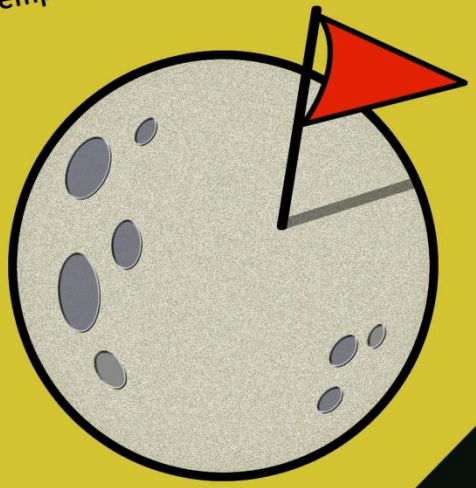
CYBERLAW by CIJIC

DIREITO: A PENSAR TECNOLOGICAMENTE

Em pleno século XXI, o ciberespaço assume-se como o novo plano da acção. Este, representa, entre outras dimensões, um conjunto cada vez mais alargado e eficiente de meios de comunicação e de informação ao serviço do Homem. A sociedade hodierna, inebriada por esta revolução tecnológica, numa quase-metamorfose híbrida, adapta-se a esta tecno-dependência. Mas, será que compreendemos, minimamente, o advento do ciberespaço e do tempo moderno em que vivemos?



CIJIC
Centro de Investigação Jurídica do Ciberespaço
da Faculdade de Direito de Lisboa

FACULDADE DE DIREITO
UNIVERSIDADE DE LISBOA

CYBERLAW by CIJIC

CYBERLAW by CIJIC Revista científica sobre *cyberlaw* | Número 01 janeiro 2016 | Grátis

DIREITO: A PENSAR TECNOLOGICAMENTE

cyber espaço
novas fronteiras

cyber ataques
algumas estratégias de mitigação

cyber segurança
preocupação global

outros
- direito constitucional do Inimigo
- obscurantismo
- DOTMLPI-I
- ENISA


CYBERLAW
by CIJIC

CYBERLAW by CIJIC

TECNOLOGIAS DE INFORMAÇÃO E SEGURANÇA PÚBLICA: UM EQUILÍBRIO INSTÁVEL

INFORMATION TECHNOLOGIES AND PUBLIC SECURITY: AN UNSTABLE EQUILIBRIUM

ANDRÉ INÁCIO [1]

[1] Ex-Inspetor da PJ, Auditor de Defesa Nacional, Doutorando em Direito Público.
Correio eletrónico: andrenacio@gmail.com

SUMÁRIO: 1. INTRODUÇÃO; 2. A *ACCOUNTABILLITY* COMO GARANTE DA SEGURANÇA PÚBLICA; 3. CONCLUSÃO

RESUMO

As Tecnologias de informação constituem-se como base dos sistemas de informações de segurança, porém operam também como importante ferramenta ao serviço da Criminalidade Organizada. No Estado de Direito Democrático, a Segurança constitui-se como um direito fundamental dos cidadãos, uma prestação a que o Estado se encontra obrigado, sendo que os novos fenómenos criminógenos, altamente complexos *determinam o recurso a novas metodologias de prevenção e combate, mais intrusivas nos Direitos Liberdades e Garantias do Cidadão.* O recurso às tecnologias de informação (TI) pelo sistema de segurança do Estado é uma necessidade premente, devendo porém assentar num quadro legal claro e objetivo, e ser alvo de sindicância adequada.

O presente estudo concentra ideias desenvolvidas na tese de doutoramento, cuja marcação da defesa o autor aguarda, e abordará o difícil equilíbrio decorrente do recurso às novas TI no hodierno modelo de segurança do Estado, incidindo na complexa, embora crucial, componente da *intelligence* policial.

Palavras-Chave: *Accountability*; Criminalidade; Direitos; Informações; Segurança Pública; TI.

