordou em princípio em manter o status quo, e a criptografia permaneceu nas listas de controle de exportação. (...)

O Acordo de Wassenaar controla a exportação de armas e de bens de dupla utilização, ou seja, bens que podem ser utilizados tanto para fins militares como civis; a criptografia é um bem de dupla utilização". [284]

Já o Conselho Europeu, nos seus regulamentos e leis internas, inclina-se tendencialmente para o processo criminal adotando a convenção 185 para o Cibercrime

"... Cada parte deve adoptar as medidas legislativas e outras que forem necessárias para habilitar as suas autoridades competentes a ordenar: a). uma pessoa no seu território para apresentar dados informáticos especificados na posse ou controlo dessa pessoa, que são armazenados num sistema informático de um suporte informático (...) As partes podem estabelecer obrigações que os dados informáticos especificados (...) devem ser produzidos da forma especificada na ordem. Isto poderia incluir referência (...) para formar, tal como que os dados ou informações sejam fornecidos em 'texto simples' ...". [285]

Esta convenção procedente do Conselho da Europa permite, mas não obriga, os Estados a adotarem o "desencriptamento", assim sendo, tudo terá de estar dentro das leis internas de cada Estado. No desenvolvimento da convenção, o Conselho da Europa tenta minimizar os efeitos negativos da Autópsia digital (Investigação Criminal) às Tecnologias da Informação, contudo, o uso da criptografia por parte dos criminosos, dificulta a restrição da Autópsia digital ao *"strictly necessary",*

284 Bert-Jaap Koops homepage - Crypto Law Survey Overview per country, In http://www.cryptolaw.org/cls2.htm
285 Idem

ainda mais quando as sucessivas recomendações não especificam as medidas a tomar ou o balanço entre *"conflict of interests between the needs of the users and law enforcement"*.[286]

Portugal foi um dos países que aderiu ao Wassenaar Arrangement mas, no que respeita à regulação das leis internas quanto à criptografia, Portugal não tem nenhuma, nem para a sua proibição, nem para a regulação.[287]

Em Portugal, jamais seria possível acontecer o que ocorreu nos EUA, onde se decretou a prisão de alguém indefinidamente pelo facto de se recusar a desencriptar o disco rígido.[288] A Convenção Europeia dos Direitos do Homem apresenta o direito a um processo equitativo,[289] concomitantemente, o princípio da presunção de inocência aparece na CRP salvaguardando a defesa da posição do arguido, em processo penal. A CRP garante um sistema acusatório no processo penal.[290]

286 Idem

287 In http://www.cryptolaw.org/cls2.htm

288 "On Monday, a US federal appeals court sided against a former Philadelphia police officer who has been in jail 17 months because he invoked his Fifth Amendment right against compelled self-incrimination. He had refused to comply with a court order commanding him to unlock two hard drives the authorities say contain child porn.", In https://arstechnica.com/tech-policy/2017/03/man-jailed-indefinitely-for-refusing-to-decrypt-hard-drives-loses-appeal/

289 "qualquer pessoa acusada de uma infração presume-se inocente enquanto a sua culpabilidade não tiver sido legalmente provada" art. 6° n° 2

290 "Todo o arguido se presume inocente até ao trânsito em julgado da sentença de condenação." art. 32° n° 2

SUBCAPÍTULO 2. PROGRAMAS

A programação, entre outros atributos, permite o rastreamento de dados de navegação do utilizador com ou sem o seu conhecimento, isto é, um programador mediano já o consegue fazer de forma invisível, supervisionando assim toda a sua atividade em torno da internet, tal como, a utilização do e-mail, os sites visitados, os fóruns, etc., traçando deste modo o perfil dos interesses, bem como os hábitos de consumo do internauta através dos cookies.

A título de exemplo, a lista de participantes na estrutura orgânica de um simples fórum pode ser tão numerosa que implica, logo à partida, um grande risco individual à liberdade dos seus intervenientes, esta estrutura engloba o utilizador, o editor, o fornecedor de alojamento do site, o fornecedor de acesso, e o respetivo operador de telecomunicações.

Se um fórum implica como que uma espécie de cadastro/pré-inscrição, já num blogue qualquer pessoa com acesso à internet pode consultar e partilhar informações que lá foram difundidas.

Quanto à recolha de dados de forma visível, um programador pode fazer um tracking ao IP, ou então pode recolher os dados através de uma simples mensagem que não recorra à criptografia, pois esta pode ser acedida por numerosos intermediários em virtude dos saltos entre servidores durante a transmissão da mensagem de A para B.

A globalização tem assim um papel reator na ciberestratégia, cibercomércio, cibergoverno, cibersaúde, ciberescola.

4.2.1 PROGRAMA 1: ECHELON

ECHELON

O Echelon é um dos programas mais devastadores da privacidade e da vida íntima, este instrumento de recolha de informação está cada vez mais aprimorado, quanto à sua interceção, registo e análise. O programa Echelon está também ao serviço do acordo UKUSA, dando assim a estes países o Hard Power no Intel global, como *"... são os e-mails e o tráfego cibernético, na net, via satélite, micro-ondas, celulares, por fibra ótica, em todo o planeta, (...) palavras-chave, ou de tipos de voz, destinatários em concreto como personalidades, números de telefone..."* [291]

291 Descrição técnica do programa Echelon narrada por Marques e Martins, in Direito da Informática, p. 44.

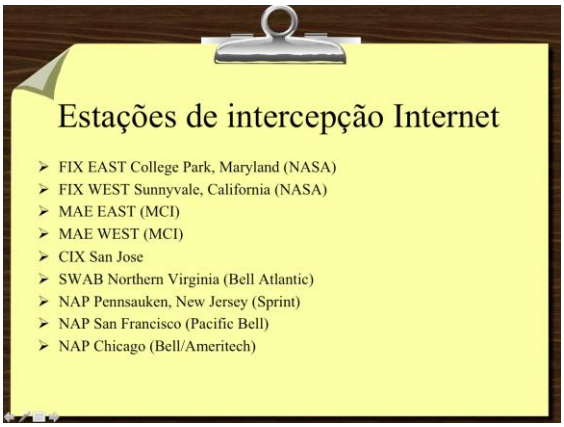

Figura 11 – Algumas das estações de interceção durante o ano dos ataque de 11 de setembro de 2001.[292]

Quem recolhe em grande parte a nossa (Portugal) informação é a Estação que fica situada em Menwith Hill, Yorkshire – UK, não obstante a estação do UK, outras estações poderão muito bem fazê-lo, e estas situam-se em: Geraldton, Austrália; Leitrim, Canadá; Etam, W Virginia, e em Morwenstow.

O Echelon colige as informações oriundas de satélites, Intelsat, feixes hertzianos, internet, rádio HF, redes de fibra ótica, cabos submarinos e das redes digitais.

O Echelon recolhe nomes, moradas, números de telefones, fax, telex sem qualquer mandato judicial.

> *"A provar-se o que consta destes estudos, trata-se duma situação muito grave. Porque estamos perante um organismo que escuta conversas, intercepta mensagens e viola direitos dos cidadãos sem mandato judicial nem controlo democrático e porque isso pode significar uma vantagem ilegal e condenável de alguns países no comércio internacional"* [293]

> *(2) O Secretário de Estado não emitirá um mandado sob esta secção, a menos que considere que o mandado é necessário:*
>
> *a) no interesse da segurança nacional*
>
> *b) com o objectivo de prevenir ou detectar crimes graves; ou*

292 Slide gentilmente cedido pelo Dr. Carlos Coelho, onde se vê a existência, pelo menos, de 9 estações de interceção de comunicações Internet da NSA, em território dos EUA.
293 O Sr. Eurodeputado Português Dr. Carlos Coelho Presidente do Comité Temporário sobre o sistema Echelon, após o relatório de Duncan Campbell.

c) com o objectivo de salvaguardar o bem-estar económico do Reino Unido [294]

Não obstante tudo o que acima foi descrito, uma interceção eficaz na Internet só é possível com a ajuda de entidades privadas, mais propriamente através de Prestadores do Serviço Universal ou Operadores.

Em Portugal, o Estado pode violar a privacidade das Comunicações, mas só mediante autorização/decisão judicial quando se trate do combate ao crime.

4.2.2 PROGRAMA 2: PRISM (WHISTBLOWER, XKEYSCORE, NAURUS, AMESYS, BLUE COAT)

Tem-se falado muito da militarização da Internet devido, especialmente, à hipervigilância em massa. A título de exemplo, programas como: Naurus, usado pela NSA; Amesys de patente francesa, usado pelo governo libanês; e Blue Coat, que monitoriza em tempo real o tráfego da internet sobre ameaças de segurança, sobretudo o tráfego encriptado, e que, só no Médio Oriente, fatura 2.8 milhões de dolares, [295]. Porém, o facto de a Blue Coat ser uma empresa Americana torna logo à partida ilegal o seu uso no Médio Oriente.

Já o Prism é a principal fonte de informações para a elaboração de relatórios de informações, a tal ponto que a *"National Security Agency e o FBI intercetam as informações das nove maiores empresas de internet (...) Microsoft, a Yahoo, a Google, o Facebook, a PalTalk, a AOL, o Skype, o YouTube e a Apple..."* [296]

Este Prism é um sistema em grande parte automatizado e de navegação simples, *"... o volume das informações (...) era tal que se tornava claramente impossível aos agentes da NSA analisarem todo o conteúdo..."* [297].

A XKeyscore, uma tecnologia usada para intercetar e rastrear o tráfego da internet, com grande capacidade, similarmente ao Prism, também é utilizada pela NSA. O XKeyscore permite à NSA fazer Autópsias Digitais mais refinadas a uma lista mais restrita que julgue conveniente. Este programa [298] *"Assenta numa rede de cerca de quinhentos servidores espalhados pelo mundo – incluindo a Rússia, a*

294 1985 UK: Interception of Communications Act
295 Palestra realizada no Chaos Communication Congress - To protect And Infect – The militarization of the internet, https://www.youtube.com/watch?v=Y1aU3uw1QnA
296 In *O Caso Snowden*, p. 50.
297 Idem, p. 187.
298 Idem, p. 190 e ss.

China e a Venezuela ..." [299], este sistema é alimentado pela SCS – Special Colletion Service, pela Fornsat – Foreign Satellite Colletion e pela SSO – Special Source Operations.

4.2.3 PROGRAMA 3: TRAILBRAZER

O programa Trailbrazer foi considerado *"... demasiadamente complexo, ruinoso e de atentar contra as liberdades ...",* a tal ponto que levou à expulsão, e posterior detenção pelo FBI, de dois altos responsáveis da NSA, William Binney e J. Kirk Wiebe, por discordarem desse programa.

O Trailbrazer é parte de um projeto chamado ThinThread. Este projeto tem, entre outras, a seguinte capacidade:

> *"...ThinThread, desenvolvido no final dos anos 90 para fornecer à NSA uma forma de peneirar o enorme volume de dados digitais que a agência poderia aspirar. (...)*
>
> *As pessoas por trás do ThinThread eram a coisa certa: eles incluíam dois funcionários de carreira, William Binney, um matemático, e J. Kirk Wiebe, um analista de comunicações. Um componente chave do ThinThread era a protecção da privacidade. O programa podia recolher dados domésticos, mas "anonimizava" nomes e outras informações de identificação com códigos de criptografia até que fossem recolhidas provas que justificassem um mandado para que os nomes pudessem ser revelados. (...)*
>
> *Mas havia uma disputa sobre a quantidade de dados que o programa poderia lidar, e anonimizada ou não, a coleta de dados domésticos sem um mandado é ilegal, aconselharam os advogados da NSA. Michael V. Hayden, que era então o novo director da NSA. (...)*
>
> *O ataque da Al-Qaeda mudou a conversa nacional sobre privacidade. De repente, a ênfase foi na detecção de enredos em vez de tentar garantir que a agência nunca espiasse os americanos, mesmo inadvertidamente..."* [300]

299 Idem, p. 192.
300 In http://www.washingtonpost.com/wp-dyn/content/article/2010/07/13/AR2010071305992_2.html??noredirect=on

4.2.4 PROGRAMA 4: EVILOLIVE

A NSA tem em seu poder programas de recolha de metadados[301] que monitorizam, entre outros, inúmeros estrangeiros, pois recolhe e analisa um número significativo de metadados. Os programas de recolha de metadados em massa, aparentemente, foram utilizados somente até 2011.

> *"Shawn Turner, diretor de comunicações da administração Obama para a Inteligência Nacional, disse ao Guardian que "o programa de coleta de metadados da internet autorizado pela corte da Fisa foi descontinuado em 2011 por razões operacionais e de recursos e não foi reiniciado".* [302]

Em 26 de dezembro de 2012, um novo capítulo nasce na NSA, aparece um novo sistema EvilOlive, este novo sistema consegue diretamente intercetar e armazenar o tráfego da internet.

> *"A NSA chamou-lhe a solução "One-End Foreign (1EF)". Pretendia o programa, codinome EvilOlive, para "alargar o âmbito" do que é capaz de recolher. Confiou, legalmente, na "Autoridade FAA", uma referência à Lei de Emendas Fisa 2008 que flexibilizou as restrições de vigilância.*
>
> *Este novo sistema, declarado pela SSO em dezembro, permite um aumento considerável da coleta pela NSA do tráfego de internet. "A solução 1EF está permitindo que mais de 75% do tráfego passe pelo filtro", diz o documento da SSO de dezembro. "Este marco não só abriu a abertura do acesso como permitiu a possibilidade de mais tráfego ser identificado, selecionado e encaminhado para os repositórios da NSA".*
>
> *E continuou: "Após a implementação do EvilOlive, o tráfego duplicou literalmente."* [303]

4.2.5 PROGRAMA 5: STELLAR WIND

O Stellar Wind foi criado em 2001. Este programa conduziu ao maior escândalo entre os EUA e as embaixadas europeias devido ao ato de espionagem levado a cabo pelos EUA a estes últimos.

---

301 Estes dados descrevem as características das comunicações interceptadas: remetente, destinatário, local de envio e de receção, duração da comunicação, endereço IP, etc.. In *O Caso Snowden*, p. 59.
302 https://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection
303 Glenn Greenwald and Spencer Ackerman, How the NSA is still harvesting your online data
In https://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection.

Sophia Veld, deputada no Parlmento Europeu, diz que *"Os nossos aliados não nos tratam como amigos, mas sim como suspeitos"* [304]

Já nessa altura se falava em conceber legislação sólida, relativa à proteção de dados individuais, que fosse semelhante à que os EUA oferecia aos seus cidadãos. Decorria o ano de 2008 e o Stellar Wind já era considerado, pelo Departamento de Justiça, um programa anticonstitucional, pois esmagava os princípios das liberdades individuais, pois o programa, através de um simples número de telefone, apoderava-se de todos os dados de um cidadão.[305]

4.2.6 PROGRAMA 6: UP STREAM

O Programa Up Stream medita sobre os fluxos da Internet que atravessa os cabos submarinos. Este programa é edificado por quatro estruturas: Fairview, Stormbrew, Blarney e Oakstar. Estas estruturas encontram-se nos pontos de chegada dos cabos de submarinos e são geridas nos "nós de rede", como tal, o volume de informação rececionado nestes é aterrador, o que impossibilita que os Sigad – Sigint Activity Designator[306] (analistas de informação) examinem todos os assuntos volvidos.

4.2.7 PROGRAMA 7: GLOBAL TELECOMS EXPLOITATION E MOBILE PROJECT

Este programa tem como técnica quase exclusiva a vigilância eletrónica sobre smartphones, pois 90% do tráfego da Internet tinha origem nos telemóveis.[307]

4.2.8 PROGRAMA 8: ORATORY

No laboratório encoberto de Beltsville, engenheiros de topo arquitetaram o programa Oratory, que tinha como função gravar a conversa das pessoas e, através de palavras-chave, selecionar e alertar o analista de informações. Este programa, tal como o Stellar Wind, esteve envolvido em escândalo, mas desta vez não nas Embaixadas Europeias, mas sim em oitenta residências diplomáticas norte-americanas, a título de exemplo, a Embaixada Americana em Roma escutou, durante dois meses, 4 milhões de metadados telefónicos italianos.[308]

304 In *O Caso Snowden*, p. 81.
305 Idem, p 152.
306 Em 2013 eram mais de 500 os Sigad, In *O Caso Snowden*, p. 169.
307 Dados internos do GCHQ para o período compreendido entre 2011-2012, p. 210.
308 In *O Caso Snowden*, p. 159.

Figura 12 – Resumo gráfico: serviços móveis 1.º Semestre 2018.[309]

4.2.9 PROGRAMA 9: TEMPORA

O programa Tempora é uma base de dados e um programa de vigilância eletrónica ao serviço, desde 2008, do GCHQ e da NSA. Este programa permite a espionagem de dados e metadados transmitidos pelos cabos submarinos de fibra ótica, sabendo nós que o Reino Unido tem estrategicamente colocado no seu território um hub, intercetando quase a totalidade do tráfego da Europa e da América do Norte. Onde se incluem também as correspondências eletrónicas através das redes sociais.

O Tempora permite armazenar conversas telefónicas durante 3 dias e metadados relativos a essas chamadas por 30 dias.

O programa Tempora é o *"maior programa de vigilância na história da humanidade"* [310]

309 In https://www.anacom.pt/streaming/STM1S18.pdf?contentId=1461982&field=ATTACHED_FILE

310 Segundo Edward Snowden o programa Tempora permite recolher diariamente cerca de 21 mil biliões de bytes, em *O Caso Snowden:* Como os EUA espião o mundo, p. 209.

SUBCAPÍTULO 3. MODELOS

A base estrutural da internet molda-se a cada passo da evolução do hardware e software, no avanço das tecnologias de informação e das suas máquinas e equipamentos.
Logo, também existem várias formas de utilização da respetiva base, tendo em conta que a precisão de cada objetivo é que irá definir o melhor modelo a utilizar para cada situação.

4.3.1 MODELO 1: PRIVATE WEB (BROWSERS, SERVERS)

O anonimato na Internet foi drasticamente reduzido com o surgimento das Redes Sociais e dos sites de domínio público que solicitam informações pessoais. A par disso, os motores de busca convencionais populares, como Google e Yahoo, armazenam a localização geográfica dos usuários para exibir os resultados. E há navegadores que armazenam informações dos usuários de várias maneiras.

Portanto, só através do uso do Browser em "modo anónimo" ou "nova janela anónima" de navegação privada é que poderemos pesquisar na Internet sem deixar para trás rasto do histórico, de senhas, de cookies e outras informações variadas, ainda assim, a dita privacidade não é total, pois, todos os conteúdos poderão ser armazenados pelos prestadores de serviço universal.

Também através de um servidor pessoal podemos configurar e administrar de forma privada, entre outros, sites e páginas dinâmicas, este método é muito usado para projetos piloto dos projetos de sistema com a capacidade de selecionar e publicar informações numa rede interna (doméstica).

4.3.2 MODELO 2: CONTEXTUAL WEB

Nos primórdios das pesquisas na web, era tudo uma amálgama de informação simplesmente de páginas HTML.

Atualmente, a contextualização da Web já não funciona assim, pois, agora a combinação dá-se por conexão de informações das condições impostas pelas pesquisas do usuário. Logo, a contextualização já não é ocasional, mas sim da troca entre pesquisa e oferta.