ABSTRACT

Information Technologies are based on the security of information systems, but also operate as an important tool in service of Organized Crime. In a Constitutional State, Security was established as fundamental citizen's rights, a benefit to which the State is bound. The new, highly complex criminal phenomenon involves the use of new methods to prevent and combat more effectively the Rights and Freedoms guarantees the Citizen**.**

The use of IT by the state security system is urgently needed, but must be supported by a clear and objective framework. These reflections are based on the study which the author is developing in his doctoral thesis that examines the difficult balance the use of new IT in the State security model based on complex but essential component of police intelligence.

Keywords: Accountability; Criminality; Rights; Informations; Public security; IT.

1.INTRODUÇÃO

O Mundo tem vindo a sofrer mutações profundas ao longo das últimas décadas em consequência desse fenómeno *plúrimo* que se convencionou designar por "Globalização", o qual acarreta progresso, desenvolvimento mas também novos riscos e ameaças cuja natureza é cada vez mais incerta e dissimulada. As Tecnologias de Informação, vulgo TI, uma realidade indiscutivelmente omnipresente, encontram-se na vanguarda deste processo, constituindo-se como o mais recente desafio aos governos, indústria e público em geral, operando como facilitador do progresso tecnológico ou do incremento do nível de ameaça, conforme os fins para que sejam usadas.

Contemplando o conjunto dos recursos tecnológicos e computacionais destinados à produção e utilização de informação, a designação TI conglomera todas as formas de tecnologia destinadas à criação, armazenamento, troca e utilização de informação nos seus diversos formatos[2], possibilitando a inclusão das tecnologias de computação e de telecomunicações num mesmo conceito, englobando para além do processamento de dados, os sistemas de informação, a engenharia de *software* e a informática, sem descurar o "fator humano", questões administrativas e organizacionais[3]. Do *Tablet* pessoal às tecnologias de satélite, cabo e naturalmente às redes sociais, as TI constituem-se como o sustentáculo do atual modelo de vida.

Na base desse fenómeno encontra-se a disseminação da *internet,* criada inicialmente pela DARPA[4], para garantir comunicações fiáveis, mesmo em casos de ataques nucleares maciços ou de precisão e que acabou por se disseminar, impulsionando o conhecimento e o comércio globais, revelando-se também um extraordinário instrumento de aproximação entre o cidadão e a máquina governamental, permitindo a transmissão de documentos, arquivos e mensagens, bem como a consulta a repositórios remotos, desde que disponíveis em rede. Porém,

---

[2] A informação pode apresentar-se sob o formato de dados corporativos, imagens, vídeo, áudio, multimédia, etc.

[3] KEEN, P.G.W. *«Information Technology and the Management Theory: The Fusion Map»*. IBM Systems Journal, 1993, v.32, n.1 p. 17 e segts.

[4] *"The Defense Advanced Research Projects Agency (DARPA) was established in 1958 to prevent strategic surprise from negatively impacting U.S. national security and create strategic surprise for U.S. adversaries by maintaining the technological superiority of the U.S. military". http://www.darpa.mil/*

simultaneamente tal ferramenta origina fundados receios relativamente à dimensão dos danos que pode causar ao cidadão e/ou ao Estado.

Ao mesmo tempo que se constituem como base dos sistemas de informações de segurança, as TI operam também como importante ferramenta ao serviço da Criminalidade Organizada[5], alimentando as redes de pedofilia, exploração sexual e tráficos das mais variadas naturezas. Também o terrorismo de pendor salafista – de que a *Al-qaeda*, e mais recentemente o auto denominado Estado Islâmico, se constituem como os "*master franchising*" –, recorre às TI com enorme sucesso, para a difusão de propaganda, recrutamento e até a comunicação entre células terroristas.