O motor de busca, hoje, evoluiu de tal forma, que reconhece o comportamento do usuário tentando transmitir-lhe no final sugestões mais significativas da sua pesquisa.

As principais propriedades da Web contextual são as seguintes: [311]

311 In, https://readwrite.com/2008/12/22/contextual_web/

"Relevância: compreender melhor o contexto do usuário impulsiona a relevância do conteúdo.

Atalhos: os atalhos contextuais reduzem a necessidade de pesquisa em bruto.

Personalização: o contexto é baseado nas intenções e no histórico do usuário.

Remixing: informação relevante de toda a web está disponível instantaneamente".

4.3.3 MODELO 3: CACHE

As instituições, cada vez com maior frequência, utilizam mais do que uma proxies para gerir a informação, entre elas, e entre funcionários, partilhando e autorizando a informação por camadas.

O uso de multi proxies capacita as instituições da utilização do modo inter-cache, isto é, um usuário de um servidor poderá ter acesso a informações contidas noutro servidor.[312]

312 Cache Array Routing Protocol (CARP)

SUBCAPÍTULO 4. SISTEMAS

Um sistema consiste num conjunto de engenhos computacionais capazes de processar informações de acordo com um programa, em geral, são compostos por dois tipos de elementos essenciais: hardware e software.

Hoje, as aplicações informáticas dão-nos uma oportunidade de variar a forma de comunicação através das Tecnologias da Informação, pois a sua simplicidade aliada a rapidez instantânea de instalação da aplicação mudam as vias de comunicação digitais, o que para uma Autópsia Digital se torna quase impossível e rocambolesco pelo emaranhado de vias a autopsiar. Pior ainda é o facto de as vias de comunicação digital mudarem de forma automática de linha através de impulsos eletrónicos, de segundo em segundo.

4.4.1 SISTEMA 1: TOR (DARK NET, DEEP WEB, I2P, BOTNET, ORBOT)

O sistema de navegação da Internet dispõe de um serviço Tor que não é mais do que um ocultador de identidade de pessoas ou organizações, pior é que algumas delas são criminosas e terroristas.

TOR

O Tor não é mais do que um browser da firefox que salta de nó em nó de rede e que utiliza essas ligações em rede de modo a deixar que a informação circule livremente, entre pontos, sempre sem comprometer a privacidade.

Esta impossibilidade de rastreamento do Tor funciona porque atua por camadas, o que dá a oportunidade de criação de conteúdos (blog, fóruns, etc.) sem que necessariamente se saiba a localização dos sites. O utilizador do Sistema Tor não é só composto por indivíduos Pró-sociais, nem criminosos, o Tor é utilizado também por Jornalistas e Organizações, existem até organizações que incentivam ao uso do Tor para que não haja rastreamento, pois torna-se uma segurança de confidencialidade, contra espionagem.

DARK NET

A Dark Net é uma pequena parte da internet profunda “Deep Web”, refere-se a sites com objetivo criminoso ou conteúdo ilícito, onde inclui também serviços, só que é uma rede mais fechada dentro da própria “Deep Web”, que é maior do que a internet superficial, a grande diferença é que não

tem uma fixação/identificação completa, o que torna quase impossível a identificação sem saber realmente a fonte. A mais valia da Dark Net é realmente o anonimato.

DEEP WEB

O termo Deep Web, para a PC Advisor, refere-se a todas as páginas da Web cujos mecanismos de pesquisa não se conseguem identificar, e abrange o que está nas camadas inferiores da internet. Grande parte da Deep Web é um mecanismo de pesquisa que não representa ameaças ao computador do usuário.[313]

I2P

O I2P, a par do Tor, também é uma rede anónima, composta igualmente por camadas descomplicadas. Os seus aplicativos comunicam de forma anónima e criptografada em quatro camadas.

O I2P é uma rede assente no *Internet Protocol*, mas possibilita a comunicação de mensagens sobreposta em *streaming*.

BOTNET

É um software malicioso que podem destruir um aparelho computorizado das mais variadas formas, algumas vezes o utilizador só dá conta posteriormente. Os piratas informáticos maioritariamente utilizam o que chamamos de Trojan "Cavalo de Tróia", organizando o Botnet num determinado conjunto de aparelhos computacionais infetados numa rede, que pode chegar com facilidade aos milhares.

Os piratas informáticos utilizam essa rede para espalhar vírus DDos, entre outros, para utilizá-la para os crimes, tais como, o *phishing*, ou roubo de dados de identidade, uma simples rede aberta pode conter *malware* transformando o aparelho computacional num Bot.

ORBOT

Orbot é uma aplicação Android, que serve para usar como uma proxy para o Tor, encriptando assim de forma mais robusta a identificação do remetente da comunicação.

313 In https://www.kaspersky.com.br/resource-center/threats/deep-web

4.4.2 SISTEMA 2: WEB CRAWLING

Web Crawling é uma forma mecânica que automaticamente controla a World Wide Web, indexando a rede por conteúdos ou por sites, como um *Bot*, assim, as sugestões de pesquisa irão aparecer consoante as percentagens de download. Isto é, o motor de busca irá sugerir ao utilizador um conjunto de sites provenientes de *Open Source* de acordo com a temática colocada.

4.4.3 SISTEMA 3: BACKLINKS

Os designados Backlinks ou links externos não são mais do que hiperligações que encaminham toda a pesquisa para o site que mais se apropria aos dados inseridos.

A Google e o seu motor de busca tem por base este sistema, que consoante os dados inseridos calcula os sites por relevância do conteúdo pelo relevo do site de origem. Portanto, quantos mais *backlinks* tiver, mais bem disposto ficará um site.

SUBCAPÍTULO 5. INFORMÁTICA

4.5.1 INFORMATION DASHBOARD

O Dashboard usa um interface ou página web para fazer um sumário, por norma em formato de gráfico onde, com um pensamento intuitivo do sistema 1, opera uma interpretação *"automática e rápida, com pouco ou nenhum esforço e sem sensação de controlo voluntário."* [314]

O Dashboard é muitas vezes usado também para demonstrar performances e é largamente utilizado em atividades cibernéticas como o propagandismo (ver em 4.5.11) .

4.5.2 USO DE BUFFERS OU OVERFLOWS

O Buffer é uma pequena memória, usado num local para instalar qualquer programa ou para execução de um processo, isto é, o Buffer serve como um input, e fica instalado no sistema do servidor do website.

O Buffer serve de "baliza" limitando tudo que excede esse Buffer, e que por norma dá um erro de sistema, caso esse erro não suceda passando automaticamente a ser um overflow.

Alguns dos ataque cibernéticos são usados através do uso de overflow até que o sistema desligue.

4.5.3 SECURITY

A segurança das Tecnologias da Informação necessita, logo à partida, de uma estratégia para a área da cibersegurança. Em Portugal, a oficina de ensaios recai no Instituto da Defesa Nacional, que tem a seu cargo o GECENI, na Autoridade Nacional de Segurança, que tem a seu cargo o CNC, e no Centro de Gestão da Rede Informática do Governo.

A informação terá assim de ser assegurada por uma política de domínio na convergência estrutural para balizar a segurança da informação, garantindo, assim, a investigação e o desenvolvimento tecnológico da sociedade da informação.

A cibersegurança e a ciberdefesa protegem e defendem as infraestruturas, garantindo a segurança das novas formas de interação e de relacionamento da evolução digital.

Como finalidade chegará sempre uma visão estratégica do domínio do ciberespaço, cujo intuito será o de fomentar e estimular a utilização das Tecnologias da Informação, assim, uma cooperação

314 O Prémio Nobel da Economia Daniel Kahneman, retrata muito bem esta forma de enganar o cérebro, no seu livro Pensar, depressa e devagar, p. 31.

internacional, afirmada ao nível jurídico, assegurará a proteção das instalações (redes) críticas e, subsequentemente, a proteção dos interesses nacionais e a confidencialidade da informação nessas mesmas redes.

> *"A Assembleia está profundamente preocupada com as ameaças à segurança da Internet pelas práticas de certas agências de inteligência, divulgadas nos arquivos Snowden, de buscar sistematicamente, usar e até mesmo criar "portas traseiras" e outras fraquezas nos padrões e implementação de segurança que poderiam ser facilmente exploradas por terroristas e ciberterroristas ou outros criminosos".* [315]

4.5.4 MALWARE: (STUXNET, FLAME, EUROGRABER, TROJAN, BOTNETS)

A amplificação do movimento no ciberespaço conduziu também ao aumento da sua aplicação de forma maliciosa, o que gerou em códigos como (vírus, trojans, criação e operação de botnets, etc.)[316] Este tipo de atividades traz consigo benefícios chegando a ultrapassar economias paralelas tais como o tráfico de cocaína e heroína.

4.5.5 TECNOLOGIAS

A tecnologia vai de mãos dadas com a atividade e com todo o progresso sociológico. Os críticos dizem que há um pendor exponencial de engrandecimento das tecnologias. Este engrandecimento leva-nos para o universalismo das tecnologias, assim sendo, impõe-se verificar as metodologias, a ética e a psicologia.

As situações tecnológicas (fotografia aérea, imagem de satélite, aparelhos de visão noturna, sensores, radares de deteção, entre outras) são áreas de interesse para o ganho de conhecimento e aumento do poderio de uma qualquer instituição.

Todas estas tecnologias são alimentadas por fontes diversas e toda a sofisticação tecnológica, quando ligada aos serviços que trabalham informações, fica à partida envolta em secretismo.

Quanto à evolução das tecnologias, no âmbito das escutas, dois dos Kamikazes que fizeram os atentados do 11 de setembro de 2001 trocaram chamadas entre si, mas, à data, a tecnologia não permitia indicar a proveniência da chamada.[317] Hoje, por seu lado, a tecnologia já pode, através de

315 Resolution 2045 (2015) *Mass Surveillance*, Dot 5. Parliamentary Assembly – Council of Europe.
316 Matéria relatada em *Estratégia de Segurança da Informação no Ciberespaço*, p. 13.
317 In *O Caso Snowden*, p. 147.

software, descodificar dados relativos à pessoa, o idioma também já não é um problema, e existem *"... softwares de interpretação por tipo de interceção: Lopers, para telefone fixo, Juggernaut, para telemóvel, bem como Drtbox, que reenvia os dados para recetores especializados."* [318]

Já quanto aos e-mails e busca de chamadas, temos os softwares Turmoil e Traffic thief, respetivamente.

A tecnologia evolui continuamente, assim como os projetos de engenharia, tais como: o Projest Wideband Extradiction, que interceta ondas longas; ou o Silkworth que vigia os rádios; o Moonpenny e o Steeplebush, que vigiam os satélites.

Figura 13 – Análise de Engenharia Informática a um correio electrónico com Trojan[319]

4.5.6 APP`S: (WHATSAPP)

A App é a abreviatura da palavra aplicativo, e as App`s não são mais do que programas que podem ser instalados em dispositivos digitais e que servem maioritariamente para comunicar ou executar uma tarefa. Ao caso, a grande diferença é que certas App`s comunicam (som e imagem) por encriptamento de mensagens, ao caso, o Whatsapp.

O Whatsapp é um serviço de troca de mensagens que labora numa e como uma estrutura teoricamente protegida de ciberespionagem.

> *"... o sistema de encriptação de mensagens do WhatsApp assenta na geração de chaves de segurança únicas através do protocolo Signal, desenvolvido pela Open Whisper Systems, que são depois trocadas e*

318 Idem, p. 191.
319 https://www.youtube.com/watch?v=Y1aU3uw1QnA , 10`35` `.

verificadas nas comunicações entre os utilizadores para garantir que as mensagens não são vistas por nenhum intermediário: apenas pelo emissor e o destinatário." [320]

4.5.7 SISTEMAS OPERATIVOS

O Sistema Operativo é um multitarefas que interliga o utilizador e o hardware garantindo que todas as soluções existentes no aparelho estão acessíveis.

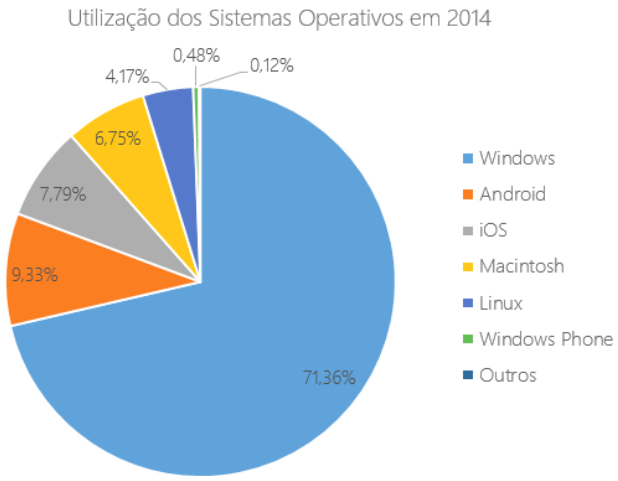

Figura 14 – Resumo gráfico: dos sistemas operativos mais utilizados.[321]

O sistema operativo gere todo o processo, gere a memória, germina recursos, cria ficheiros e assegura o tratamento de dados. O sistema operativo possibilita o aproveitamento máximo do equipamento de forma acessível e fiável.

4.5.8 SOCIAL NETWORK

As redes sociais são sítios virtuais onde existem relações de troca de comunicações de diversos conteúdos, cada rede social tem uma utilidade própria com o intento de um fim específico.

320 https://www.publico.pt/2017/01/13/tecnologia/noticia/whatsapp-mensagens-encriptadas-podem-ser-espiadas-1758170

321 https://pplware.sapo.pt/informacao/conheca-os-sistemas-operativos-mais-utilizados-em-2014/

Rede social	Característica
Facebook	Interação e expansão de contatos.
YouTube	Compartilhamento de vídeos.
WhatsApp	Envio de mensagens instantâneas e chamadas de voz.
Instagram	Compartilhamento de fotos e vídeos.
Twitter	Compartilhamento de pequenas publicações, as quais são conhecidas como "tweets".
Pinterest	Compartilhamento de ideias de temas variados.
Skype	Chamada de voz e vídeo.
LinkedIn	Interação e expansão de contatos profissionais.
Badoo	Relacionamentos amorosos.
Snapchat	Compartilhamento de vídeos curtos, tendo cada um o máximo de 10 segundos.
Messenger	Envio de mensagens instantâneas.
Flickr	Compartilhamento de imagens.
Tumbrl	Compartilhamento de pequenas publicações, semelhante ao Twitter.

Figura 15 – Grelha das redes sociais e as suas características[322]

4.5.9 SISTEMAS DISTRIBUÍDOS, SERVIDORES E ARMAZENAMENTO DE REDES

Estes sistemas, servidores e armazenamento de redes e processadores muitas vezes são controlados pelos serviços que trabalham as informações, nas estações de escuta.[323]

Alguns sistemas de armazenamento de dados, como discos rígidos internos ou memórias de disco, são mais rápidos e sofisticados para realizarem aplicações e serviços.

4.5.10 INTERFACES

Um interface é uma ferramenta que permite a movimentação de um sistema de uma qualquer tecnologia das informações que permite que dois sistemas diferenciados comuniquem entre si.

4.5.11 ATIVIDADES CIBERNÉTICAS

Os grandes benefícios da massiva utilização de cibernet são irrefutáveis, mas potenciam toda uma série de atividades criminógenas com possibilidades de anonimato, o que por si só deixa ao Estado uma árdua tarefa no controlo deste setor de atividade.

Entre outras instituições de controlo destaca-se a Direção de Comunicações e Sistemas de Informação do Exército Português que está sobre a alçada do Ministério da Defesa Nacional, que tem como missão, entre outras, a Ciberdefesa e Segurança da Informação com capacidade de resposta a

322 Juliana Diana, Professora de Biologia e Doutora em Gestão do Conhecimento In, https://www.todamateria.com.br/redes-sociais/

323 Antoine Lefébure, afirma que a NSA disponha de estações de escuta em Menwith Hill, no Yorkshire, e também na Vint Hill Farm, em que eram recolhidas informações provenientes de todo o mundo, tanto por satélite como por fitas magnéticas, in *O Caso Snowden*, p. 202 e ss.

diversas ocorrências e eventos da Rede de Dados do Exército – RDE, onde os técnicos têm como objetivo monitorizar através da Investigação Forense e *ethical hacking*.

Existem várias atividades cibernéticas de índole criminosa, uma dessas atividades é o terrorismo, ao caso ciberterrorismo, que tem como conceito primário a repetição de atos de violência (terror) para demonstração de poderio e, assim, através do choque emocional, coagir as pessoas a aceitarem os seus fundamentos e objetivos, que podem ter, entre outros motivos, a religião, a política ou ideologias.

O mal maior do terrorismo é a insegurança que provoca na sociedade, produzindo perturbações e desconfianças sobre a autoridade do Estado.

Em 2013, o Irão foi o país mais vigiado do mundo com um total de 14 mil milhões de documentos recolhidos, seguindo-se Paquistão, a Jordânia, o Egipto e a Índia, respetivamente. Estes documentos servem para preparar ações psicológicas, recolha de prova criminal, entre outros objetivos.

Este tipo de atividade serve também para supervisionar, entre outras, as atividades que se seguem:

HACKTIVISMO

Hacking é o ato de invadir um sistema informático, com ou sem autorização, e quebrar uma ou mais barreiras de segurança. Este ato não tem fórmulas conhecidas, tudo é gerado de forma diversa. Pese embora este ato esteja conotado com matéria ilícita/criminal, não é inteiramente verdadeira esta conotação, pois o hacking divide-se em três grandes grupos: *white hats, black hats and grey hats*, cuja atividade diverge da seguinte forma:

> *"... Profissionais de chapéu branco hackeam para verificar os seus próprios sistemas de segurança para torná-los mais à prova de hack. Na maioria dos casos, eles fazem parte da mesma organização. Os hackers de chapéu preto hackeiam para assumir o controle do sistema para ganhos pessoais. Eles podem destruir, roubar ou até mesmo impedir que usuários autorizados acessem o sistema. Eles fazem isso encontrando brechas e fraquezas no sistema. Alguns especialistas em informática chamam-lhes crackers, em vez de hackers. Os hackers de chapéu cinza são pessoas*

curiosas que têm quase o suficiente conhecimento da linguagem de computador para permitir que eles invadam um sistema para localizar possíveis brechas no sistema de segurança de rede. Os chapéus cinzentos diferem dos chapéus pretos no sentido de que os primeiros notificam o administrador do sistema de rede sobre os pontos fracos descobertos no sistema, enquanto que os segundos só procuram ganhos pessoais". [324]

À exceção dos *white hat*, todos os outros são considerados praticantes de ações ilegais, pois, em Portugal, a criminalização sustenta-se, principalmente, sobre dois pontos de vista essenciais: o "acesso indevido" e o "acesso ilegítimo". [325]

O Hacktivismo ou ciberativismo é, assim, o comportamento que ocorre através de um individuo ou por ação de um grupo social. Este tipo de movimento social está associado por norma a benefícios económicos, vantagens táticas ou competitivas, motivações políticas, destruição ou dano, fama ou vingança. O Hacktivismo pode passar também por um ataque simples ou por ataques organizados por vezes coordenados a grande escala.

Segundo o Centro Criptológico Nacional de Espanha *"O Hactivismo tornou-se especialmente importante em 2011, não apenas pelo número de ataques e pela sua frequência de execução, mas também pela sua agressividade e pelo seu elevado nível de divulgação social."* [326]

PROPAGANDISMO

O Propagandismo é uma forma de expor informação ou Contra-informação para persuadir uma pensamento ou uma ação. A prática do propagandismo muitas vezes tem contornos de manipulação da informação com o objetivo principal de influenciar uma audiência.

---

324 In https://economictimes.indiatimes.com/definition/hacking

325 "1 - Quem, sem a devida autorização, por qualquer modo, aceder a dados pessoais cujo acesso lhe está vedado é punido com prisão até um ano ou multa até 120 dias. 2 - A pena é agravada para o dobro dos seus limites quando o acesso: a) For conseguido através de violação de regras técnicas de segurança; b) Tiver possibilitado ao agente ou a terceiros o conhecimento de dados pessoais; c) Tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial. 3 - No caso do n.º 1 o procedimento criminal depende de queixa.". Acesso indevido art. 44.º da Lei Lei n.º 67/98, de 26 de Outubro - Lei da Proteção de Dados Pessoais, também "1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias. 2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior. 3 - A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança. 4 - A pena é de prisão de 1 a 5 anos quando: a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado. 5 - A tentativa é punível, salvo nos casos previstos no n.º 2. 6 - Nos casos previstos nos n.os 1, 3 e 5 o procedimento penal depende de queixa." Acesso ilegítimo art. 6.º da Lei Lei n.º 109/2009, de 15 de Setembro Lei do Cibercrime.

326 In, *IDN Cadernos, Estratégia da Informação e Segurança no Ciberespaço*, p. 23, ss.

As atividades do propagandismo, por vezes, produzem uma resposta emocional e não racional, traduz-se no terrorismo que se exponencia, entre outros, *online*, quando recruta terroristas através da internet *"...surgiu uma rede mundial de centenas de sites que inspiram, treinam, educam e recrutam jovens muçulmanos para a jihad..."*. [327]

TERRORISMO

Na sociedade de hoje, a significação unitária do termo terrorismo levaria a uma confrontação de autores e à criação de uma idiossincrasia a roçar a utopia, pois a divergência de objetivos, em causa de razões variadas, conduziria a uma infindável antagonia. Ainda assim, pode afirmar-se que o Terrorismo é a manipulação da apreensão dos outros em causa própria ou de um grupo com carga iniciadora de índole social.

Há autores que defendem o seguinte conceito:

O terrorismo é *"...uso sistemático do terror como forma de coação (...) com objetivos religiosos, políticos ou ideológicos (...) violência contra não combatentes."* [328] Outro dos conceitos pressupõe *"...causar a morte ou dano físicos (...) em civis (...) intimidar a população em geral (...) organização (...) a praticar (...) um qualquer ato"*,[329] ou, como referiu o Presidente dos EUA, George Bush, em Washington, três dias depois dos atentados de 11 de setembro de 2001: *"o inimigo não é um único regime político, pessoa, religião ou ideologia. O inimigo é o terrorismo – violência premeditada, com motivação política perpetrada contra inocentes."*.[330]

Poder-se-á, assim, afirmar que Portugal nunca teve um verdadeiro Terrorismo nestas últimas décadas, no entanto haverá quem questione: Então e o nosso território marítimo? E os Piratas Somali? Não serão para nós uma ameaça? Claro que sim. A este respeito urge enaltecer a excelente decisão sobre a compra dos submarinos, devido às potencialidades dos mesmos para abordagem operacional ou de mera fiscalização surpresa, por terem neles incorporados os melhores radares existentes para a monitorização naval.

327 Apontamentos gentilmente cedidos pelo docente, Mestre Augusto Meireis, da unidade curricular de Segurança e Prevenção da Licenciatura em Criminologia da Universidade Lusíada do Porto.
328 De facto e conforme Meireis explicita nos apontamentos generosamente cedidos pelo próprio aos seus alunos.
329 Iden.
330 O Sr. General Garcia Leandro define desta forma o Terrorismo em Uma visão militar sobre o terrorismo, in Terrorismo, p. 403.

CAPÍTULO 5. ESCUTAS TELEFÓNICAS

5.1 ESCUTAS JUDICIÁRIAS E ADMINISTRATIVAS: OS MEIOS DE OBTENÇÃO DE PROVA

A evolução das tecnologias da informação levaram a um aumento das comunicações faladas, aumentando assim o fluxo das informações, assim sendo, também arrastou consigo o aumento de obtenção de prova dos ilícitos criminais por este meio.

Este meio de aquisição de prova atenta com direitos fundamentais, mas aqui poderá imperar a justiça, tornando este meio de obtenção de prova, constitucionalmente lícito.[331]

Nas escutas telefónicas importa distinguir dois tipos de escutas, as judiciárias e as administrativas.[332]

Este meio de obtenção de prova apela à sua excecionalidade, o que exclui logo à partida uma interpretação analógica , mas admite uma interpretação extensiva.[333]

Esta excecionalidade contrabalança o princípio da proporcionalidade, adequação e necessidade.

> *"A regra é a proteção e salvaguarda dos direito, liberdades e garantias. A excepção é a restrição dos referidos direitos mas, apenas e tão só, na esteira da proteção de outros direitos fundamentais."* [334]

A palavra escrita perdura no tempo, ao contrário da palavra falada, que se extingue no imediato, a não ser que haja lugar a uma interceção e gravação das conversas.[335]

Na prática a gravação da escuta telefónica é transcrita, indicando as partes mais pertinentes, de modo resumido o respetivo teor e elucidando o alcance para o processo criminal. A interceção de conversa é ainda reforçada pela lei de combate à criminalidade organizada e económico-financeira.[336]

---

331 *"2. A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos."* n. 2 do Art. 18° da Constituição da República Portuguesa.

332 Segundo, Ana Raquel Conceição as escutas administrativas não exitem em Portugal. *"Estas são determinadas pelo poder executivo, com vista à manutenção da segurança interna e externa..."* ainda segundo Ana Raquel, nalguns países estas escutam passam pela intervenção de entidades independentes, e são autorizadas pelo Governo e não por um Juiz, In Escutas Telefónicas, Regime Processual Penal, p. 25, ss.

333 *"As normas excepcionais não comportam aplicação analógica, mas admitem interpretação extensiva."* Artigo 11° do Código Civil.

334 In, *Escutas Telefónicas* Regime Processual Penal, p. 59.

335 As Escutas Telefónicas são admitidas, mas impõem condições *"1 - A intercepção e a gravação de conversações ou comunicações telefónicas só podem ser autorizadas durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público, quanto a crimes..."* Art. 184 do Código do Processo Penal.

336 *"1 - É admissível, quando necessário para a investigação de crimes referidos no artigo 1.º, o registo de voz e de imagem, por qualquer meio, sem consentimento do visado, 2 - A produção destes registos depende de prévia autorização ou ordem do juiz, consoante os casos, 3 - São aplicáveis aos registos obtidos, com as necessárias adaptações, as formalidades previstas no artigo 188.º do Código de Processo Penal"* Art. 6.° da Lei n.° 5/2002 de 11 de janeiro.

A interceção e gravação de comunicações , fora da lei é tipificada como crime.[337]

Esquematicamente, nas escutas telefónicas lícitas, tem que estar a decorrer a fase de inquérito, a escuta tem que ser autorizada por um juiz, e o seu intuito tem que reforçar[338] os indícios de prova da prática de um crime, o teor da escuta terá que trazer uma valoração, e no final terá que ser elaborado um auto de transcrição para junção ao processo.

As escutas telefónicas trazem consigo um problema, jurídico, criminal e forense, que é o do *conhecimento fortuito.* No *intelligence* não se deve colocar da mesma forma como no processo penal com o seu conhecimento de investigação, nem a proibição da sua prova, pois o conceito de intelligence e todo o processo de conhecimento é casual, por vezes acidental para evitar o imprevisto. Sendo que toda a matéria do *intelligence* está envolta numa grande lacuna legal. Então à que avivar a doutrina de forma a que renasça uma tendência para a aceitação, quer nos tribunais, quer na sociedade, relembramos que o *intelligence* todo o conhecimento é fortuito montado com isso os factos para alcançar o objeto. Há que valorar então o *intelligence* para que deixe de carecer sempre de autorização legal, assim todo o conhecimento fortuito, que vá ao arrepio com o conhecimento de investigação deverá levantar certidão para correr processo autónomo a valer como notícia de um crime para operar a investigação criminal em concordância com devida autorização judicial, neste caso nunca deverá operar uma conexão processual, pois os conhecimentos (fortuitos vs investigação) são diferentes, mas se houver de facto interesse público então tudo interessa aferir a ligação, dos pontos de conexão para construir a prova, se o conhecimento fortuito é meramente indicador, já o conhecimento de investigação é incriminador. Neste sentido chamar a excecionalidade ao conhecimento fortuito resvala a legítima utilização e valoração (interesse público) necessária, proporcional e adequada à sociedade.

A simples analogia entre o conhecimento fortuito e o conhecimento de investigação é errónea.

Argui-se assim uma coerência racional que lhe é exigível sendo uma valoração lícita dentro do âmbito da autópsia digital com admissibilidade jurídica, criminal e forense, logo há todo o interesse institucional na sua valoração.

Hoje em dia há um estado de necessidade da autópsia digital, às tecnologias da informação, a todo o inimigo da sociedade com todo o suporte que lhe é dado pelo Direito Penal do Inimigo também

337 *"1 - Quem sem consentimento: a) Gravar palavras proferidas por outra pessoa e não destinadas ao público, mesmo que lhe sejam dirigidas; ou b) Utilizar ou permitir que se utilizem as gravações referidas na alínea anterior, mesmo que licitamente produzidas; é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias."* Art. 199° do Código Penal.

338 *"As provas têm por função a demonstração da realidade dos factos."* Função das provas, Artigo 341.° do Código Civil.

suportado ainda pela constituição pela Direito à Segurança do Art. 27.º da CRP na justa medida da segurança.

Ao contrário do Direito à Segurança, que é suportado pela constituição, o *Intelligence* está completamente ausente da CRP.

6. CRÍTICAS E PROPOSTAS DE REVISÃO

6.1 CRÍTICA ÀS ESTRUTURAS E AOS MÉTODOS

Na verdade existe uma multiplicidade de configurações estruturantes, bem como uma diversidade de métodos utilizados pelos vários Comités de *Intel*, mas, basicamente, todos se agregam aos cinco princípios habituais da produção de informações: Direção, Obtenção, Análise, Divulgação e, por último, a Estratégia.

As questões do *Intel,* matéria fundamentalmente dos Ministérios da Administração Interna, da Defesa Nacional e dos Negócios Estrangeiros, atuam hoje, numa mecânica de troca pela sobrevivência de Estados, como um só, assentes em organizações, tais como a *Interpol*, a *Europol*, entre outras, construindo estratégias comuns com a consciência de competências e autoridade muito similares. Projetando assim políticas internas e externas, de segurança e defesa, convocando auxílios, responsabilizando também a sociedade global, instâncias formais de controlo social incluídas.

A comunhão em uníssono pela segurança oriunda da junção de proveitos definem uma ameaça comum, assim, mecanismos de segurança e contenção do crime, tais como o *Intelligence,* são fundamentais.

As instituições de informações interpretam obrigatoriamente da mesma forma o combate, mas não os modelos e formas do processo.

O alarme social, em virtude dos ataques terroristas, levantou uma onda de preocupação das atividades das organizações de investigação criminal mobilizando todos os intervenientes, nos assuntos de segurança, a alterarem regras de empenhamento, assim sendo, hoje, a autópsia digital tem licitude com base em injunções jurídicas, criminais e forenses, não obstante as grandes dificuldades pelo uso do *Intelligence*.

Em Portugal, no que se refere aos serviços que trabalham informações, não existe a prevenção do crime quando se usa o *Intelligence* de forma lícita.

Hoje, sabe-se que o fenómeno da criminalidade é otimizado através do uso das Tecnologias da Informação, como parte estrutural das organizações criminosas.

As Tecnologias da Informação facilitam a criminalidade quando as organizações criminosas, por exemplo: enviam um e-mail cujo intuito é ilícito; enviam uma transferência financeira para branqueamento de capitais ou para aquisição de material para fins criminosos; enviam conteúdos para os Social Media com fins de propaganda política ou religiosa ou com intuitos radicais; ou ainda quando enviam imagens de satélite ainda que disponíveis online em *Open Source* para planear ações estratégicas de operações criminais.

As organizações criminosas conjeturam uma panóplia de variáveis de extrema preocupação e de grande problemática para a segurança, principalmente, pelo uso das Tecnologias da Informação, como forma de comunicação, dentro da estrutura, para coordenar ações conjuntas, ou decisões ideológicas, motivando assim as massas.

Os atentados terroristas devem ser qualificados como atos de subversão, e os seus instigadores, coautores e autores devem estar sob a tutela do Direito Penal, mas a montante sob a alçada da segurança preventiva das escutas administrativas (*Intelligence*). Esta segurança preventiva deverá ter justificação no sentido da supra legalidade tendo em conta a necessidade, proporcionalidade e adequação.

6.2 REFLEXÕES SOBRE O ESTUDO: LIÇÕES APREENDIDAS (proposta de revisão)

A prática de uma determinada situação pode ser vista sob três formas: Positiva, Negativa ou Neutra, aquilo que observamos, recolhemos, examinamos e reportamos dessa experiência é que fará diferença em situações futuras, com as devidas readaptações casuísticas. O reajustamento a essa situação trará consigo a eficácia, a eficiência e, subsequentemente, o êxito.

Confrontar a história, e incluí-la numa análise de dados (verificação de registos de entrada) possibilita prever e provisionar o Risco Calculado de uma determinada Tomada de Decisão.

Na análise do risco calculado devemos ter três tipos de peritos: Profissionais, Académicos ou Funcionários.

Assim, o Conselho Decisor (CD) terá ao seu dispor uma abordagem, de diversos pontos de vista, de uma determinada experiência. O CD ficará com uma ferramenta vantajosa para poder tomar uma resolução sobre um assunto de forma mais livre e consciente. Podendo, assim, elaborar com os seus executivos e operacionais a melhor estratégia a adotar para uma determinada situação.

Devido ao formato do mundo atual, com constantes e rápidas mudanças, a implementação de melhorias deverá ser assumida de forma o mais pronta possível, baseada em protótipos de perfeição.

Assim o impõe o paradigma do modernismo e da mutação para uma melhoria de operabilidade prática, evitando os erros do passado pela importância do *Intelligence*.

A capacidade de progresso será tanto mais eficaz com a partilha de experiências das observações resultantes de uma ação ocasionada. Portanto, a exploração de um futuro impõe-se nestes casos.

A ato de tratar as informações impõe três períodos distintos: o primeiro é a recolha, o segundo a análise, e por último, a tomada de decisão para a ação.

Existe um passo subsequente mas não poderá ser considerado dentro do período de tratamento das informações que é o facto de comunicar (partilha de informação) os resultados obtidos, até porque, por estratégia, por vezes poderão ter de ser ocultados.

O Coronel John Boyd explana de forma muito clara esta teoria através do seu ciclo.

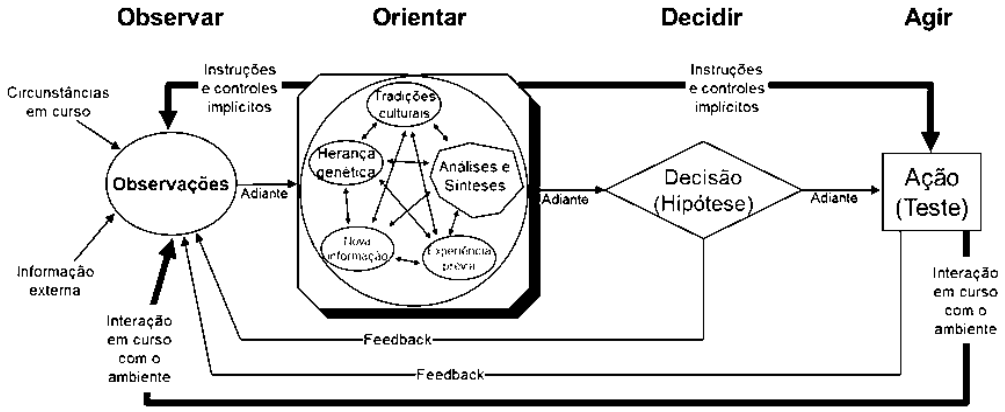

Figura 16 – Ciclo de Tomada de Decisões de Boyd

Podemos verificar que, na primeira fase, a da observação, esta fica a cabo dos operacionais dos departamentos de informações, que têm como função recolher toda a informação, seja ela oriunda ou rececionada de qualquer forma ou meio. Após isso, na segunda fase, os analistas dos departamentos de informações fazem uma análise dos dados recolhidos e traduzem a causa e efeito da recolha. Na terceira fase, e tendo em conta as duas fases anteriores, vai ser elaborado um conjunto de fórmulas de hipótese, contendo os prós e contras e a respetiva percentagem de sucesso. Neste momento entrará em jogo o conselho de decisão para, de seguida, imputar uma ação a um ou mais elementos que tenham mobilidade para agir e efetivar a sua prática.

Embora toda esta estrutura esteja muito bem definida, não podemos deixar de relembrar que a motivação é a única variável da ciência, assim, o favorecimento só será recíproco se o indivíduo e a instituição virem essa melhoria como um bem comum. Assim, cada um destes terá a capacidade de

estimular a transformação positiva de forma ativa, também foi neste sentido que foi levada a cabo a entrevista aos analistas de informações.

O grande intuito das Lições Apreendidas (LA) é proporcionar fundamentações saudáveis para inovar o modo dos acontecimentos, aperfeiçoando o desempenho de experimentação de atividades vindouras.

Com todas estas ferramentas, o CD pode de forma inequívoca apoiar os Srs. Diretores, os Srs. Ministros, etc., na tomada de decisões.

Os responsáveis pelas Lições Apreendidas estavam como que um pouco embotados até ao dia 11 de setembro de 2001, pois, até então, as LA eram tratadas muito ao estilo da guerra clássica, elaborando-se grandes manuais tático-logísticos, descuidando a futurologia das Tecnologias da Informação e a busca incansável dessas novas ferramentas. Pelo que as primeiras interpretações predominantes do evento eram vazias. *"Imprevista, extraordinariamente espetacular, a operação terrorista Kamikaze não tinha nome, autor ou finalidades explícitas.*[339]

Ver um acontecimento e não o compreender é o maior ato de ineficácia da Rede de Informações, e foi exatamente isso que aconteceu no dia 11 de setembro aos SI dos EUA.

O Estado Norte-americano não foi capaz de conter, de uma forma suficientemente célere, o alarme social causado pelo atentado às Torres Gémeas, em Nova Iorque. Cada indivíduo interpretou aquelas imagem, repetidas pelos media vezes sem conta, à sua maneira, catalogando-as conforme as percecionou.

A forma muito particular daquele atentado, não só impulsionou um conjunto de métodos e técnicas, de recolha, tratamento e análise das Informações, como também incentivou a uma estrutura verdadeiramente em rede dos SI. Isto é o tal "pronto-a-pensar" tantas vezes retratado, no livro de Boniface, *As lições do 11 de setembro*.