Encontrando-se as economias modernas intrinsecamente dependentes de infraestruturas criticas como as redes de transportes, de fornecimento de energia e de comunicações, as quais operam totalmente dependentes das TI, a Cibercriminalidade, assume atualmente uma dimensão de arma política, económica e militar, operando sobretudo em três grandes domínios: as telecomunicações, a que recorrem para defesa própria e dissimulação da atividade, mas também pela exploração fraudulenta desses serviços; os meios eletrónicos de pagamento, nomeadamente pela falsificação de cartões de crédito e prática de burlas no domínio do comércio na *Internet* e, por fim, o acesso ilegítimo a alvos pré-definidos para sabotagem ou obtenção de dados confidenciais.

Assim, as TI têm introduzido novas fontes de conhecimento e criado novas vulnerabilidades, exigindo maior integração dos esforços operacionais e de *inteligência* entre as agências de segurança (militares, serviços de informações, policiais, etc.), face à crescente dimensão transnacional das ameaças. Os esforços vêm sendo empreendidos por indivíduos, organizações, empresas, bem como pelos Estados, de forma individual e coletivamente, visando desenvolver capacidades de resposta adequadas às hodiernas vulnerabilidades. Consequentemente, a forma como

[5] Conforme *«computerworld»,* 15 de Março de 2013 às 09:59:43*: "Os ciberataques são uma ameaça crescente. Estão perto do topo da lista das mais graves ameaças que os EUA enfrentam, com as preocupações a rivalizarem com o terrorismo e a Coreia do Norte, disseram as autoridades de inteligência da administração do presidente Barack Obama. O diretor de segurança nacional, James Clapper, e o diretor do FBI, Robert Mueller, estavam entre os funcionários que apontaram os ciberataques como as principais ameaças durante uma audiência realizada esta semana na Comissão de Inteligência do Senado. Clapper, um general reformado da Força Aérea, disse que não viu uma "matriz mais diversificada de ameaças e desafios" para a segurança nacional dos EUA durante o seu tempo na defesa e nas comunidades de inteligência."*

são coligidos, analisados, aplicados e acedidos esses dados pessoais, constitui-se como um dos riscos imanentes que importa despistar de forma isenta e segura a cada momento, acautelando hipotéticas violações dos Direitos Liberdades e Garantias.

Em resposta às crescentes ameaças não tradicionais à segurança das instituições, negócios e pessoas – de que cibercrime é uma componente em franco crescimento – os governos vem implementando renovadas iniciativas visando mitigar os riscos, nomeadamente ao nível da troca de informações sobre ameaças e vulnerabilidades detetadas.

Por sua vez, também a indústria tem sido sujeita a muitas das ameaças e problemas enfrentados pelos Governos ao nível da segurança, desde a sabotagem à espionagem económica, exigindo avultados investimentos no domínio da proteção de sistemas. Na verdade, é no setor privado que muito do trabalho para melhorar e proteger o domínio digital se está a desenvolver, pela urgência de encontrar respostas seguras, pelo facto de os processos de decisão serem bem mais rápidos e eficientes do que na pesada máquina administrativa do Estado, e sobretudo porque os seus decisores, ao contrário dos políticos em geral, tem a consciência de que a sobrevivência económica dessas entidades depende do investimento na sua segurança[6]. Os setores público e privado tendem assim a incrementar parcerias[7],

---

[6] AMARAL, Paulo Cardoso do, «*TOP SECRET – Como Proteger os Segredos da sua Empresa e Vigiar os seus Concorrentes*», Academia do Livro, Lisboa 2008, ISBN: 978-989-8194-02-2. (Pag. 17 e 18) …"*a gestão das informações é essencial para antecipar e compreender a envolvente das organizações. Em competição a antecipação e a surpresa são o segredo do sucesso. (...) Já num cenário de ética duvidosa, as organizações têm de se proteger com técnicas da contra-espionagem, do terrorismo e da subversão. É o que se chama «segurança». Por tudo isso é importante compreender a importância dos serviços de informações e as suas atividades de produção de informações e de segurança e contras espionagem no ambiente empresarial. (...) Quando se fala em segurança está a considerar-se a existência de espionagem, terrorismo e subversão. Para todas estas três vertentes, a produção de conhecimento sobre o que se está a passar no meio envolvente e as atividades de contra-espionagem fazem parte da doutrina da segurança".*