O significado dos conflitos vai para além da história, da demografia, ou dos conflitos étnicos. Sendo necessário, então, deixar as leituras esterilizadas para assim configurar conflitos e delimitar as suas zonas de atuação. Seria caso para dizer tranquilizem-nos com guerras.

O facto de não existirem guerras convencionais faz com que os Estados tenham de elevar a sua presença na cena internacional, mostrando assim a sua capacidade para fazer a guerra. Esses tais Estados, muitas vezes, descuram a sua soberania interna, deixando que comunidades ideológicas de

339 Como refere Ragaru em *Os atentados do 11 de setembro ou a emergência de um pronto-a-pensar* p. 33.

qualquer tipo oscilem entre a amizade e a inimizade, não obstante todos estes acontecimentos, a comunidade global e sem fronteiras gera por si só, frequentemente, o choque civilizacional.

6.3 SUGESTÕES DE INVESTIGAÇÃO: EUROINTEL

A aceção de Informações deverá ter em conta os seus respetivos segmentos de informações (militares e de segurança, políticos e sociais, económicos e empresariais e científicos e tecnológicos), deverá também ser concebida aos olhos do *Intelligence*, o que compelirá a uma cooperação verdadeiramente pura entre os vários serviços de informações, e isto deverá ser a prioridade.

Assim, após toda a prospeção levada a cabo ao longo desta tese de mestrado, chega-se às seguintes propostas:

1. Criação de uma entidade Europeia de Informações, subsidiária ao Conselho da Europa, composta por analistas dos Estados-Membros. Esta entidade deverá através dos respetivos tratados (regulamentos, diretivas, decisões, recomendações e pareceres) abraçar os objetivos da EU, professando através dos diferentes tipos de atos legislativos, a vinculação ou não dos Estados-Membros.

2. A par disso, deverá ser implementada uma colaboração estreita, através de um canal direto entre o |EuroIntel| e os vários colaboradores: prestadores do serviço universal, NATO, e outras corporações multinacionais europeias de especial relevo para o *Intel*. O objetivo deste |EuroIntel| deverá passar por um serviço especializado na recolha e análise de todas as fontes de inteligência, principalmente as oriundas através das Tecnologias da Informação, abordando todos os segmentos de informações. Todos os relatórios produzidos nas instalações do |*EuroIntel*| ou nas delegações a serem criadas se necessário deverá traduzir-se em relatórios com classificação e grau de segurança, do tipo *SupIntRep*, que, por sua vez, deverá desencadear análises e briefings temporais, que respondam às necessidades oriundas dos segmentos de informações conjeturados pelo Conselho da UE.

Subsequentemente, estas análises deverão ser difundidas, se necessário pelas respetivas instituições europeias, autoridades nacionais de segurança dos países membros da UE. Subjugando, assim, todos os Membros da UE, e em especial os membros da UKUSA, através da criação da Guerra Preventiva, que o Professor Rui Pereira tanto defende como resposta do sistema penal e de informações, evitando, assim, toda e qualquer surpresa, seja ela de caráter bélico, económico, ou outro.

CONCLUSÃO

Afirmando que a identidade, a natureza, o projeto, o imaginário do *Intelligence* se mantém na mesma e que nada alterará essa matriz, admitimos que o entendimento Governamental com outros Estados possa gerar confusão. Mas defendemos que um *Intelligence* pode fazer este tipo de acordos, por motivos políticos concretos, e um Intel com características puras pode assumir compromissos com outros Estados, incluindo com Estados ditos não democráticos, mas que não sejam compromissos abstratos.

Entendemos que uma Autópsia Digital às Tecnologias da Informação deverá ter uma conceção materialista e dialética do *Intelligence*, que se assuma como vanguardista da Sociedade de forma supranacional. Hoje, na realidade, nada alterou a matriz do antigo *Intelligence*, nem nada altera a matriz dos objetivos dos segmentos de informações (militares e de segurança, políticos e sociais, económicos e empresariais e científicos e tecnológicos).

O capitalismo está mergulhado numa profunda crise, numa crise estrutural, e isso afeta em muito o *Intelligence*.

Hoje, podemos dizer que a humanidade é confrontada com perigos imensos, incertezas em relação a desfechos que possam estar relacionados com a segurança, com as situações mais explosivas no planeta. Essa crise estrutural do capitalismo, que se tem vindo a agravar, demonstra que se estão a acumular forças, no plano objetivo, para a transformação económica e social. Naturalmente, reconhecemos que as condições subjetivas estão criadas. Mas em termos de atualidade e validade, continuamos a considerar que a vida atual, a situação internacional confirma a justeza da posição e matriz do *Intel*.

Esta tese crítica os desvios e erros de algumas instituições voltadas para a materialização pessoal. O conjunto de análises de dados que serviram de referência trazem com ele elementos fundamentais para um processo de governação do *Intelligence* que não se distancie dos valores da sociedade e dos sentimentos do povo, contando com a mobilização de todos e com a participação e intervenção de quem de direito. Falando no plano social, o *Intel* toca a todos porque se concebe numa participação passiva do povo e numa participação ativa dos profissionais (analistas) que laboram o *Intelligence*.

O *Intelligence* não deverá ceder nem confundir-se com ações particulares de um qualquer agente, tanto quanto se fez saber ao longo desta tese não houve acordos aglutinadores de Direitos,

Liberdade e Garantias dos indivíduos Pró-sociais, numa relação de forças, o *Intelligence* puro será sempre visto de forma positiva.

A infinita evolução civilizacional tem levado ao desenvolvimento de diferentes estádios em diversas experiências, tanto ao nível nacional como internacional, passíveis de orientar a evolução das estratégias doutrinais, nas normas e procedimentos, estabelecendo uma boa gestão da integridade e capacidade da rede, explorando, assim, ao máximo, o poder da atmosfera universal da informação que atualmente alimentamos.

Tudo isto traz consigo ameaças de desmedido risco e de danos à escala internacional, tais como: acidentes biotecnológicos ou nucleares; manipulação de mercados económicos; grandes fusões e agitamento de mega empresas. Estas ameaças sacodem e arguem aos bens jurídicos supra individuais, isto traz consigo os tipos de perigo abstrato, e só por isso dever-se-á discutir uma maleabilidade das normas e leis que arguam as contingências de uma conceção do processo penal/administrativo garantista, para que com isto se profetize um forte combate aos crimes de poder.

Também os bens jurídicos transindividuais são arguidos e abalroados, através do uso das tecnologias das informação, tais como: a prostituição infantil ou a exploração de menores.

Assim sendo, reclama-se a figura jurídica do coletivismo e dos direitos difusos, sustentando a relevância do interesse público.

Os patronos (Associação para a Promoção e Desenvolvimento da Sociedade da Informação, Fundação Portuguesa das Comunicações, Fundação para a Divulgação das Tecnologias de Informação, Fundação para a Ciência e a Tecnologia – Departamento da Sociedade da Informação) pertencentes às Tecnologias da Informação, bem como a Comissão da Assembleia da República de Assuntos Constitucionais, Direitos, Liberdades e Garantias devem participar ativamente com todas as entidades que trabalhem o *Intelligence*, em todos os esboços de enquadramento, para legitimar o direito e a informática na sua plenitude e para que seja imposto, sempre e somente, o exercício necessário e proporcional que a comunidade e os órgãos sociais de controlo lhe imponham, salvaguardando assim todo o sistema digital da perigosidade na ofensa da privacidade e intimidade, travando na fonte todo e qualquer excesso de abuso de poder.

Certo é que uma sociedade não pode evoluir sem o uso constante de um risco permitido, que assegure não só o contrato social mas que obrigue também à imposição de normas do Direito administrativo e penal. Aqui o bem jurídico a ser preservado pela norma de um perigo abstrato deverá

ser apreciado, pelo legislador, sem esquecer os valores essenciais salvaguardados pela Constituição, perpetuamente conforme a dignidade da pessoa humana.

Deverão então os Estados da União Europeia criar uma Força Internacional das Telecomunicações, que seja multidisciplinar, composta por políticos, juristas, engenheiros, técnicos, entre outros, pois a mesma traria à internet uma melhoria através do seu redesenhamento e à sociedade o garante da não sideração e desassossego subjacente nas Tecnologias da Informação, devendo esta Força participar em tudo quanto lhe fosse confiado.

Esse controlo deveria ser superiormente imposto pelos Governos dos países da UE, assim a criação de uma Intelligence Europeia deveria gozar da total independência política regional de cada país e submeter-se a um plano obrigatório derivado da Comissão Europeia, tendo em conta a capacidade, a obrigatoriedade de guardar sigilo por parte dos seus colaboradores e a vital importância da informação para os poderes que derivam do plano, sejam informações do segmento militar, de segurança, político, social, económico, empresarial, cientifico, tecnológico, pois o objetivo deverá ser a de uma Europa de todos e para todos, onde o verdadeiro inimigo se encontra fora dela. Assim os planos estratégicos de *Intelligence* poderiam controlar a Ásia, a África, a Europa de leste, e sobretudo a América.

Pois nesta tese conclui-se que a análise de informações efetuada a partir de informações limitadas (regionais) não produz grandes resultados, referimo-nos à desinformação, levada a cabo pelo *counter-intelligence*, e às estratégias bilaterais do *competitive intelligence* entre alguns parceiros (membros da Europa), destruturando assim, a ideologia da verdadeira Europa.

Para remate final, só resta acrescentar que o grande repto do jurisconsulto da era das Tecnologias da Informação é conciliar as garantias constitucionais e adquiridas na delonga histórica dos Direitos Humanos com a congruência das constantes transformações sociais e sucessivas inovações tecnológicas.

QUESTIONÁRIO DA ENTREVISTA

ENTREVISTA TÉCNICA A ANALISTAS DE INFORMAÇÕES

1. GENERALIDADES

a. As Entrevistas Técnicas a Analistas de Informações – ETAI foram organizadas e conduzidas de acordo com o princípio do anonimato preconizando uma entrevista fiel à realidade dos órgãos PSP, GNR, SEF, SIS, Polícia Municipal, PJM, PJ, AT, Polícia Marítima, DGRSP.

b. As ETAI serão um instrumento fundamental para a avaliação do exercício funcional dos Sistemas de Informações Administrativo/Criminal sobre o controlo do *Intelligence* e as injunções jurídicas, criminais e forenses e, como tal, darão uma visão clara, e objetiva, da situação atual das Tecnologias da Informação, no capítulo da licitude.

2. FINALIDADE

Verificar, Comparar e Contabilizar o tratamento e a classificação da informação, bem como, a segurança, os ficheiros, a recepção, expedição e arquivo de documentos de informação sensível integrada nas Tecnologias da Informação, no âmbito das injunções jurídicas, criminais e forenses.

3. EXECUÇÃO

a. Conceito

(1) As ETAI foram planeadas e integradas na Tese referente ao ano civil 2020, determinadas pelo autor e pelo respetivo orientador;

(2) As ETAI foram coordenadas pelo orientador, e executadas de forma sigilosa entre o autor e os respetivos analistas, em virtude das informações serem uma área sensível e de conhecimento restrito.

(3) Cada ETAI decorreu por via telefónica/e-mail ou presencial e incidiu nas finalidades do ponto 2., atinentes às injunções jurídicas, criminais e forenses, e segundo a Lista de Verificação que se encontram no Anexo A; cada ETAI foi objeto duma avaliação resultante da valorização dos diversos itens das Listas de Verificação e terá uma classificação final resultante do modelo constante do Anexo B;

(4) Cada ETAI deu origem a um Relatório, que foi submetido ao conhecimento do Orientador, após isso foi ocultado desta Tese por motivos de confidencialidade.

b. Organização e Execução

(1) Cada ETAI foi realizada através de contacto direto, entre o autor da Tese Autópsia Digital às Tecnologias da Informação (ADTI) e os Entrevistados que são Analistas de Informações, e que integram os órgãos citados em 1. a. durante a realização da Tese ADTI. A Entrevista contém informação e aspetos sobre o tratamento e a classificação de informações incluídas no uso das Tecnologias da Informação. Destas ETAI foram dadas ao conhecimento do orientador;

(2) Após a receção da ETAI, o autor remeteu à Tese a informação nela contida de forma global, nomeadamente as matérias relativas ao tratamento e a classificação de informação habitual tratada nas Tecnologias da Informação, no âmbito das injunções jurídicas, criminais e forenses;

(3) O formato da ETAI foi precedida duma reunião de coordenação entre o autor e o orientador, para afinar aspetos referentes à matéria a abordar nas ETAI;

(4) Cada ETAI desenrola-se normalmente em um dia, iniciando-se com a confirmação, pelo Autor da Tese ao Analista de informações sobre confidencialidade da entrevista; seguidamente, segue-se um brífingue de informação feito pelo Autor, após o que se inicia a Entrevista, propriamente dita;

(5) A Tese integrará atividades de análise documental, avaliação de procedimentos críticas do *Intelligence*, nomeadamente das Tecnologias da Informação, tais como as que integram Sistema de Informação Criminal e outras que contemplem a infraestrutura em rede, e inclui avaliação de procedimentos de elementos dos respetivos Órgãos, nomeadamente na curadoria das informações;

(6) Todas as ETAI permitiram o registo e avaliação dos itens constantes das Listas de Verificação, assim como registo de procedimentos e informações que estejam em linha com a doutrina e as normas em vigor;

(7) A Tese, em termos de redação decorreu de forma a expor e relevar todos os aspetos em percentagem revelados na ETAI;

(8) As ETAI só terminaram com a elaboração do relatório final traduzido em percentagens cuja sua difusão foi refletida na Tese, após parecer do Orientador;

(9) A avaliação final das ETAI foram alvo de redação na Tese no Ponto 6. Criticas e propostas de revisão, na crítica às estruturas e aos métodos, nos conflitos entre *intelligence* e informações criminais determinando a execução duma segunda reflexão sobre o estudo nas Lições apreendidas sobre uma proposta de revisão às sugestões de investigação, em especial a avaliação final das ETAI foram tidas em conta na conclusão da Tese;

(10) As ETAI foram levadas a cabo pelo método indutivo, dum modo geral, preparadas e conduzidas em curto espaço de tempo e incidem em itens específicos das Listas de Verificação.

Anexo A (Listas de verificação, a aplicar nas ETAI)

1. Generalidades

a. A lista de verificação foi submetida somente à área da Segurança da Informação

b. As Áreas estão divididas em itens, subitens e critérios.

c. Dentro de cada Critério existem medidas de desempenho, sob a forma de perguntas, que serão avaliadas e registadas como Sim ou Não na folha de registo. As medidas de desempenho são numeradas de forma seguida dentro de cada área ou subárea.

d. Existem medidas de desempenho que, pela sua importância e criticidade, quando têm uma avaliação negativa afetam a classificação do critério onde estão inseridas. São designados por elemento eliminatório e aparecem, nas listas de verificação.

e. Cada subitem ou critério será objeto duma avaliação expressa sob a forma duma percentagem que expressa a classificação de todas as medidas de desempenho inseridas nesse subitem/critério, devendo o inspetor da área preencher, quando aplicável (especialmente em avaliações abaixo de Excelente), as observações e recomendações que julgue adequadas nas caixas respetivas, com a melhorar o desempenho da no futuro.

f. Poderão existir itens e/ou medidas de desempenho que não possam ser avaliadas/observadas por razões diversas (falta de doutrina/normas aplicável, inexistência de equipamentos, entre outras), sendo que este facto não irá prejudicar a classificações parciais e final, na ETAI.

2. Regras para o preenchimento das folhas de registo das Listas de Verificação

a. Na coluna "S" coloca-se "1" se cumpre.

b. Na coluna "N" coloca-se "1" se não cumpre.

c. Na coluna "N/A" coloca-se "1" quando não é aplicável. Não se contabiliza para avaliação.

d. A avaliação de um "SUB ITEM/CRITÉRIO" é feita com a soma unicamente da coluna do "S".

e. Quando existirem linhas não aplicáveis "N/A", estas não poderão contar para a avaliação.

(1) No caso de uma linha, a média da coluna "S" não contabiliza a linha "N/A".

(2) No caso de ser todo o "SUB ITEM/CRITÉRIO", não se contabiliza para a média do "ITEM". Neste caso coloca-se no campo de avaliação "Não considerado para a avaliação." e deixa-se a célula vazia à direita de % .

f. Quando um "SUB ITEM/CRITÉRIO" retorna um valor nulo, o inspetor deverá alterar a fórmula do campo de modo a que o retorno seja: "SUB ITEM/CRITÉRIO NULO".

g. As listas de verificação, quando preenchidas, têm a classificação de Segurança de CONFIDENCIAL.

ITEM	A1. ÁREAS CLASSIFICADAS			
SUB ITEM	A1.1 SEGURANÇA DAS TECNOLOGIAS DA INFORMAÇÃO			
CRITÉRIO				
ORDEM	MEDIDAS DE DESEMPENHO	S	N	N/A

1	A proteção das informações classificadas é adequada em função da classe de segurança a que cada pertence?			
2	Existe controlo de acesso às Tecnologias da Informação?			
3	Existe uma política de recolha de documentos classificados no final do dia de serviço?			
4	O Sistema das Tecnologias da Informação possui controlo fora do horário de serviço?			
5	O Sistema está organizado por camadas com os regulamentares graus de segurança consoante a matéria classificada existente?			
Avali:		%		
Obs:				
Rec:				
ITEM	A1. ÁREAS CLASSIFICADAS			
SUB ITEM	A1.2 SEGURANÇAS DAS TECNOLOGIAS DA INFORMAÇÃO			
CRITÉRIO	A1.2.1 PROCEDIMENTOS			
ORDEM	MEDIDAS DE DESEMPENHO	S	N	N/A
6	O acesso às Tecnologias da Informação é alterado com frequência (6 em 6 meses)?			
7	Existe uma relação nominal do pessoal autorizado (código)?			
8	Existe um registo de abertura (GDH, identificação e rubrica)?			

9	Existe um registo de existências?			
10	Existe um indicador de aberto/fechado?			
Avali:		%		
Obs:				
Rec:				
ITEM	A1. ÁREAS CLASSIFICADAS			
SUB ITEM	A1.3 ARMÁRIOS E FICHEIROS			
CRITÉRIO	A1.3.1 ROBUSTEZ/PROCEDIMENTOS			
ORDEM	MEDIDAS DE DESEMPENHO	S	N	N/A
11	Possuem condições de segurança de acordo com os regulamentos em vigor em concorrência com a matéria que guardam?			
12	As chaves (código) estão apenas na posse de um responsável?			
13	As chaves (código) são entregues no final do serviço ao responsável pelo chaveiro (com assinatura do livro de entrega/receção)?			
Avali:		%		
Obs:				
Rec:				
ITEM	A2. TRATAMENTO DO MATERIAL CLASSIFICADO			

SUB ITEM	A2.1 GENERALIDADES			
CRITÉRIO	A2.1.1 PROCEDIMENTOS			
ORDEM	MEDIDAS DE DESEMPENHO	S	N	N/A
14	O custódio/informático é conhecedor de todos os procedimentos inerentes ao tratamento de material classificado?			
Avali:		%		
Obs:				
Rec:				
ITEM	A2. TRATAMENTO DO MATERIAL CLASSIFICADO			
SUB ITEM	A2.2 RECEÇÃO DE DOCUMENTOS			
CRITÉRIO	A2.2.1 PROCEDIMENTOS			
ORDEM	MEDIDAS DE DESEMPENHO	S	N	N/A
15	Existe uma norma que regule o fluxo de receção de todos os documentos classificados?			
16	Existe uma entidade autorizada para abrir a correspondência MUITO SECRETO?			
17	Existe uma entidade autorizada para abrir a correspondência SECRETO?			
18	Existe uma entidade autorizada a abrir a correspondência CONFIDENCIAL?			

Avali:		%		
Obs:				
Rec:				
ITEM	A2. TRATAMENTO DO MATERIAL CLASSIFICADO			
SUB ITEM	A2.3 REGISTO DE ENTRADA/EXPEDIÇÃO /ENCAMINHAMENTO DE DOCUMENTOS			
CRITÉRIO	A2.3.1 PROCEDIMENTOS			
ORDEM	MEDIDAS DE DESEMPENHO	S	N	N/A
19	Existe um responsável pelo registo de entrada e expedição de documentos/informações?			
20	O responsável é conhecedor da norma superiormente aprovada para a elaboração do registo de entrada e expedição de documentos/informações?			
21	O seu encaminhamento é controlado através de Protocolo/Folha de Circulação/Certificado de Transferência?			
Avali:		%		
Obs:				
Rec:				
ITEM	A2. TRATAMENTO DO MATERIAL CLASSIFICADO			
SUB ITEM	A2.4 MANUSEAMENTO/ARQUIVO DE DOCUMENTOS			
CRITÉRIO	A2.4.1 PROCEDIMENTOS			

ORDEM	MEDIDAS DE DESEMPENHO	S	N	N/A
22	Existe uma norma que identifique a entidade que autoriza o seu manuseamento?			
	a. Interno			
	b. Externo			
23	Existe uma norma que identifique a entidade que autoriza o seu arquivo?			
24	É verificado e encerrado o Protocolo/Folha de Circulação aquando da entrega para arquivo?			
25	Existe um registo atualizado de documentos arquivados?			
26	Existem arquivos separados para documentos classificados de MUITO SECRETO, SECRETO e CONFIDENCIAL?			
27	Existe nomeado um responsável pela salvaguarda/manutenção do seu inventário físico?			
28	Existe uma relação nominal de pessoas com acesso ao arquivo?			
Avali:		%		
Obs:				
Rec:				

RESOLUÇÃO 2045 (2015) DO CONSELHO EUROPEU

Resolution 2045 (2015) Mass surveillance

Author(s): Parliamentary Assembly

Origin - Assembly debate on 21 April 2015 (12th Sitting) (see Doc. 13734, report of the Committee on Legal Affairs and Human Rights, rapporteur: Mr Pieter Omtzigt; and Doc. 13748, opinion of the Committee on Culture, Science, Education and Media, rapporteur: Sir Roger Gale). Text adopted by the Assembly on 21 April 2015 (12th Sitting). See also Recommendation 2067 (2015).

1. The Parliamentary Assembly is deeply concerned about the mass surveillance practices that have been disclosed since June 2013 by journalists to whom a former United States National Security Agency (NSA) contractor, Mr Edward Snowden, had entrusted a large amount of top secret data establishing the existence of mass surveillance and large-scale intrusion practices hitherto unknown to the general public and even to most political decision makers.

2. The information disclosed so far in the Snowden files has triggered a massive, worldwide debate about mass surveillance by the intelligence services of the United States and other countries and the potential lack of adequate legal regulation and technical protection at national and international levels, and/or their effective enforcement.

3. The disclosures have provided compelling evidence of the existence of far-reaching, technologically advanced systems put in place by United States intelligence services and their partners in certain Council of Europe member States to collect, store and analyse communication data, including content, location and other metadata, on a massive scale, as well as targeted surveillance measures encompassing numerous people against whom there is no ground for suspicion of any wrongdoing.

DEFINIÇÕES

Acesso - a disponibilização de recursos e ou serviços a outra empresa, segundo condições definidas, em regime de exclusividade ou não exclusividade, para efeitos de prestação de serviços de comunicações electrónicas, mesmo quando estes forem utilizados para a prestação dos serviços previstos nas alíneas a) e b) do n.º 1 do artigo anterior, abrangendo, nomeadamente, o acesso a elementos da rede e recursos conexos, podendo incluir a ligação de equipamento, através de meios fixos ou não fixos (incluindo, em especial, o acesso ao lacete local e a recursos e serviços necessários para prestar serviços pelo lacete local); o acesso a infra-estruturas físicas, incluindo edifícios, condutas e postes; o acesso a sistemas de software pertinentes, incluindo sistemas de apoio operacional; o acesso a sistemas de informação ou bases de dados para pré-encomenda, aprovisionamento, encomenda, pedidos de manutenção e reparação, e facturação; o acesso à conversão numérica ou a sistemas que ofereçam uma funcionalidade equivalente; o acesso a redes fixas e móveis, em especial para fins de itinerância (roaming); o acesso a sistemas de acesso condicional para serviços de programas televisivos e de rádio digitais; o acesso aos serviços de rede virtual.

Adaptador de Rede - Placa de expansão ou outro dispositivo usado para ligar um computador a qualquer tipo de rede.

Analógico X Digital
Refere-se ao sistema de representação que pode ser por analogias ou semelhanças (analógico) ou por dígitos numéricos (digital). Por exemplo, nas antigas gravações de música, a onda sonora dos instrumentos musicais gravada nos discos tinha uma representação análoga ao da onda sonora original, ao passo que nos atuais CDs, a forma de onda dos instrumentos musicais é representada por dígitos numéricos.

Antiescuta - Todas as medidas, activas e passivas, tendentes a detectar e neutralizar a escuta.

Aplicação informática - Conjunto de programas usados como um todo para a solução informática de um caso concreto.

Aplicativos - Softwares com fins específicos.

Arquivo - Nome dado à forma como as informações são armazenadas no disco rígido.

Array - Matriz. Pode ser referenciada tanto na área de softwares como na área de hardware.

Assinante - a pessoa singular ou colectiva que é parte num contrato com um prestador de serviços de comunicações electrónicas acessíveis ao público para o fornecimento desses serviços.

Atribuição de espectro - a designação de uma dada faixa de frequências para ser utilizada por um ou mais tipos de serviços de radiocomunicações, se necessário, em condições especificadas.

Attachment - Qualquer anexo do tipo de arquivo (programa, texto, imagem, som, vídeo, etc) que vai anexado a uma mensagem enviada por correio eletrônico.

Auditoria - O meio pelo qual os acessos ao sistema, processos e transacções podem ser vigiados e registados de modo que as quebras e tentativas de acesso possam ser detectadas.

Autópsia - É a inspeção em forma de análise crítica.

Back-Up - Sistema de segurança que consiste na cópia de ficheiros informáticos para suportes magnéticos suplementares.

Banco de Dados - São programas que organizam e classificam grandes quantidades de informação.

Bastidores de rede – Local onde se organiza (distribui ou repete de dados) todo o material associado à rede local do edifício e às suas comunicações com o exterior.

Bulletin Board System - Serviço eletrônico que oferece recursos como correio eletrônico, acesso a outros computadores e serviços remotos.

Basic Input Output Services - Sistema básico de entrada e saída. Camada que controla o trânsito entre o hardware do computador e o software que aceita as teclas digitadas e redireciona os dados para e a partir do monitor.

Bot - Diminutivo de Robot

Boot - Procedimento de carregar um sistema operacional na memória RAM principal, executado por um pequeno programa, contido no BIOS da memória ROM, que instrui o microprocessador sobre como proceder para localizar o sistema operacional no disco e carregá-lo na memória. Referente ao momento de inicialização do computador, quando ele é ligado ou reinicializado.

Bits Per Second - É a medida de velocidade de transmissão de dados, pela qual bits de dados são transmitidos por um meio de comunicação, como um modem. 10 bps equivalem a cerca de um caráter por segundo.

Browser - Navegador. Programa utilizado para visualizar as páginas da World Wide Web (WWW).

Bug - Defeito em um programa.

Centro de informática - Área onde estão instalados sistemas informáticos e onde são feitos a concepção de desenvolvimento das aplicações.

Chamada - a ligação estabelecida através de um serviço de comunicações electrónicas acessível ao público que permite uma comunicação bidireccional.

Ciberespaço - É o conjunto formado pela rede de computadores e serviços que compõe a internet.

Classificação - Atribuição de um grau de segurança a um documento, ficheiro de dados, programa ou suporte informático que impede que este seja acedido por alguém cuja credenciação seja menor do que a do referido documento.

Competitive Intelligence - Informações sobre produtos e mercados do meio empresarial ou da gestão de empresas tendo em conta as regras básicas da economia de mercado.

Comprometimento - É o conhecimento, parcial ou total, de matérias classificadas por parte de pessoas não autorizadas, isto é, pessoas sem a adequada credenciação ou sem acesso autorizado às referidas matérias.
Considera-se ter havido comprometimento sempre que matérias classificadas tenham estado sujeitas ao risco de divulgação a pessoas não autorizadas ou tenham estado perdidas, ainda que temporariamente, no exterior de uma área de segurança. Considera-se também ter havido comprometimento sempre que matérias classificadas não sejam localizadas nas conferências periódicas ou que tenham sido perdidas, ainda que temporariamente, no interior de uma área de segurança, até que uma investigação de segurança venha provar o contrário.

Compilador - Programa principal de uma linguagem de programação. Transforma um programa fonte (o programa que as pessoas entendem) em linguagem de computador (programa executável).

Comunicação - qualquer informação trocada ou enviada entre um número finito de partes mediante a utilização de um serviço de comunicações eletrónicas acessível ao público.

Conectividade - O termo refere-se às redes de comunicação ou ao ato de comunicar entre computadores e terminais.

Conexão Direta - Ligação permanente entre dois computadores. Também é conhecida como linha dedicada.

Configuração - Grupo de dispositivos e programas integrados entre si de forma a operarem como um sistema único de processamento de dados.

Consumidor - a pessoa singular que utiliza ou solicita um serviço de comunicações electrónicas acessível ao público para fins não profissionais.

Contra-espionagem - Actividades que tenham por finalidade detectar e neutralizar a espionagem.

Contra-informação - Actividades que tenham por finalidade identificar e neutralizar as ameaças aos vários segmentos das informações, postas por serviços de informações hostis e organizações ou

pessoas envolvidas em actividades de espionagem, sabotagem, subversão e terrorismo, bem como actividades que tenham por finalidade encobrir as nossas vulnerabilidades e as nossas potencialidades.

Contra-sabotagem - Actividades que tenham por finalidade detectar e neutralizar a sabotagem.

Contra-subversão - Actividades que tenham por finalidade detectar e neutralizar a subversão.

Contra-terrorismo - Actividades que tenham por finalidade detectar e neutralizar o terrorismo.

Contra-vigilância - Todas as medidas, activas e passivas, que tenham por finalidade neutralizar a vigilância.

Correio Eletrônico - Sistema de transmissão de mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que possa ser armazenada na rede ou no equipamento terminal do destinatário até que este a recolha através do uso de computadores.

Counter-intelligence – Ver Contra-informação

Credenciação - Determinação ou reconhecimento feito pela autoridade nacional de segurança no sentido de que, sob o ponto de vista da segurança, uma determinada pessoa, estabelecimento, empresa, organismo ou serviço está apto a assegurar a adequada protecção a informações de uma certa categoria de classificação e de todas as restantes categorias inferiores.

Criminais - Relativos ao crime, ao processo, ou ao tribunal criminal.

Dados - Qualquer tipo de informação (em um processador de texto, programa de imagem, etc.) processada pelo computador.

Dados de localização - Quaisquer dados tratados numa rede de comunicações eletrónicas ou no âmbito de um serviço de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas acessível ao público.

Dados de tráfego - Quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma.

Delegado de segurança - Elemento representante do encarregado de segurança e por este nomeado para cumprimento de missões específicas.

Difusão - Comunicação, em tempo útil, de uma notícia ou informação, por forma e meios adequados, a quem delas deve ter conhecimento.

Digital - É um computador ou uma máquina que opere informação representada sob a forma de dígitos associados a impulsos elétricos.

Digitalizar - Processo de transformação de som ou imagem em sinais binários (dígitos). Exemplo: por meio de um scanner uma foto pode ficar armazenada no computador sob a forma de um arquivo.

Diretório - Arquivos em alguns sistemas de computadores que ficam agrupados. Arquivos comuns para um mesmo tópico; geralmente ficam organizados em diretórios e subdiretórios separados.

Disco rígido - Disco interno ou externo para armazenamento de grandes volumes de informação. O padrão do tamanho dos discos de mercado está acima de 6 gigabytes (GB).

Dispositivo - Aparelho ou objeto de engenharia com capacidade informática.

Documento - É todo e qualquer registo gráfico ou de outra natureza de qualquer assunto, nomeadamente:
Manuscritos, cartas, notas, actas, relatórios, memorandos, mensagens, papéis taquigrafados, impressos, apontamentos e listagens de computador; Planos, esboços, croquis, desenhos, plantas e cartas topográficas; Registos fotográficos ou cinematográficos de qualquer natureza (vídeos, por exemplo), cartões ou fitas perfurados e registos em banda magnética; Composições gráficas, material litográfico, matrizes, zincogravuras, stencil, fitas de máquina de escrever, papel químico ou absorvente, ou qualquer outro material de reprodução de documentos.

Domínio - Nome oficial na linguagem da Internet para um computador, departamento ou organização que faça parte da rede. Consiste de uma sequência de nomes separados por pontos.

DOS - Sistema operacional de PCs, que se baseia em linhas de comando.

Download - É a transferência de um arquivo de outro computador para o seu computador através da rede.

Drive - Dispositivo de armazenamento de dados na forma de arquivos.

Drivers - Itens de software que permitem que o computador se comunique com um periférico específico, como uma determinada placa. Cada periférico exige um driver específico.

Dynamic Link Library - Biblioteca de Conexão Dinâmica. Um conjunto de funções e rotinas de programação que podem ser acedidas dinamicamente por um programa. Isso significa que tais funções e rotinas são acrescentadas ao código do programa na medida em que surge a necessidade de usá-las.

Emulador - Programa que permite um computador simular outro computador ou sistema eletrônico.

Encarregado de segurança - Responsável por todas as actividades de segurança atribuída aos gabinetes ou núcleos de segurança, com funções de conselheiro junto do ministro ou presidente do governo regional ou do director do estabelecimento, empresa, organismo ou serviço, respectivamente.

Encarregado de segurança informática - Responsável por todas as actividades de segurança informática, na dependência hierárquica dos núcleos e gabinetes de segurança.

Endereço Eletrônico - Dado de identificação do usuário na internet.

Equipamento avançado de televisão digital - os conversores para conexão a aparelhos de televisão ou aparelhos integrados de televisão digital capazes de receber serviços de televisão digital interactiva.

Escuta - Termo genérico que designa a intercepção não autorizada de notícias ou informações que sejam difundidas por qualquer meio sonoro ou electromagnético.

Escuta activa - É a que visa obter informações classificadas por intermédio de microfones, com ou sem fio, ou de outros dispositivos instalados para o mesmo efeito. A protecção contra este tipo de escuta exige a inspecção de segurança técnica de toda a estrutura do compartimento em causa, do seu mobiliário, decoração, equipamento, material de escritório, máquinas e meios de telecomunicações.

Escuta passiva - É a que visa obter informações classificadas através de meios de telecomunicações não protegidos ou por escuta directa.
A protecção contra a escuta passiva exige inspecções de segurança técnica e pode requerer a insonorização das paredes, portas, tectos e soalhos.

Espionagem - Actividade que visa a recolha de notícias ou informações por métodos clandestinos.

Estratégia - É a conjugação estruturada entre o conhecimento, o pensamento, e a ação para a tomada de decisão relativamente a uma ação, ou omissão, para alcançar uma determinada finalidade.

Ferramentas de Busca - Instrumentos para realizar pesquisas na internet através de assuntos ou palavras-chaves.

Fibra Ótica - Cabos de comunicação que usam fios de vidro finos para transmitir pulsos de luz. Um único cabo permite transmissões de bilhões de bits por segundo.

Fideicomisso - É o nomeado por determinação para uma propriedade plena de um bem jurídico.

'Fidelização' - o período durante o qual o consumidor se compromete a não cancelar um contrato ou a alterar as condições acordadas.

Firewall - Combinação de hardware e software cujo papel é o de filtrar o trânsito de informações entre redes fechadas. Impede que usuários não autorizados entrem nesta rede interna, via Internet. Sistemas de monitoração que olham tudo o que entra e sai do servidor e outros protocolos de segurança.

Five Eyes - Conjunto de países que tem um acordo de segurança entre eles, na partilha informações (EUA, UK, Canadá, Austrália, e Nova Zelândia).

Forenses - Relativos ao foro judicial ou dos tribunais.

Gabinete de segurança - Órgão do canal técnico funcionando na dependência directa dos ministérios e governos das regiões autónomas, destinado a apoiar no campo da segurança estas entidades, de acordo com as normas regulamentares.

Guardas de segurança - pessoas que desempenham ou venham a desempenhar funções de guardas em cumprimento de missão específica no acompanhamento de material classificado, podendo ser militares ou civis, estar armados ou não e ser titulares de certificados de credenciação apropriados.

Gaiola de Faraday - Revestimento interior de uma sala com uma malha metálica que impede a captação do exterior da radiação electromagnética.

Gateway - Computador que interliga duas redes diferentes, ou uma rede local (LAN) à internet.

Hardware - Termo usado para expressar de forma genérica o equipamento informático.

Header - A parte de um pacote que precede os dados e que contém a fonte, o destino e o endereço, verificador de erros e o remetente, dia e hora, de uma mensagem electrónica.

Hacker - É considerado uma espécie de especialista informático e conhecedor da eletrônica, consegue quebrar e aceder com facilidade a sistemas de segurança em empresas e instituições.

Host - Computador da Internet onde as páginas de um site ficam hospedadas.

HyperText Markup Language - Linguagem de Marcação de Hipertexto. É a linguagem que usamos para fazer páginas na Internet.

Hyper Text Transfer Protocol - Protocolo de Transferência de Hipertexto. Conjunto de regras que torna viável o envio de uma página em HTML de um computador a outro na rede.

Hub – Plataforma de junção de diferentes cabos e redes interligando computadores de uma rede local.

ICQ - Serviço da Internet que permite a um usuário saber se uma determinada pessoa está conectada a Internet no momento. Além disso, permite a conexão ponto a ponto e troca de dados com essa pessoa.

Indivíduo não autorizado - É todo aquele que não está credenciado nem autorizado a ter acesso a matérias classificadas ou que, embora credenciado, não conste das respectivas listas de acesso.

Indução eléctrica - Efeitos das tensões de linhas eléctricas sobre os condutores vizinhos.

Informação - É a notícia dada ou recebida pelo homem ou por uma máquina electrónica.

Informações - É o produto resultante da análise e tratamento de notícias obtidas que permitam o aumento de conhecimento em determinada matéria.