[7] Nos Estados Unidos, essas parcerias adquiriram enquadramento legal por via do "*Cyber Intelligen*ce *Sharing Act*", vulgo CISA: "Passed House amended (04/26/2012) Cyber Intelligence Sharing and Protection Act - Amends the National Security Act of 1947 to add provisions concerning cyber threat intelligence and information sharing. Defines "cyber threat intelligence" as intelligence in the possession of an element of the intelligence community directly pertaining to: (1) a vulnerability of a system or network of a government or private entity; (2) a threat to the integrity, confidentiality, or availability of such a system or network or any information stored on, processed on, or transiting such a system or network; (3) efforts to deny access to or degrade, disrupt, or destroy such a system or network; or (4) efforts to gain unauthorized access to such a system or network, including for the purpose of exfiltrating information. Excludes intelligence pertaining to efforts to gain unauthorized access to such a system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access. Requires the Director of National Intelligence (DNI) to: (1) establish procedures to allow intelligence community elements to share cyber threat intelligence with private-sector entities and utilities, and (2) encourage

visando aumentar a segurança de sistemas e infraestruturas, partindo para tal das lições aprendidas ao longo da última década em matéria de ameaças.

A dimensão da ameaça ultrapassa o âmbito nacional, pelo que a UE enquanto coletividade de Estados com fins comuns, vem desenvolvendo políticas comuns[8] nesta área. *Lord Robertson*, ex-Secretário-Geral da NATO[9], observou que a Europa "*...acordou coletivamente para a importância da recolha de informações e de partilha...*" e que a própria natureza da ameaça coletiva, bem como para uma nação em particular, mudou dramaticamente, em grande parte devido aos avanços na tecnologia. Hoje, muito do que fazemos tem lugar no domínio cibernético, sendo que a *inteligência* deve operar com base num leque maior de fontes de informação e técnicas adequadas, combinadas com o aumento da velocidade com que os eventos ocorrem.

É responsabilidade máxime do Estado controlar – no sentido de "assegurar da legalidade de" – os mecanismos de recolha, tratamento e utilização de informação, asseverando a necessária reserva da privacidade do cidadão e o direito à informação, ao mesmo tempo que tutela o bem comum, impedindo que a máquina administrativa e/ou judicial passem a controlar a vida das pessoas ou, evitando que se tornem tão legalistas que percam a noção do real e, na ânsia da defesa dos direitos do individuo de forma singular, ignorem a proteção de direitos fundamentais, também eles constitucionalmente protegidos, de natureza coletiva. Concomitantemente cumpre-lhe desenvolver as medidas atinentes à deteção e erradicação de vulnerabilidades, face ao elevado risco de entes criminosos acederem indevidamente aos sistemas de informações estatais ou de interesse público, manipulando-os ou destruindo-os.

---

the sharing of such intelligence. (…)" disponível em: https://www.congress.gov/bill/112th-congress/house-bill/3523

[8] A exemplo dessa preocupação a Comissão Europeia, vulgo CE, elaborou a «Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social europeu e ao Comité das Regiões» Bruxelas 24.7.2003 *COM(2013)542 final* – "Para um Sector de Defesa e Segurança Mais competitivo e Eficiente" –, documento que se assume como um plano de ação, onde se esboçam as linhas de criação da nova moldura para o desenvolvimento da cooperação Civil/Militar em matéria de indústria de Segurança e Defesa, rentabilizando os meios e dando resposta ao atual quadro de riscos e ameaças. A CE, nesse documento, exorta à criação de sinergias e regulação das relações comerciais no domínio da indústria de segurança e defesa, potenciando as valências de cada Estado membro, evitando a duplicação de esforços e acautelando a perda de direitos de propriedade intelectual, bem como, o investimento por parte de países terceiros em empresas estruturantes da defesa e segurança europeia. Importa apurar que "*novas abordagens de inteligência e capacidades são necessárias, especialmente de forma colaborativa ou conjunta, a fim de atender às necessidades de segurança coletiva da Europa".*

[9] *«Fórum Global Intelligence»* OTAN, Bruxelas, 20 e 21 de Setembro de 2012. Discurso proferido na conferência Inaugural.