Informação de segurança - Informação sobre a identidade, capacidades e intenções de organizações ou pessoas hostis que possam estar envolvidas em espionagem, terrorismo, sabotagem ou subversão.

Injunção – É a obrigação da imposição da ordem formal.

Inquérito de segurança - Actividade desenvolvida no sentido de se determinar se uma pessoa possui a lealdade, integridade, honestidade, reputação e hábitos compatíveis com os requisitos que a concessão de uma credenciação exige.

Instalações - Quaisquer infra-estruturas fixas necessárias ao desenvolvimento e funcionamento eficaz da actividade.

Intel - Intelligence

Intelligence - É a recolha de conhecimento total ou parcial de notícias de interesse relevante oriundas de fontes abertas ou cobertas com o intuito de produzir matéria de difusão maioritariamente restrita que permite criar uma estratégia que vise prevenir e resolver conflitos, auxiliando da melhor forma uma tomada de decisões consciente necessária à proeficiência de um qualquer sector de atividade.

Interferência prejudicial - qualquer interferência que comprometa o funcionamento de um serviço de radionavegação ou qualquer outro serviço de segurança ou que de outra forma prejudique seriamente, obstrua ou interrompa repetidamente um serviço de radiocomunicações que opere de acordo com as normas internacionais, comunitárias ou nacionais aplicáveis.

Interligação - a ligação física e lógica de redes de comunicações públicas utilizadas por uma mesma empresa ou por empresas diferentes de modo a permitir a utilizadores de uma empresa comunicarem com utilizadores desta ou de outras empresas ou acederem a serviços oferecidos por outra empresa. Os serviços podem ser oferecidos pelas partes envolvidas ou por terceiros que tenham acesso à rede. A interligação é um tipo específico de acesso implementado entre operadores de redes públicas.

Interface de programas de aplicação (IPA) - o software de interface entre aplicações, disponibilizado por operadores de rádio, televisão ou de distribuição ou fornecedores de serviços, e os recursos no equipamento avançado de televisão digital para serviços de rádio e televisão digitais.

Investigação de segurança - Actividade destinada a esclarecer qualquer incidente que envolva quebra de segurança ou comprometimento, com a finalidade de avaliar o seu grau e extensão, concluir sobre as medidas de segurança a tomar para evitar outras violações e apurar responsabilidades.

Interface - Conexão entre dois dispositivos num sistema de computação.

Intermediação - A atividade que consiste negociar ou transacionar um bem entre diferentes pessoas singulares ou coletivas.

Internet Protocol - O mais importante dos protocolos em que se baseia a Internet. Parte IP do protocolo TCP/IP, é responsável por direcionar os pacotes de informação na rede da origem até o destino.

Inteligência Artificial - Técnicas utilizadas em programas normalmente para simular comportamento humano.

Intranet - São redes corporativas que utilizam a tecnologia e infra-estrutura de comunicação de dados da Internet. Utilizadas na comunicação interna da própria empresa e/ou comunicação com outras empresas.

IP - Endereço numérico que identifica de forma única um computador na internet.

Internet Relay Chat - Sistema que permite a conversação online entre várias pessoas.

Java - Linguagem de programação desenvolvida pela Sun Microsystem para uso na internet e que interliga diferentes tipos de computadores tais como PCs e Macs.

Javascript - Linguagem de programação derivada da linguagem Java que se encontra nas própria páginas da web.

Jaz Drive - Tipo de disco magnético que armazena grande capacidade de informação (em torno de 1 gigabyte).

JPEG /JPG (Joint Photographic Experts Group) - Algoritmo para comprimir imagens. Arquivos deste tipo costumam ser menores que os arquivos tipo GIF e possuem alto grau de fidelidade, permitindo armazenar imagens de até 16,7 milhões de cores. Para desenhos de até 256 cores, é recomendada a utilização do padrão GIF que gera arquivos menores neste caso.

Jurídico - Relativo, ou em conformidade, com os princípios do direito.

K - Em computação, corresponde ao valor 1024 (2 elevado a décima potência). Veja Mega.

KB - Significa Kilobyte. São 1024 bytes.

Keyword ou Palavra-Chave - Palavra usada em ferramentas de busca ou base de dados, que traz em si o significado de um assunto; assim, através dela, é possível localizar esse assunto.

Kilobyte (Kb) - Corresponde a 1024 bytes.

Kit Multimídia - Conjunto formado por placa de som, caixas de som e um dispositivo de leitura de CD-ROM que deve constar do computador para este ser considerado equipado para multimídia.

Lacete local - o circuito físico que liga o ponto terminal da rede nas instalações do utilizador final a um repartidor ou ao recurso equivalente na rede fixa de comunicações electrónicas públicas.

LAN (Local Area Network) - Qualquer rede tecnológica física de comunicações que opera em alta velocidade (10 a 100 Mbps) em curtas distâncias. Serve aos usuários dentro de uma área geográfica limitada.

LEGO-Logo - É um sistema onde os dispositivos construídos com as peças tradicionais do LEGO (blocos, tijolos, engrenagens, motores, polias, etc) podem ser controlados através de programas escritos na linguagem

LICITUDE permitido pela Lei, pelas normas da justiça, ou por qualquer princípio superior

Linha (Local Area Network) - Linha telefônica que fica permanentemente ligada entre dois lugares. Linhas dedicadas são encontradas frequentemente em conexões de tamanho moderado a um provedor de acesso.

Link - É a ligação de um item em um documento a outros documentos. Este link pode levar a um texto, uma imagem, som, vídeo, outro documento ou mesmo outro protocolo, através do seu endereço na Rede.

Linha dedicada - Linha telefônica com fim específico de prover uma conexão permanente entre duas redes. São bastante usadas para a conexão de uma rede local (LAN) a Internet.

Linhagem - Ligação de dois ou mais programas (ou subprogramas) distintos, acopulando-os, de modo a formarem um todo.

Link/Hiperlink - Elemento de ligação que leva a um outro ponto de ligação que pode estar na mesma página, em páginas diferentes no mesmo computador ou mesmo em páginas situadas em computadores que podem estar em pontos distintos do planeta.

Linux - Sistema operacional freeware no estilo do UNIX, que possui versão para computadores pessoais.

Lista de Discussão - Grupo de discussão sobre algum tema específico onde as mensagens são distribuídas por correio eletrônico àqueles que estão inscritos em tais listas.

Logo - Linguagem de computador Conjunto de palavras e símbolos que definem uma forma de criar programas mais amigável às pessoas.

Logo - palavra utilizada pela equipe coordenada pelos pesquisadores Seymour Papert e Marvin Minsky no Instituto de Tecnologia de Massachussets (MIT) para designar simultaneamente uma teoria de aprendizagem, uma linguagem de programação, um material que permite ao indivíduo demonstrar os processos mentais empregados na resolução de problemas num contexto de ação sobre o mundo exterior.

Logon - Procedimento de abertura de sessão de trabalho em um computador. Normalmente, consiste em fornecer para o computador um username (também chamado de login) e uma senha, que serão verificados se são válidos, ou não. Pode ser usado para fins de segurança ou para que o computador possa carregar as preferências de um determinado usuário.

Logoff - Trata-se da desconexão de um sistema de computação, geralmente selecionando um item de menu ou digitando exit, bye ou logout.

Macro - Pequena rotina de programação escrita numa linguagem de macros. Macros são excelentes recursos para realizar tarefas repetitivas e longas como, por exemplo, visualizar uma pequena linha de texto com todas as fontes instaladas no sistema ou, no Excel, realizar operações complexas com números variáveis.

Mainframe - Designativo do computador de grande porte ou do computador central de uma instalação. Atualmente, é preferentemente chamado de "servidor corporativo".

Máquina Fotográfica Digital - Máquina fotográfica que armazena as imagens sob a forma de números (dígitos binários) em arquivos que possam ser lidos por softwares gráficos. Algumas dessas máquinas gravam as fotos diretamente num disquete flexível de computador. As máquina fotográficas tradicionais guardam uma imagem análoga (similar, idêntica) a imagem real numa película especial (filme), por isso é chamada de imagem analógica em contraposição à imagem representada por dígitos numéricos (digitalizada).

Matéria classificada - É toda a informação que tem classificação, (área, notícia, material ou documento) que, se for do conhecimento de indivíduos não autorizados, pode fazer perigar a segurança nacional dos países aliados ou de organizações de que Portugal faça parte.

Material - É todo o documento, substância, elemento de máquina, de equipamento ou de arma, fabricado, em curso de fabricação, ou em estudo, bem como construções ou instalações, nomeadamente: Matérias-primas e manufacturadas; Modelos, montagens, cunhos, matrizes, chancelas e selos brancos; Trabalhos, edifícios e instalações; Armamento, munições e equipamento; Dados, programas, aplicações informáticas.

Matriz ativa - Tela de cristal líquido em que cada pixel na tela é um circuito separado e que pode ser ativado independentemente de qualquer outro pixel.

Matriz passiva - Tela de cristal líquido em que se utilizam cruzamentos de fios horizontais e verticais. Energizando cada fio, a interseção se ilumina, o que corresponde a um pixel, isto é, um ponto da imagem.

Mega - Valor que corresponde a 1024 vezes 1024. Há outras abreviaturas deste tipo, correspondendo a valores maiores que o mega, como G (giga) que equivale a 1024 mega, e o T (tera) que equivale a 1024 giga.

Megabyte - Corresponde a 1024 Kilobytes (Kb)

Megalogo - Versão da linguagem Logo desenvolvida para o ambiente Windows e que dispõe de recursos multimídia tais como sons, imagens animadas e vídeo.
Memória de computador

Memória - Circuitos, componentes ou partes mecânicas de um computador que armazenam informações.

Memória Alta, Reservada ou Superior - Em um PC, a porção de memória RAM principal (de 640 KB a 1024 KB) não utilizada pelo DOS para execução de programas. É ocupada (nos micros com placas de vídeo VGA) pela "memória de vídeo" (640 a 768 k) e pelo "BIOS VGA" (768 a 800 k), ficando vazia a área entre 800 k e 960 k que é utilizada como RAM quando usados programas gerenciadores de memória.

Memória Baixa ou Convencional - A memória RAM principal abaixo de 640k, que é facilmente acessada por todos os programas de DOS.

Memória Cache Primária - Área com cerca de 16 KB (32 KB na tecnologia MMX) de armazenamento temporário de dados existente no próprio processador. A maior parte dos dados necessários ao processamento fica à disposição nesse cache, reduzindo o número de leituras no disco. <

Memória Cache Secundária - Área com cerca de 256 KB (ou 512 KB atualmente) para armazenamento temporário de dados que melhora a velocidade do computador. Se encontra entre a CPU e a memória principal.

Memória Estendida - Toda a memória além de 1 MB (num computador com 8 MB de memória principal, existem 7 MB de memória estendida). Como o DOS foi desenvolvido para atuar somente no limite de 640 KB, toda essa memória ficou disponível para os aplicativos do sistema e não os do usuário. Seu melhor aproveitamento faz-se por programas gerenciadores.

Memória Expandida - Memória desenvolvida para que programas possam utilizar a memória principal acima do limite de 640 KB imposto pelo DOS, que geralmente a eleva a 4, 8, 16 Mb ou mais. É um tipo de memória normalmente não acessível a aplicativos rodando sob DOS. Requer o uso de um programa administrador de memória.

Memória Flash - Um tipo de chip de memória que retém as informações quando a energia elétrica é interrompida (memória não-volátil). Usado em alguns computadores para armazenar as informações relativas ao BIOS, que podem assim ser atualizados (sem que o chip BIOS seja substituído) à medida que surgem novos aperfeiçoamentos. A memória flash poderá ser usada no futuro para substituir unidades de disco rígido. Pode ser regravada dezenas de milhares de vezes, mas não infinitamente.

Memória Principal - Também chamada de Memória RAM ou Memória do Sistema, é a memória de trabalho do computador. Os dados e programas (incluindo o sistema operacional) ficam na memória RAM enquanto estão sendo processados. Quando um trabalho é concluído e arquivado e o programa encerrado, a memória RAM é liberada para novos dados e novos programas. Ela é dividida em Memória Convencional, Memória Reservada, e Memória Estendida ou Expandida.

Memória de Vídeo - Chips de memória usados por uma placa de vídeo para processar as imagens. Quanto mais memória uma placa tiver, maior será a resolução que ela pode atingir.

Memória Virtual - Memória oferecida pelo sistema operacional para ampliar o tamanho da memória principal do computador. Se trata de uma simulação da memória principal em disco, o que permite que o espaço de endereçamento do computador ultrapasse a memória física disponível. Ela é dividida em páginas, trazidas para a memória real quando necessárias.

Mercados transnacionais - os mercados referidos no n.º 5 do artigo 59.º que abrangem a União Europeia ou uma parte substancial desta, localizados em mais de um Estado membro.

Metadados - São informações detalhadas de comunicações tais como: destinatário, remetente, duração, data, local, tipo de computador ou telefone.

MIDI (Musical Instrument Digital Interface) - Uma maneira de armazenar músicas como uma série de instruções computadorizadas. O arquivo resultante pode ser reproduzido em uma ampla variedade de computadores e instrumentos eletrônicos. A porta MIDI serve de conexão com instrumentos musicais.

MMX (Multimedia Extensions) - Recurso evoluído de processadores que permite que o chip processe sons e imagens, melhorando a velocidade de processamento. Através dessa tecnologia, placas auxiliares de vídeo e som – e também periféricos como o fax/modem – podem ser substituídas por softwares.

Modem (MOdulator/DEModulator) - Dispositivo eletrônico que converte os sinais enviados pelo computador em sinais de áudio, que serão enviados ao longo das linhas telefônicas e recebidos por outro modem que irá receber o sinal sonoro e convertê-lo de volta em sinais entendidos pelo computador. O modem também disca a linha, responde à uma chamada e controla a velocidade de transmissão.

MPEG (Motion Pictures Experts Group) - Uma maneira de comprimir filmes para diminuir o tamanho dos arquivos e facilitar a reprodução. Um chip MPEG pode reproduzir filmes usando toda a tela.

MP3 (Mpeg Layer-3) - Tipo de arquivo utilizado para armazenar sons. Bastante popular na Internet.

Multitarefa - É a capacidade de um sistema operacional de executar várias tarefas (programas) simultaneamente.

Mirror - Servidor que contém uma duplicata de um site na Internet. Serve para diminuir o tráfego no site principal ou para tornar a transferência de dados mais rápida.

Modem (MODulador/DEModulador) - É um dispositivo que converte os sinais digitais gerados pelo computador em sinais analógicos modulados e vice-versa para permitir a sua transmissão por linhas telefônicas.

Multimídia - Combinação de imagens gráficas, aúdio, vídeo e texto.

Navegadores - Ver Browser.

Netiqueta - Conjunto de regras de etiqueta sobre o modo como o indivíduo deve proceder quando utiliza a rede, principalmente em relação ao correio eletrônico.

NetMeeting - Programa que possibilita a comunicação instantânea (onlline, em tempo real) de voz e dados na internet. Através desse programa duas ou mais pessoas situadas em locais diferentes (prédios, cidades, estados ou países) podem trabalhar simultaneamente (compartilhar) no mesmo aplicativo, transferir arquivos, ver e modificar a mesma tela que aparece no monitor de cada um dos participantes.

Netware - Sistema operacional para gerenciamento de redes locais baseadas em PCs.

Newsgroup - Grupo de dicussões sobre assuntos determinados abertos a qualquer pessoa que queira consultá-los e/ou respondê-los. No newsgroup as mensagens são dirigidas para um determinado grupo de interesse ficam disponíveis em determinados computadores chamados news servers (servidores de notícias). Os diversos news servers formam uma rede denominda usenet.

Nó - Qualquer dispositivo, inclusive servidores e estações de trabalho, ligados a uma rede.

No-Break - Ver Estabilizadores e No-Breaks.

Notebook - Computador pessoal portátil.

Núcleo de segurança - Órgão do canal técnico, funcionando na dependência directa dos directores dos estabelecimentos, empresas, organismos ou serviços, destinado a dar apoio em todas as atribuições na área da segurança, de acordo com as presentes normas.

Número - o recurso do Plano Nacional de Numeração ou o recurso de um plano internacional de numeração, em que a ARN tem competências nomeadamente de notificação, que serve para identificar assinantes, serviços ou aplicações, empresas que oferecem redes ou serviços, redes ou elementos de rede.

Número geográfico - o número do Plano Nacional de Numeração que contém alguns dígitos com significado geográfico, cuja função é encaminhar as chamadas para o local físico do ponto de terminação de rede (PTR).

Número não geográfico - o número do Plano Nacional de Numeração que não seja um número geográfico, incluindo, nomeadamente, os números móveis, de chamadas gratuitas para o chamador e de tarifa majorada.

Oferta de rede de comunicações electrónicas - o estabelecimento, operação, controlo ou disponibilização da referida rede.

Office - Pacote de softwares da Microsoft composto basicamente por editor de textos (Word), planilha eletrônica (Excell), banco de dados (Access) e programa de apresentação (Power Point).

Offline - Comunicação ou operação que é feita quando o computador não estiver conectado a outro.

Online - Qualquer atividade executada enquanto o computador estiver conectado a um outro computador ou rede.

Operador - uma empresa que oferece ou está autorizada a oferecer uma rede de comunicações pública ou um recurso conexo.

Organismo de Reguladores Europeus das Comunicações Electrónicas (ORECE) - o organismo criado pelo Regulamento (CE) n.º 1211/2009, do Parlamento Europeu e do Conselho, de 25 de Novembro.

Organismo de segurança designado - ministério, serviço ou organismo governamental designado por uma nação membro como responsável pela coordenação e execução da política nacional em matéria de segurança industrial.

OS/2 - Sistema operacional criado pela IBM para PCs.

Overdrive - Tipo de processador que se encaixa sobre o chip já existente e lhe dá um ganho de velocidade de processamento. Dessa forma, efetua-se um upgrade no sistema.

Package - Programa ou conjunto de programas concebidos para resolver problemas genéricos, comercializados como produto acabado.

Packet - Em uma transmissão por rede, os dados são desmembrados em pequenas porções chamadas de "pacotes". O tamanho dos "pacotes" pode variar de 40 até 32.000 bytes, dependendo da rede. Normalmente menos de 1.500 bytes.

Packet Radio (Rádio Pacote) - Sistema de comunicação à distância usando um computador conectado a um aparelho de radioamador. O sistema funciona de forma similar à internet, onde o telefone é substituído por um aparelho de radioamador e o modem dá lugar a uma caixa denominada TNC (Terminal Node Control – Controlador de Nó de Terminal). As informações são transmitidas pelas ondas de rádio em pequenos pacotes (packets) de cada vez (daí o nome rádio-pacote)

Paint - Sotware que acompanha o Windows usado para edição e elaboração de gráficos (desenhos, imagens em geral)

Par Trançado - Cabo de rede ou telefone de baixo custo produzido por pares de fios de cobre trançados uns aos outros, fazendo com que se cancelem os efeitos de ruídos elétricos.

Password - Conjunto de caracteres previamente escolhidos (pessoal e intransmissível) pelo utilizador e que permite o acesso a sistemas, dados ou programas.

Pasta - Ver diretório.

PC (Personal Computer – computador pessoal) - Primeiro computador pessoal, de onde surgiu o nome. Termo que designa computadores que utilisam processador da família Intel e compatíveis. Incluem desde o PC-XT, AT até o atual Pentium III.

PC-Speaker - Auto-falante interno do computador pessoal. Permite a reprodução de sons não muito complexos.

PCI (Peripheral Component Interconnect) - Interconexão de componentes periféricos. Um padrão de barramento local inventado pela Intel que permite a adição de até 10 dispositivos de barramento local e suporta operação simultânea da CPU e do barramento mestre. Suporta também o processador Pentium de 64 bits. Veja USB.

PDF (Portable Document Format) - Formato de arquivo criado pela Adobe. O PDF permite o envio de documentos formatados para que sejam vistos ou impressos em outro lugar, sem a presença do programa que o gerou. Os arquivos PDF são criados pelo programa Adobe Acrobat, que se compõe de duas partes: um gerador e um leitor de arquivos. O primeiro (Acrobat) é vendido pela Adobe; o outro (Acrobat Reader) é distribuído gratuitamente (www.adobe.com).

Periférico - Componentes de hardware através dos quais os utilizadores comunicam com o sistema informático, terminais, impressoras, scanner, sintetizador de voz, etc.

Pessoa não autorizada - elemento que não está credenciado nem autorizado a ter acesso a matérias classificadas ou que, embora credenciado, não conste das respectivas listas de acesso, nos termos da SEGNAC 2.

PIF (Program Information File) - Arquivo que contém informações sobre que medidas o Windows 3.x deverá tomar quando for executar um programa desenvolvido para rodar sob DOS. Na maioria das

vezes, os arquivos PIF guardam informações sobre o uso da memória, administração da janela, do mouse, e de outros detalhes.

Pixel (Picture Element) - É o menor ponto de luz cuja cor e luminosidade podem ser controladas na tela. As imagens são formadas com a combinação de grande número de pixels. O termo é usado para se referir a resolução de uma placa de vídeo ou monitor (ex: 800 x 600 pixels).

Placa de Som - Componente interno do microcomputador, conectado à placa mãe. Possibilita a reprodução de sons com bastante fidelidade.

Planilha Eletrônica - São programas que foram inspirados nos antigos livros de contabilidade e realizam cálculos complexos. Exemplo: Excel.

Placa Mãe - Componente interno do microcomputador, localizado dentro do gabinete. É a placa que interliga todos os outros componentes do computador.

Porta Paralela - Tipo de conexão que transmite oito bits simultaneamente, mas seguem uma única direção. Seu uso mais comum em PCs é para conectar a impressora, e por isso é conhecida como LPT1 (do inglês Line Printer), mas também serve de entrada para Zip-drives e câmeras de vídeo conferência.

Porta Serial - Tipo de conexão bidirecional, através da qual os bits fluem um de cada vez (em série). Esta conexão é feita por dois fios de dados. Isto significa que uma porta serial pode enviar e receber informações simultaneamente. Normalmente os PCs têm pelo menos duas delas, conhecidas como COM1 e COM2, que podem ser usadas para conectar diversos dispositivos, como um mouse, modem, ou notebook.

Posto público - o equipamento terminal em local fixo acessível ao público em geral, cuja utilização pode ser paga com moedas e ou cartões de crédito/débito e ou cartões de pré-pagamento, incluindo cartões a utilizar com códigos de marcação.

Ponto de terminação de rede (PTR) - o ponto físico em que é fornecido ao assinante acesso à rede de comunicações públicas; no caso das redes que envolvem comutação ou encaminhamento, o PTR é identificado através de um endereço de rede específico, que pode estar associado ao número ou nome de um assinante.

PostScript - Padrão usado para impressão de gráficos.

PPP (Point to Point Protocol) - Protocolo de comunicação entre computadores por linha telefônica usado para conexão internet.

Processador - Componente interno do computador. É o "cérebro" do computador, quem faz o processamento de dados e instruções. Fica conectado à placa mãe .

Processamento em tempo real - Modo de funcionamento de um sistema informático em que as informações provenientes dos periféricos são imediatamente processadas, actualizando os ficheiros.

Programa - Sequência de instruções a ser executada pelo computador.

Protecção criptofónica - Protecção resultante da conversão de linguagem clara para linguagem ininteligível, destinada a proteger as comunicações contra intercepção não autorizada.

Protocolo - Uma designação formal dos formatos de mensagens e de regras de dois computadores que precisam ser seguidos para que possa haver troca de mensagens, incluindo o controle de fluxo (início-fim), a detecção ou correção de erros e os parâmetros (bits de dados, bits de parada, paridade). O padrão de protocolos que permite computadores de diferentes usuários comunicarem-se, fazendo com que programas "rodem" em ambos, concordando com os dados contidos. O protocolo básico utilizado na Internet é o TCP/IP

Provedor - Empresa que presta serviços de acesso à Internet.

Provedor de Acesso ou Provider - Empresa que presta serviço de conexão à Internet, tornando possível o acesso através de uma ligação telefônica, geralmente local.

Proxy - Um servidor que se encontra entre um computador cliente e um servidor de FTP ou HTTP, por exemplo. Ele é utilizado para acelerar a requisição ou por questões de segurança.

Psicosegundos - Medida (1 × 10-12) em segundos, que será usada futuramente por toda a fibra ótica, alcançando instruções da ordem de um trilião por segundo.

Quebra de segurança - É toda a acção contrária ou omissa aos regulamentos de segurança em vigor que faça perigar ou possa comprometer as matérias classificadas.

Quicktime - Formato de vídeo lançado pela Apple para compactação e transmissão de vídeo via Internet.

RAM (Random Access Memory) - Memória cujas informações armazenadas podem ser alteradaas pelo usuário. As informações existentes na RAM não são estáveis e, caso não sejam salvas no disco, serão perdidas ao se desligar o computador. Veja Memória Principal.

Recursos conexos - os serviços associados, as infra-estruturas físicas e outros recursos ou elementos associados a uma rede de comunicações electrónicas e ou a um serviço de comunicações electrónicas que permitem e ou servem de suporte à oferta de serviços através dessa rede e ou serviço, ou têm potencial para fazê-lo, e incluem nomeadamente edifícios ou entradas de edifícios, cablagem de edifícios, antenas, torres e outras estruturas de apoio, condutas, tubagens, postes, câmaras de visita e armários.

Rede - Conjunto de computadores interligados, compartilhando um conjunto de serviços.

Rede de comunicações electrónicas - os sistemas de transmissão e, se for o caso, os equipamentos de comutação ou encaminhamento e os demais recursos, nomeadamente elementos de rede que não se encontrem activos, que permitem o envio de sinais por cabo, meios radioeléctricos, meios ópticos, ou por outros meios electromagnéticos, incluindo as redes de satélites, as redes terrestres fixas (com comutação de circuitos ou de pacotes, incluindo a Internet) e móveis, os sistemas de cabos de electricidade, na medida em que sejam utilizados para a transmissão de sinais, as redes de

radiodifusão sonora e televisiva e as redes de televisão por cabo, independentemente do tipo de informação transmitida.

Rede de comunicações públicas - a rede de comunicações electrónicas utilizada total ou principalmente para o fornecimento de serviços de comunicações electrónicas acessíveis ao público.

ROM – BIOS - Chip usado pelos fabricantes para colocar no computador programas ou informações de forma permanente. O termo ROM (Read Only Access Memory) se refere a um tipo de memória cujos dados vem gravados da fábrica e não podem ser alterados.

RTV - Abreviação para placas que permitem que o usuário possa assistir TV ou sintonizar estação de rádio FM. Uma das principais vantagens deste recurso, é o uso simultâneo dos recursos da placa, com outros aplicativos do equipamento.

Raiz (Root) - Designa o diretório de onde derivam todos os outros. O mais alto na hierarquia. O termo root também se refere a superusuário.

Realidade Virtual - Ambiente artificial criado com recursos computacionais que é apresentado ao usuário de modo que pareça com um ambiente real.

RealPlayer - É um programa que permite ao navegador exibir áudio e vídeo numa pequena janela que se abre na tela da pagina onde o recurso foi inserido. Dessa forma podemos ouvir musica, assistir a um vídeo/videoclip qualquer, assistir ou participar de uma videoconferência transmitida pela internet e ver imagens captadas por câmeras colocadas em locais previamente escolhidos.

Rede local - Ver LAN.

Robótica - Área interdisciplinar envolvendo a engenharia mecânica, elétrica, eletrônica e ciência da computação. A robótica educacional ou pedagógica caracteriza ambientes de aprendizagem onde são reunidos materiais de sucata ou kits de montagens composto por peças diversas e controlados por computador e softwares que permitam programar o funcionamento de modelos construídos.

RTF (Rich Text Format) - Formato de documentos de texto suportado por vários editores de texto.

Redes sociais - Facebook...

Responsável pelos subcontratos - representante de uma firma, devidamente designado, que está habilitado a negociar, a adjudicar ou a superintender subcontratos em nome da firma para realização de trabalhos classificados.

Responsável do sistema informático - Pessoa a quem compete gerir o sistema informático. Basicamente, faz parte das suas atribuições a implantação da metodologia para exploração dos equipamentos informáticos e desenvolvimento de projectos informáticos.

Roll back - Reposição dos dados na sua situação inicial, após erro ou avaria durante a execução de uma transacção.

Sabotagem - É a destruição, ruína ou avaria intencional de equipamento ou parte do equipamento, material ou instalações por elementos hostis ou a favor destes.

Script - Descrição de uma tarefa complexa ou de uma série de tarefas usando uma determinada linguagem, chamada de A linguagem de scripts. O script permite que o procedimento nele descrito seja executado automaticamente.

Segmentos de informação - São assuntos de âmbito: militares e de segurança, políticas e sociais, económicas e empresariais, científicas e tecnológicas.

Segurança - Um estado que se alcança quando a informação classificada, o pessoal, as instalações e as actividades estão protegidas contra a espionagem, sabotagem, terrorismo e subversão, bem como contra perdas ou acesso não autorizado. O termo também se aplica às medidas necessárias para se conseguir aquele estado e às organizações responsáveis por estas medidas.

Segurança das operações - processo que confere a uma operação ou movimentação a segurança apropriada, usando meios ativos ou passivos, para negar ao inimigos o conhecimento dos dispositivos, capacidades e intenções de opositores.

Segurança do pessoal - a parte da segurança que se preocupa com todas as medidas relacionadas com o pessoal destinadas a neutralizar as ameaças postas pelos serviços de informação hostis ou por pessoas ou organizações subversivas.

Segurança electrónica (ELSEC) - Protecção resultante de todas as medidas destinadas a negar a pessoas não autorizadas notícias que possam ser obtidas pela intercepção e estudo de radiações electromagnéticas (extracomunicações).

Segurança física - A parte de segurança que se preocupa com as medidas físicas destinadas a salvaguardar o pessoal e prevenir acessos não autorizados a informações, materiais e instalações, contra a espionagem, sabotagem, danificação e roubo, tanto nos locais de fabrico ou armazenagem como durante deslocações.

Segurança informática - salvaguarda dos sistemas de processamento automático de dados e prevenção da divulgação, distorção ou destruição ilícita das informações classificadas.

Segurança protectiva - sistema organizado de medidas defensivas instituído e mantido a todos os níveis, com o objectivo de obter e manter a segurança.

Segurança das telecomunicações (COMSEC) - protecção resultante de todas as medidas destinadas a negar, a pessoas não autorizadas, notícias que possam ser obtidas por intercepção e estudo das telecomunicações ou para confundir as pessoas não autorizadas nas suas interpretações dos resultados de tal estudo. Inclui a segurança física das instalações, segurança do pessoal, segurança dos meios e processos de transmissões, segurança criptográfica, segurança informática e segurança das radiações.

Servidor - Computador que controla acesso aos recursos de uma rede, como diretórios e impressoras. Hoje em dia, em tempos de Internet, o termo "servidor" representa bem mais. Na Net, servidor é aquela máquina que oferece serviços a quem fizer acesso a ela. Um servidor de Web, por exemplo, "serve" home page; um servidor de FTP serve arquivos; um servidor de IRC ofereçe serviços de bate-papo eletrônico, também conhecido como "chat". E assim por diante.

Serviço de comunicações electrónicas - o serviço oferecido em geral mediante remuneração, que consiste total ou principalmente no envio de sinais através de redes de comunicações electrónicas, incluindo os serviços de telecomunicações e os serviços de transmissão em redes utilizadas para a radiodifusão.

Serviços conexos - os serviços associados a uma rede de comunicações electrónicas e ou a um serviço de comunicações electrónicas que permitem e ou servem de suporte à oferta de serviços através dessa rede e ou serviço, ou têm potencial para fazê-lo, e incluem nomeadamente os sistemas de conversão de números ou os sistemas que oferecem uma funcionalidade equivalente, os sistemas de acesso condicional e os guias electrónicos de programas, bem como outros serviços como o serviço de identidade, localização e presença.

Serviço de televisão de ecrã largo - um serviço de programas televisivo constituído, na totalidade ou em parte, por programas produzidos e editados para serem apresentados em todo um ecrã de formato largo, sendo o formato 16:9 o formato de referência para estes serviços.

Serviço telefónico acessível ao público - o serviço ao dispor do público que permite fazer e receber, directa ou indirectamente, chamadas nacionais ou nacionais e internacionais através de um número ou de números incluídos num plano nacional ou internacional de numeração.

Serviço universal - o conjunto mínimo de serviços, definido na presente lei, de qualidade especificada, disponível para todos os utilizadores, independentemente da sua localização geográfica e, em função das condições nacionais, a um preço acessível.

Shareware - Software disponível em muitos locais da Internet. Inicialmente, o software é grátis, mas os autores esperam que o pagamento seja enviado depois de um período inicial de testes. Normalmente, os preços são baixos. É uma espécie de “teste antes e pague depois”.

SIMM (Single Inline Memory Module) - Tipo de módulo de memória mais comum nos PCs. É uma pequena placa de circuitos impresso contendo vários chips de memória.

Sistema de acesso condicional - qualquer medida e ou disposição técnica, por meio da qual o acesso, de forma inteligível, a um serviço de programas televisivos ou de rádio protegido fica condicionado a uma assinatura ou a qualquer outra forma de autorização prévia individual.

Sistema informático - Conjunto formado por equipamentos informáticos, instruções, normas, procedimentos, pessoal e meios de transmissão de tal modo organizado e interligado que permita trabalhar e comunicar informações.

Sistema No break - Unidade que garante o fornecimento ininterrupto de energia ao equipamento, em caso de falha no abastecimento do exterior.

Sistema Operacional - Software que tem como função controlar a alocação de recursos tais como: comunicação com os usuários, espaço em discos, uso de memória, tempo que cada programa pode rodar, etc. DOS, Windows NT e UNIX são sistemas operacionais.

Sistema operativo - Conjunto de programas que fazem a gestão dos recursos de um sistema informático.

SITE - Um endereço dentro da Internet que permite acessar arquivos e documentos mantidos no computador de uma determinada empresa, pessoa, instituição. Existem sites com apenas um documento; o mais comum, porém, principalmente no caso de empresas e instituições, é que tenha dezenas ou centenas de documentos.

Slots - Locais físicos dentro da CPU de um computador em que se encaixam as placas de vídeo, memória e de recursos de expansão em geral.

Software - Termo utilizado para indicar programas ou conjuntos de programas. Pode ser traduzido por suporte lógico.

Software-house - Empresa dedicada à realização de programas.

Software de base - Conjunto de programas geralmente fornecidos com o equipamento, tais como o sistema operativo, subsistemas, compiladores, etc.

Software de Domínio Público (Freeware) - Um programa não protegido por copyright, que pode ser utilizado sem que seja necessário fazer alguma forma de pagamento para o seu autor.

Subcontratante - entidade industrial, comercial de ensino ou qualquer outra entidade que tenha efectuado um contrato com um contratante principal ou com outro subcontratante para prestação de um serviço ou fabrico de um artigo, como contribuição parcial de um contrato classificado, e que é obrigada a respeitar as regras de segurança estabelecidas, em função do grau de classificação de segurança do subcontrato.

Sublacete local - um lacete local parcial que liga o ponto terminal da rede nas instalações do utilizador final a um ponto de concentração ou a um repartidor intermédio especificado na rede fixa de comunicações electrónicas públicas.

Subversão - Acção destinada a enfraquecer o potencial militar, económico e político de uma nação, minando o moral, a lealdade e a confiança dos seus cidadãos.

Suporte informático - Discos magnéticos ou ópticos, bandas magnéticas, disquettes, cassettes ou cartridges, sobre os quais se podem registar dados.

SVGA (Super Video Graphics Array) - Significa qualquer modo de vídeo igual ou superior à resolução de 640×480 pontos com 256 cores ou mais.

TCP/IP (Transmission Control Protocol/ Internet Protocol) - Os dois protocolos básicos da Internet, usados para viabilizar a transmissão e troca de dados de redes diferentes, permitindo assim que os computadores se comuniquem. Foi criado em 1970 pelo governo americano. Como o TCP/IP foi desenvolvido a partir de fundos públicos, ele não pertence a uma empresa específica e pode ser utilizado por qualquer computador para o compartilhamento de informações com outro computador.

Tecnologias - É um conjunto diverso de instrumentos técnicos, que permite através de métodos e processos específicos substituir a forma de execução levada a cabo pelo Homem, de uma forma mais eficaz.

Telecomunicação - Transmissão, receção ou emissão de sinais representando símbolos, escrita, imagens, sons ou informações de qualquer natureza, por fios, por sistemas óticos, por meios redioeléctricos e por outros sistemas eletromagnéticos

Teleprocessamento - Transmissão à distância da informação emitida ou recebida por um sistema informático, devidamente codificada e sem alterar o seu significado.

Tempest - Equipamento informático que não emite radiações nem emana sinais eléctricos ou electromagnéticos para o exterior.

Terrorismo - o uso sistemático da intimidação, por meios violentos ou não, para fins políticos.

TIC - Tecnologias de Informação e Comunicação

Tiff (Tagged Image File Format) - Um tipo de arquivo para a armazenagem de gráficos e figuras de alta qualidade, desenvolvido pela Aldus e pela Microsoft. Especialmente prático para transferir entre computadores PC e Macintosh.

TPI - Tribunal Penal Internaional.

Transito - A passagem de qualquer tipo de bens que tenha como destino outro local.

True Color Video Card - Uma placa de vídeo que pode exibir 16,7 milhões de cores – que é aproximadamente o maior número de cores que o olho humano pode distinguir em um monitor.

UART - Acrônimo de Universal Asynchronous Receiver/Trasmitter ou "Trasmissor/Receptor assíncrono Universal". Transmite e recebe todos os dados durante comunicações seriais. Os projetos mais antigos de UART, como 0 8250 e o 16450 podem ter problemas com as comunicações e operações de alta velocidade dos ambientes multitarefa. O projeto de 16550 alivia esses problemas através da incorporação de um buffer FIFO (First-in/First-out) – o primeiro que entra é o primeiro que sai – de 16 bytes.

UNSCOM (United Nations Special Commission) - É onde operam NSA, CIA os serviços de informações Israelitas e Britânicos.

URL (Uniform Resource Locator) - É o sistema de endereçamento e localização utilizado pelo WWW e um padrão de endereçamento proposto para toda a Internet. Os endereços usados na Web, por exemplo (http://www.microtec.com.br) são URLs.