2.A *ACCOUNTABILLITY* COMO GARANTE DA SEGURANÇA PÚBLICA

A segurança constitui-se como um valor inestimável, um pilar do Estado Social de Direito. Exige porém um equilíbrio complexo, asseverando a legalidade dos meios, na medida em que a ação do aparelho de segurança do Estado incide diretamente sobre a esfera mais restrita das liberdades fundamentais do indivíduo. Assim, a segurança desempenha um duplo papel de *"*condição*"* e "qualidade", necessários para o bem-estar individual e coletivo, tendo de ser encarado sobre um novo prisma, sem delimitações fronteiriças, temáticas, organizacionais ou outras. Tem de ser suficientemente amplo para garantir o regular funcionamento do Estado Social de Direito, no respeito pelas liberdades individuais e na defesa do interesse coletivo. Para tal, as autoridades socorrem-se de soluções inovadoras, baseadas em tecnologias emergentes, com a dupla função de poder processar em tempo útil a informação e de tentar garantir a segurança de elementos críticos de infraestruturas e ambientes de trabalho, desenvolvendo complexos sistemas de proteção, *firewall's* e antivírus, recorrendo ainda a elaborados sistemas eletrónicos de gestão de direitos. Ainda assim, a segurança dos sistemas contra acessos indevidos é uma luta permanente "do gato e do rato[10]".

As TI constituem-se como ferramentas indispensáveis à Segurança do Estado, a que recorrem desde os Serviços de informações aos corpos de polícia criminal e autoridades judiciárias, consubstanciando novas metodologias de investigação, cooperação policial e formas rápidas e eficientes de obter dados, que podem constituir meios de investigação e probatórios decisivos. *El tratamiento de la información es una herramienta fundamental en el desarrollo de la labor de protección de la seguridad pública que llevan a cabo las Fuerzas y Cuerpos de Seguridad"* [11].

São exemplos de TI aplicadas à Segurança e Justiça a vídeo vigilância, as escutas ambientais, as interceções telefónicas, a localização por satélite e sobretudo, concentrando, processando e disponibilizando toda a informação sobre cada alvo, os sistemas de informações, mais concretamente as bases de dados. Aí se destacando o

[10] Recorde-se como exemplo a referência constante no *«Relatório Anual de Segurança Interna»*, vulgo RASI, documento emitido pelo Secretário-geral do Sistema de Segurança Interna, na sua edição referente ao ano de 2010 onde se assume a deteção de tentativas de acesso ilegítimo a bases de dados governamentais, nomeadamente por Serviços de Informações de países terceiros.

[11] GUERRA, Amadeu*«El Tratamiento de Dados Personales Para Fines de Prevención e Investigación Criminal.»,* Revista Espanhola de Proteción de Datos, nº 7, Julio-Junio 2009-2010, pag. 11.