USB (Universal Serial Bus) - Nova interface para conexão ao micro, com funcionamento Plug and Plaay, capaz de receber de maneira simples e rápida até 127 dispositivos externos, ligados por meio de um computador. O barramento nas portas USB atinge 12 Mbps, enquanto nas portas seriais a velocidade máxima é 115 Kbps, velocidade que vai favorecer, sobretudo, a utilização dos DVDs.

Username (Nome do Usuário ou ID) - Nome pelo qual o Sistema Operacional identifica o usuário.

Utilizador - a pessoa singular ou colectiva que utiliza ou solicita um serviço de comunicações electrónicas acessível ao público.

Utilizador final - o utilizador que não oferece redes de comunicações públicas ou serviços de comunicações electrónicas acessíveis ao público.

Violação de dados pessoais - Uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais

transmitidos, armazenados ou de outro modo tratados no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público.

Violação de segurança - Ver quebra de segurança.

Vírus informático - Programas propositadamente inseridos no sistema informático com intenção de impedir ou dificultar o seu funcionamento. Alguns tipos de vírus estão programados de modo a corromper a integridade dos dados.

Vírus - São programas desenvolvidos para alterar nociva e clandestinamente softwares instalados em um computador. Eles têm comportamento semelhante ao do vírus biológico: multiplicam-se, precisam de um hospedeiro, esperam o momento certo para o ataque e tentam se esconder para não serem exterminados. Estão agrupados em famílias (boot, arquivo e programa), com milhares de variantes.

VL-Bus - Um padrão de barramento local desenvolvido pela VESA (Video Eletronics Standards Association) que permite que os didpositivos sejam conectados diretamente ao barramento do processador e operem em suas velocidades de clock. O VL-Bus pode suportar até três dispositivos de barramento local e é uma simples extensão do barramento padrão ISA ou EISA. Veja PCI.

VRAM - Memória especialmente rápida, usada nas placas de vídeo mais sofisticadas. Utilizada para armazenar imagens digitalizadas. Veja RAM.

V.90 - Padrão de comunicação para modems de 56 Kbps, aprovada em fevereiro deste ano pela União Internacional de Telecomunicação (ITU). O V.90 combina duas tecnologias concorrentes: X2, da 3Com, e K56Flex, da Rockwell. Os novos modems fabricados pelas duas empresas são compatíveis com o padrão.

Wav - Tipo de formato de arquivo de som do Windows.

Webmaster - A pessoa responsável pela administração de um host WWW.

Workgroup - Grupo de pessoas que trabalham juntas e compartilham os mesmos arquivos e bancos de dados numa rede local. Softwares especiais coordenam o grupo de trabalho e permitem que os usuários editem arquivos e atualizem bancos de dados harmoniosamente.

Workstations - Computadores que, embora fisicamente sejam parecidos com os computadores pessoais, têm uma capacidade de processamento muito superior. São usadas na computação gráfica (televisão e filmes), serviços de metereologia, aplicações científicas e de engenharia, etc. Apresentam processadores mais poderosos, maior quantidade de memória RAM e sistemas operacionais mais avançados e estáveis como Unix e Windows NT.

World Wide Web (WWW) - Literalmente, teia de alcance mundial. Serviço que oferece acesso, através de hiperlinks, a um espaço multimídia da Internet. Responsável pela popularização da Rede, que agora pode ser acessada através de interfaces gráficas de uso intuitivo, como o Netscape, o Web possibilita uma navegação mais fácil pela Internet. A base da WWW é a hipermídia, isto é, uma maneira de conectar mídias como texto, sons, vídeos e imagens gráficas. Através destas conexões hipermídia, você pode navegar pelos assuntos de seu interesse.

x86 - Série de microprocessadores fabricados pelo fabricante americano Intel. O mais antigo, desenvolvido no início dos anos 80, era o 8086, que deslanchou a indústria do Personal Computer (computador pessoal). Os chips cresceram em poder de processamento para o 286, 386 e 486 e, mais recentemente, o Pentium II e Pentium III.

Y2K - É a abreviatura de Year 2000 – Ano 2000

Zip Drive - Disco flexível de alta capacidade desenvolvido pela Iomega, que também fabrica o Jaz Drive. Mais espessos e ligeiramente maiores que os disquetes de 3,5 polegadas, os discos do Zip Drive têm espaço para guardar até 100 MB de informações. Eles são hoje a mídia mais popular para backup ou transporte de dados.

LEGISLAÇÃO

Acções Encobertas - Lei n.º 101/2001, de 25 de Agosto

Aprova medidas de combate à corrupção - Lei n.º 19/2008, de 21 de Abril

Brigadas Anticrime e Unidades Mistas de Coordenação - DL n.º 81/95, de 22 de Abril

Comércio Electrónico no Mercado Interno e Tratatamento de Dados Pessoais - DL n.º 7/2004, de 07 de Janeiro

Conservação de Dados Gerados ou Tratados no Contexto Oferta de Serviços de Comunicações Electrónicas - Lei n.º 32/2008, de 17 de Julho

Construção, Acesso e Instalação de redes - DL n.º 123/2009, de 21 de Maio

Convenção sobre o Cibercrime - Resolução da AR n.º 88/2009, de 15 de Setembro

Constituição da República Portuguesa - Decreto de 10 de Abril de 1976

Código Civil - DL n.º 47344/66, de 25 de Novembro

Código de Processo Civil (Novo) - Lei n.º 41/2013, de 26 de Junho

Código de Processo Penal - DL n.º 78/87, de 17 de Fevereiro

Convenção das Nações Unidas Contra a Corrupção - Resolução da AR n.º 47/2007, de 21 de Setembro

Convenção do CE sobre Branqueamento, Perda de Bens, Financiamento do Terrorismo - Resolução da AR n.º 70/97, de 13 de Dezembro

Convenção Penal Sobre a Corrupção, do Conselho da Europa - Resolução da AR n.º 68/2001, de 26 de Outubro

Condições e Procedimentos para Instituir o Sistema Integrado de Informação Criminal - Lei n.º 73/2009, de 12 de Agosto

Emissão e Execução de Decisões de Apreensão de Bens ou Elementos de Prova na U. E. - Lei n.º 25/2009, de 05 de Junho

Estabelece Competências das Unidades da Polícia Judiciária - DL n.º 42/2009, de 12 de Fevereiro

Estatuto Profissional do Pessoal com Funções Policiais da Polícia de Segurança Pública - DL n.º 243/2015, de 19 de Outubro

Intercâmbio de Dados e Informações de Natureza Criminal na União Europeia - Lei n.º 74/2009, de 12 de Agosto

Lei da Protecção de Dados Pessoais - Lei n.º 67/98, de 26 de Outubro

Lei das Comunicações Electrónicas - Lei n.º 5/2004, de 10 de Fevereiro

Lei do Cibercrime - Lei n.º 109/2009, de 15 de Setembro

Lei Orgânica do Gabinete Nacional de Segurança - DL n.º 3/2012, de 16 de Janeiro

Lei da Cooperação Judiciária Internacional em Matéria Penal - Lei n.º 144/99, de 31 de Agosto

Lei do Combate ao Branqueamento de Capitais e do Financiamento ao Terrorismo - Lei n.º 25/2008, de 05 de Junho

Lei de Organização da Investigação Criminal - Lei n.º 49/2008, de 27 de Agosto

Lei de Política Criminal - Biénio de 2015-2017 - Lei n.º 72/2015, de 20 de Julho

Lei Quadro da Política Criminal - Lei n.º 17/2006, de 23 de Maio

Lei da Organização do Sistema Judiciário - Lei n.º 62/2013, de 26 de Agosto

Lei de Organização e Funcionamento dos Tribunais Judiciais (NLOFTJ) - Lei n.º 52/2008, de 28 de Agosto

Lei de Organização da Investigação Criminal - Lei n.º 49/2008, de 27 de Agosto

Lei de Combate ao Terrorismo - Lei n.º 52/2003, de 22 de Agosto

Medidas Combate à Corrupção e Criminalidade Ec. e Financeira - Lei n.º 36/94, de 29 de Setembro

Medidas de Combate à Criminalidade Organizada - Lei n.º 5/2002, de 11 de Janeiro

Orgânica da Polícia Judiciária - Lei n.º 37/2008, de 06 de Agosto

Protecção de Dados Pessoais e Privacidade nas Telecomunicações - Lei n.º 41/2004, de 18 de Agosto

Protecção Jurídica das Bases de Dados - DL n.º 122/2000, de 04 de Julho

Protecção Jurídica de Programas de Computador - DL n.º 252/94, de 20 de Outubro

Protocolo Adicional à Convenção sobre o Cibercrime - Resolução n.º 91/2009, de 15 de Setembro

Regime Jurídico Aplicável ao Tratamento de Dados - Sistema Judicial - Lei n.º 34/2009, de 14 de Julho

Regras Aplicáveis à Identificação dos Processos Crime - Portaria n.º 1223-A/91, de 30 de Dezembro

Regulamento da Lei de Acesso ao Direito - Portaria n.º 10/2008, de 03 de Janeiro

Regula a Utilização de Câmaras de Vídeo - Lei n.º 1/2005, de 10 de Janeiro

Sistemas de Vigilância Electrónica Rodoviária - Lei n.º 51/2006, de 29 de Agosto

Sistemas de Vigilância Rodoviária e Tratamento da Informação - DL n.º 207/2005, de 29 de Novembro

Tramitação Eletrónica dos Processos Judiciais - Portaria n.º 280/2013, de 26 de Agosto

23ª Alteração ao Código Penal - Lei n.º 59/2007, de 04 de Setembro

REFERÊNCIAS BIBLIOGRÁFICAS

Agra, C. (1986). Projecto da psicologia transdisciplinar do comportamento desviante e auto-organizado. Análise Psicológica, IV (3/4), 311-318.

Anes, J. (2010). Organizações criminais. Ensaios. Universidade Lusíada. Lisboa.

Baud, J. (2005), Le Renseignement et la Lutte Contre le Terrorisme. Paris: Lavauzelle.

Berkowitz, B. et al. (2000), Best Truth, Intelligence in the Information Age. New Haven: Yale University Press.

Betts, R. (2007), Enemies of Intelligence, Knowledge and Power in American National Security. New York: Columbia University Press.

Blanc, M. Ouimet, M. & Szabo, D. (Coords.). (2003). Tratado de criminologia empírica. Montréal, Climepsi.

Birkinshaw, P. (1990). Reforming the secret state, University Press, Milton Keynes-Philadelphia.

Braz, J. (2009). Investigação criminal: Os desafios da nova criminalidade. Coimbra, Almedina.

Carmo, R. (2005). A prova pericial: Enquadramento legal. In R. A. Gonçalves & C. Machado (Coords.), Psicologia Forense (pp. 33-54). Coimbra: Quarteto.

Castells, M. (2011). A sociedade em rede. Fundação Calouste Gulbenkian. Lisboa.

Castro, C. (2005). Direito da informática, Privacidade e dados pessoais. Almedina. Coimbra.

Clark, R. (2007), Intelligence Analysis: a Target-Centric Approach. Washington: CQ Press.

Crelinsten, R. (2009), Counterterrorism. Cambridge: Polity Press.

Costa, J. (1998). Direito Penal da comunicação, Alguns escritos. Coimbra Editora.

Cradock, P. (2002). Know your Enemy: How the joint intelligence committee saw the world, London.

Denécé, É. (2008), Renseignement et Contre-Espionnage. Actions Clandestines, Technologies, Services Secrets. Paris : Hachette.

Demo, P. (1981). Metodologia científica em ciências sociais. Atlas. São Paulo.

Diário de Bordo. (2010). I Congresso Nacional de Segurança e Defesa. Europress. Lisboa.

Dias, J. Andrade, M. (1992). Criminologia: o homem delinquente e a sociedade criminógena. Coimbra: Coimbra.

Dulles, A. (2006), The Craft of Intelligence. Connecticut: Lyons Press.

Farson, S. (2000). Parliament and its servants: their role in scrutinizing canadian intelligence, in intelligence and nacional security, A Frank Cass journal.

Ferguson, H. (2004), Spy: a Handbook. London: Bloomsbury.

Fonseca, A. C. (Ed.). (2004). Comportamento anti-social e crime – Da infância à idade adulta. Coimbra: Almedina.

Ganor, B. (2005), The Counter-Terrorism Puzzle, New York: Transaction Publishers.

Ganor, B. (2012), "Dilemmas and Challenges for the Israel Intelligence Community in Fighting Terrorism", in Gilboa, Amos et al. [ed.] Israel`s Silent Defender, An Inside Look at Sixty Years of Israeli Intelligence. Jerusalem: Gefen Publishing House.

Gill, P. (1994). Policing Politics: Security intelligence and the Liberal democratic state. Frank Cass: London.

Glenny, M. (2008). McMáfia: O crime organizado sem fronteiras. Civilização Editora. Barcelos.

Gómez, A. (2007), "Doctrina de Infiltración para Inteligencia Contraterrorista", in Athena Paper, vol. 2 (3), pp. 1-23.

Herman, M. (2007), Intelligence Power in Peace and War. New Jersey: Princeton University Press.

IDN Cadernos. (2012). Contributos para uma estratégia abrangente de gestão de crises. IDN. Lisboa.

IDN Cadernos. (2013). Estratégia da Informação e segurança no ciberespaço. IDN. Lisboa.

Jacobs, G. Meliá, M. (2007). Direito penal do inimigo – noções e críticas. 2. ed. Porto Alegre: Livraria do Advogado.

Jesus, J. (2015). Espionagem e Contraespionagem em Portugal. Edições 70. Lisboa.

Johnson, L. (ed.) (2010), The Oxford Handbook of National Security Intelligence. New York: Oxford University Press.

Joint Chiefs of Staff (1993), Joint Tactics, Techniques and Procedures for Antiterrorism - JP 3-07.2, U.S. Army.

Jones, I. (2010), The Human Factor, Inside the CIA´s Dysfunctional Intelligence Culture. New York: Encounter Books.

Kent, S. (1951), Strategic Intelligence For American World Policy. New Jersey: Princeton University Press.

Lara, A. (2011). Ciência Política: Estudo da ordem e da subversão. Instituto de Ciências Sociais e Políticas. Lisboa.

Laurent, S. (2001). The French secret services: Intelligence and the politics of the republican legitimacy. Intelligence National Security.

Lowenthal, M. (2006), Intelligence: From Secrets To Policy. Washington: CQ Press.

MacGaffin, J. (2005), "Clandestine Human Intelligence – Spies, Counterspies, and Covert Action", in Sims, J. et al. (eds.) Transforming U.S. Intelligence, pp. 79-95. Washington: Georgetown University Press.

Marques, A. et al. (2002). 101 Perguntas e respostas do direito da internet e da informática. Centro Atlântico. V. N. Famalicão.

Marques, G. Martins, L. (2006). Direito da Informática. Almedina. Coimbra.

Matos, H. (2011), "O Terrorismo Internacional de Matriz Islamista. A Intelligence no Contraterrorismo". Lisboa: Instituto da Defesa Nacional.16 de 17

Matos, H. (2012a), "E Depois de Bin Laden? Implicações Estratégicas no Fenómeno Terrorista Internacional: Uma Reflexão", in Politeia, Ano VIII, 2011, pp. 9-38. Coimbra: ISCPSI.

Matos, H. (2012b) "Contraterrorismo Ofensivo, o "targeted killing" na eliminação de alvos terroristas: o caso dos EUA e Israel". Lisboa: ISCPSI (no prelo).

McGarrell, E. et al. (2007), "Intelligence-Led Policing As a Framework for Responding to Terrorism", in Journal of Contemporary Criminal Justice, Volume 23 (2), pp. 142-158.

Molina, A. (2002). Criminologia. 4. ed., rev. e atual. São Paulo: RT.

Moreira, A. et al (Coords.). (2004) Informações e Segurança. Prefácio. Lisboa.

Nunes, P. (2012) A Definição de uma Estratégia Nacional de Ciber Segurança, Nação e Defesa. N.º 133-5ª Série, pp. 113-127.

Pillar, P. (2003), Terrorism and U.S. Foreign Policy. Washington: Brookings Institute Press.

Pollard, N. (2009), "On Counterterrorism and Intelligence", in Treverton, Gregory et al., National Intelligence Systems. New York: Cambridge University Press, pp. 117-146.

Ratcliffe, J. (2008), Intelligence-Led Policing. Oregon: Willan Publishing.

Rego, H. (2007), "Global Threats Need Global Answers", in Revista Segurança & Defesa, n.º 4. Loures: Diário de Bordo.

Rego, H. (2010), "As Informações na Prevenção do Terrorismo", Comunicação efectuada, em 4 de Maio, na Conferência "Polícia e Informações na Prevenção do Terrorismo". Lisboa: ISCPSI.

Richelson, J. (1995). The U.S. Intelligence community. West press, Boulder-San Francisco Oxford.

Rodrigues, B. (2009). Direito Penal parte especial – Tomo I Direito Penal Informático-digital, Coimbra Editora.

Rogeiro, N. (2002). Guerra em tempo de paz: A defesa Nacional na nova ordem mundial. Hugin Editores. Lisboa.

Santos, G. (2007). Dicionário de criminologia. Icone editora. São Paulo.

Santos, L. (1983). Incursões no domínio da estratégia. Fundação Calouste Gulbenkian. Lisboa.

Severino, A. (2000). Metodologia do trabalho científico. 21, ed., rev. e ampl. Cortez. São Paulo.

Shulsky, A. et al. (2002), Silent Warfare, Understanding the World of Intelligence. Washington: Potomac Books.

Silva, A. (2006). A informação: Da compreensão do fenómeno e construção do objeto científico. Edições Afrontamento. Porto.

Silva, J. et al (1994). Direito da Informática – Legislação e Deontologia. Edições Cosmos. Lisboa.

Sims, J. et al. (eds.) (2009), Vaults, Mirrors & Masks. Rediscovering U.S. Counterintelligence. Washington: Georgetown University Press.

Todd, P. et al. (2004), Global Intelligence. The World`s Secret Services Today. New York: Zed Books.

Tomé, L. (2007) Revista Estratégia 24/25, Portugal e o futuro da Europa - De Roma a Lisboa. Bizâncio. Lisboa.

Torres, J. (2009), Terrorismo Islâmico, Gestão dos Riscos para a Segurança Nacional. Lisboa: EDIUAL.

Venâncio, P. (2011). Lei do Cibercrime. Coimbra Editora.

Vilela, A. (2009) Segredos e corrupção – O negócio de armas em Portugal. Casa das Letras. Alfragide.

Webster, C. Hucker, S. (2003). Release decision making. Hamilton, ON: Forensic Services, St. Joseph's Healthcare.

Comissão de Inquérito sobre A Vigilância electrónica em massa aos cidadãos da união Europeia, in http://www.europarl.europa.eu/committees/pt/gsahighlight.html?query=(2013%2f2188+(INI)).+&url=http%3a%2f%2fwww.europarl.europa.eu%2fcommittees%2fpt%2flibe%2fsubject-files.html%253Fid%253D20130923CDT71796

Resolução 2045(2015) do Conselho Europeu Relativo À Vigilância em Massa, in, http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692&lang=en