Sistema Integrado de Informação Criminal, vulgo SIIC[12] e a Base de dados de ADN[13]. Mas, o exemplo que melhor ilustra a preocupação subjacente à opção pelo tema são as recentemente implementadas bases de dados supostamente destinadas à prevenção e repressão de atentados terroristas, das quais se constituem como controverso exemplo, as desenvolvidas no âmbito da segurança da aviação civil contra actos de interferência ilícita, cujo objeto são os dados contidos nos registos de identificação dos passageiros (*PNR – Passenger Name Records)*. Tais bases de dados constituem-se como autêntico vértice da pirâmide da informação de segurança, por visarem a deteção de perfis criminosos[14]. Tal questão tem vindo a sofrer uma significativa evolução na última década, sendo relevante citar, numa perspetiva histórica, o parecer 8/2004 do Grupo de Proteção de Dados do Artigo 29.º[15]*".*

Constituindo-se o recurso às novas tecnologias em geral e às bases de dados em particular como instrumentos fundamentais da segurança do Estado e do cidadão, importa porém garantir o equilíbrio indispensável nos mecanismos de recolha,

---

[12]SIIC, Sistema Integrado de Informação Criminal, previsto no art.º 8º da *«Lei de Organização e Investigação Criminal» (LOIC), Lei 49/2008 de 27 de Agosto,* onde se pode ler: *"*1- *O dever de cooperação previsto no artigo anterior é garantido, designadamente, por um sistema integrado de informação criminal que assegure a partilha de informações entre os órgãos de polícia criminal, de acordo com os princípios da necessidade e da competência, sem prejuízo dos regimes legais do segredo de justiça e do segredo de Estado. 2 - O acesso à informação através do sistema integrado de informação criminal é regulado por níveis de acesso, no âmbito de cada órgão de polícia criminal. 3 - As autoridades judiciárias competentes podem, a todo o momento e relativamente aos processos de que sejam titulares, aceder à informação constante do sistema integrado de informação criminal. 4 - A partilha e o acesso à informação previstos nos números anteriores são regulados por lei."*

[13]Em Portugal a *«Lei 5/2008 de 12 de Fevereiro»,* criou a base de dados de perfis genéticos de ADN para fins de investigação criminal e civil.

[14] A análise de perfis criminais constitui-se, na sua génese como uma técnica forense, auxiliar da investigação Criminal, a qual a partir dos indícios e vestígios resultantes da análise de uma cena de crime e da vítima, procura identificar padrões comportamentais com o objetivo de predizer o comportamento, as características de personalidade e os indicadores sócio demográficos do autor, diminuindo o leque de suspeitos. Na sua atual dimensão, a técnica do *profiller* está já a roçar o limiar da ficção, pretendendo antecipar potenciais comportamentos criminosos com base no tratamento da informação disponível sobre os passageiros. Sobre os perfis criminais ver SOEIRO, Cristina, *«Os Perfis Criminais: Contornos e aplicabilidade de uma Técnica Forense»,* Ousar e Investigar – Revista de Reinserção Social e Prova, nº 4, Lisboa 2009, pag. 9-20. No que respeita à ficção DICK, Phillipp K. *"Relatório Minoritário",* imortalizado no cinema, em 2002 por Steven Spielberg, com Tom Cruise no principal papel.

[15] *Grupo de Trabalho de Proteção de Dados do Artigo 29.º, parecer 8/2004.* Trata-se de um orgão consultivo europeu independente em matéria de proteção de dados e privacidade. As suas atribuições são descritas no art.º 30º *da Diretiva 95/46/CE e no art.º 15º da Diretiva 2002/58/CE. "(...)Nos termos da legislação norte-americana, o Serviço das Alfândegas e Proteção das Fronteiras dos Estados Unidos (Customs and Border Protection – CBP) recebe informação sobre viagens e reservas, conhecida como dados contidos nos registos de identificação dos passageiros ou PNR, relativa a passageiros de voos entre a União Europeia e os EUA. O CBP compromete-se a utilizar estes dados contidos nos PNR para fins de prevenção e combate ao terrorismo e outros crimes transnacionais graves. O PNR pode incluir informação fornecida durante o processo de reserva ou proveniente de companhias aéreas ou agências de viagens. A informação será retida durante três anos e meio, pelo menos, podendo ser partilhada com outras autoridades*

tratamento e troca de informações, nas diversas modalidades de bases de dados no seio da organização Policial e do aparelho do Estado, impedindo atropelos ao respeito pelos princípios da *necessidade* e da *competência*, impondo-se a salvaguarda dos Direitos Fundamentais dos Cidadãos, constitucionalmente consagrados, o que apenas pode ocorrer sobre escrutínio democrático, por via das instituições de controlo, assegurando a *accountabillity*.

Atualmente, as próprias fronteiras geográficas são essencialmente referenciais no que concerne à atuação da criminalidade organizada e especialmente violenta, o que conduz à necessária implementação de sistemas em rede de informação policial, cujo controlo efetivo da legalidade do seu âmbito e fins de utilização se revela forçosamente mais difícil. *"A abordagem clássica em matéria de segurança exigia uma compartimentação rigorosa do ponto de vista organizacional, geográfico e estrutural das informações em função da sua sensibilidade e categoria. Esta abordagem deixou de ser realmente viável no mundo digital, uma vez que o processamento da informação está fragmentado."* [16]

Entretanto as parcerias público-privadas não se esgotam ao nível da indústria, e é aí que a *accountabillity* tem de funcionar de forma exemplar. Os custos e os limites legais impostos à Administração têm paulatinamente conduzido a uma política de parcerias também no domínio da recolha, gestão e tratamento de dados, conferindo poderes a entidades privadas no desempenho da segurança pública, nomeadamente no que respeita à gestão de sistemas de informação, o que acarreta genuinamente preocupações acrescidas em termos de controlo da legalidade. Conforme resultou da divulgação pública pelo ex-Analista da NSA *Edward Snowden*[17], existem graves riscos na relação com o setor privado devido ao desenvolvimento de parcerias que permitem ao Governo obter por via de entidades privadas, informações de segurança através de métodos a que estaria constitucionalmente inibido por via oficial.

O corolário dos riscos para a Democracia e o Estado de Direito será seguramente o Sistema designado por *National Surveillance State, vulgo NSS, o qual* conforme

[16] *«Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões», COM(2000)890 final.* Bruxelas 26.1.2001 (pag.6).
[17] SNODWDEN, Edward, ex-agente da CIA que expôs a mega operação de espionagem levada a cabo pelos EUA através da Agência Nacional de Segurança (NSA)

Jack M. Balkin[18], tem vindo a ser desenvolvido pelos Estados Unidos, desde os finais do século XX. Constituído por um conjunto de elaboradas bibliotecas digitais, interligadas entre si e destinadas ao apoio à decisão, que recolhem, analisam e cruzam informação sobre cidadãos, assume-se como uma nova forma de *governance* em matéria de informações, permitindo a recolha, análise e cruzamento de informações sobre indivíduos não apenas nos Estados Unidos mas também no resto do mundo. A fundamentação doutrinal de tal sistema assenta na relevância da identificação antecipada dos problemas, permitindo repelir potenciais ameaças e prestar apoio social às populações. Assim o NSS é patenteado como um caso especial de "Informações de Estado", visando identificar e resolver questões de *governance,* no interesse das populações.

Criada e desenvolvida com fundamento na ameaça terrorista, esta ferramenta encontra-se maioritariamente nas mãos de entidades privadas, consequência do aproveitamento por parte do Governo da evolução da tecnologia de informação e das parcerias com o sector privado, privatizando áreas fundamentais da segurança nacional, com consequentes perigos para a liberdade e cidadania. De facto, o recurso a tal sistema permite uma via paralela de aplicação das regras de prevenção contornando as garantias fundamentais constantes do "*Bill of Rights*[19]". Ao mesmo tempo, e resultado da sua eficácia, esta nova ferramenta tenderá a sobrepor-se, por pressão política, aos restantes sistemas na aplicação da lei geral, na resolução dos problemas de segurança diários, conduzindo a que a Segurança e a Justiça, até por questões de redução de custos, sejam cada vez mais delegadas em entidades privadas.

Como se compreende, são enormes os riscos resultantes da promíscua relação com o poder privado, permitindo às entidades oficiais aceder a informação por vias a que estariam constitucionalmente inibidos por via oficial. Simultaneamente, essas empresas privadas ficam de posse de informação sobre os cidadãos, permitindo a elaboração de "*ratings*" em tecnologia de informação, identificando possíveis clientes e afastando os que considere indesejáveis.

---

[18] BALKIN, Jack M., *«The Constitution in The National Surveilllance State»,* Minnesota Law Review, Vol. 93 Nº 1. 2008 Yale Law School Working Paper Nº 168
papers.ssrn.com/sol3/papers.cfm?abstract_id=1141524

[19] «*Bill of Rigths*», nome pelo qual as dez primeiras emendas à Constituição dos Estados Unidos são conhecidas.

Assim, o NSS veio colocar graves questões em sede de modelo de Estado de Direito, constituindo-se como o corolário dos excessos que importam prevenir, exigindo novas estratégias de preservação dos valores constitucionais e do governo democrático. Os Direitos Fundamentais têm de ser considerados com a sua verdadeira dimensão, eles são Pilares do regime e não instrumentos de governos.

3.CONCLUSÃO

As TI vieram para ficar, sendo impossível conceber um modelo de progresso e desenvolvimento à margem dessa tecnologia. Já a segurança do Estado, das empresas, da comunidade e do próprio cidadão passa pelo conhecimento. As informações são inevitáveis e legitimas, desde que necessárias e úteis, sendo que a insuficiência de informações conduz ao sentimento de isolamento e consequentemente ao medo. Acarreta porém garantias de escrutínio democrático e institucional dos procedimentos atinentes às informações em geral e às bases de dados em particular, garantindo o enquadramento institucional e organizacional apropriado. O mesmo é dizer, encontrar-se alicerçado num regime legal e num sistema de fiscalização que permita definir de forma objetiva o que se recolhe e trata; porque se recolhe e trata; como se recolhe e trata; e por último, quem acede e com que fim. Neste modelo de *accountabillit*y cumpre aos órgãos de fiscalização desenvolver um duplo papel, controlando a atuação dos sistemas de informações e garantindo a legalidade da sua atuação, contribuindo assim para que a população confie no sistema de segurança do Estado. Esta questão é tanto mais relevante na medida em que os direitos do cidadão, perante esta "máquina", se encontram extremamente mitigados, não tendo acesso aos registos em seu nome e consequentemente vendo-se impossibilitado de exercer o "contraditório". Compete pois aos órgãos de fiscalização assegurar a legalidade e idoneidade do processo, evitando discricionariedades por parte do sistema.

Numa frase, importa garantir a legalidade e particularmente os Direitos Fundamentais do cidadão, na utilização dessa ferramenta indispensável à eficácia do sistema de segurança que são as informações policiais.

Cumpre ao Estado garantir que a informação recolhida, o foi pelos motivos corretos, será tratada e guardada em função dos princípios da necessidade e da

competência, sendo apenas utilizada para fins de prevenção e combate à criminalidade, e para tal, disponibilizada em função do "*princípio da necessidade do conhecer*"[20], na exclusiva tutela da segurança da sociedade como um todo, acautelando o respeito pelos direitos de cada cidadão individualmente considerado. A tudo isto acresce o risco de acessos indevidos" às bases de dados policiais e consequente exposição pública, ilícita e difamatória, com as inerentes responsabilidades para os Estados. Ora, só um efetivo controlo democrático da atuação, permite assegurar o equilíbrio na complexa dicotomia "*dever de obter informações/respeito pelos Direitos fundamentais"*.

[20] O Principio da necessidade do conhecer constitui o pilar basilar da segurança em matéria de informações. Apenas tem acesso à informação quem dela necessite de ter conhecimento de forma legalmente justificável e apenas na medida do que necessita de saber.